TESIS DE DOCTORADO

HIGH DIMENSIONAL AUTOCOMPENSATING QUANTUM CRYPTOGRAPHY IN OPTICAL FIBERS IMPLEMENTED WITH DISCRETE AND INTEGRATED PHOTONIC DEVICES

Daniel Balado Souto

ESCUELA DE DOCTORADO INTERNACIONAL DE LA UNIVERSIDAD DE SANTIAGO DE COMPOSTELA

PROGRAMA DE DOCTORADO EN LÁSER, FOTÓNICA Y VISIÓN

SANTIAGO DE COMPOSTELA

2021

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

DECLARACIÓN DO AUTOR/A DA TESE

D./Dna. **Daniel Balado Souto**

Título da tese: **HIGH DIMENSIONAL AUTOCOMPENSATING QUANTUM CRYPTOGRAPHY IN OPTICAL FIBERS IMPLEMENTED WITH DISCRETE AND INTEGRATED PHOTONIC DEVICES**

Presento a miña tese, seguindo o procedemento axeitado ao Regulamento, e declaro que:

1) A tese abarca os resultados da elaboración do meu traballo.
2) De ser o caso, na tese faise referencia ás colaboracións que tivo este traballo.
3) Confirmo que a tese non incorre en ningún tipo de plaxio doutros autores nin de traballos presentados por min para a obtención doutros títulos.

E comprométome a presentar o Compromiso Documental de Supervisión no caso de que o orixinal non estea na Escola.

En **Santiago de Compostela**, **25 de Decembro de 2020**.

Sinatura electrónica

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

AUTORIZACIÓN DOS DIRECTORES DE TESE

HIGH DIMENSIONAL AUTOCOMPENSATING QUANTUM CRYPTOGRAPHY IN OPTICAL FIBERS IMPLEMENTED WITH DISCRETE AND INTEGRATED PHOTONIC DEVICES

D. Jesús Liñares Beiras
D. Xesús Prieto Blanco

INFORMAN:

Que a presente tese, correspóndese co traballo realizado por **D. Daniel Balado Souto**, baixo a nosa dirección, e autorizamos a súa presentación, considerando que reúne os requisitos esixidos no Regulamento de Estudos de Doutoramento da USC, e que como directores desta non incorremos nas causas de abstención establecidas na Lei 40/2015.

De acordo co indicado no Regulamento de Estudos de Doutoramento, declaran tamén que a presente tese de doutoramento é idónea para ser defendida en base á modalidade de Monográfica con reproducción de publicaciones, nos que a participación do/a doutorando/a foi decisiva para a súa elaboración e as publicacións se axustan ao Plan de Investigación.

En Santiago de Compostela, 23 de Decembro de 2020

Asdo.-Jesús Liñares Beiras

Asdo.-Xesús Prieto Blanco

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

Agradecementos

En primeiro lugar, quero agradecer aos meus directores da tese Suso Liñares e Xesús Prieto, sen os cales esta tese non sería posible. Grazas por toda a paciencia que tivestedes comigo, por todo o que aprendín de vos e por toda a axuda que me déstedes. Tamén quero agradecer ao meu vello compañeiro David Barral, do que aprendín moito no comezo desta etapa e tamén contribuíu de xeito fundamental a esta tese. A Héctor, pola sua imprescindible axuda experimental e consellos inestimables, e a Ana, polas non menos importantes aportacións mecánicas e polos momentos entretidos. A Carlos Montero, por tódalas dubidas que me resolveu e polos programas que me deixou. A Vicente Moreno, por todas esas conversas interesantes que me animaron días. A Gabriel, o meu relevo o que lle desexo unha boa tese. E por último, a todo o resto da xente do departamento, dos que tamén teño boas memorias.

Likewise, I would like to thank doctor Djeylan Aktas, for being my great supervisor in my stay at *QET Labs* from Bristol, where I did learn a lot and had a great time. Thanks to doctor Massimo Borghi as well, who also helped me a lot, and to the other great friends I met there: Javier, Takafumi, Jorge, Stefano, Caterina and all the others. And also, to my friend on the Way.

Quero agradecer tamén a todas aquelas persoas que me acompañaron durante todos estes anos. A Amelia, prezada amizade que está sempre aí, aturandome con amabilidade. A Yago, compañeiro de aventuras durante moitos anos, e a todos os seus consellos, axudas, críticas e demáis conversas entretidas. A Jose, por tódolos bos momentos compartidos ao longo da vida. A David Ferro, que apareceu cando me atopaba baixo para levantarme o ánimo e que ahí segue. A David Mosquera, gran persoa e novo gran compañeiro de xogo que espero dure moito tempo. A Penín, e tódalas suas historias. Aos cabaleiros restantes Álvaro e Rebeca, por tódalas risas. A Anita, eterna compañeira deportiva. A Garaboa, por tódalas comidas amenas e boas conversas. A Tato, a ver se recuperamos os vellos tempos. A Malpica, sempre confiable. Tamén quero acordarme do resto de compañeiros que me acompañaron durante a carreira, e de toda a xente que me acompañou o longo dos anos.

Pero, sobre todo, teño que darlle as grazas ao máis importante da miña vida: a miña familia. A todos os meus tios e tias, especialmente aos que xa non están, por tódolos bos recordos que teño e que espero ter. A tódolos meus primos e achegados, por todo o que desfrutei e seguirei disfrutando sempre que estou ao voso lado. E por último e máis importante, a meus pais Gerardo e Otilia, a miña irmá María, e a miña avoa Otilia. Grazas por terme educado, coidado, apoiado, regañado e, por suposto, querido durante toda a miña vida.

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

A miña familia.

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

Caminante, son tus huellas
el camino y nada más;
caminante, no hay camino,
se hace camino al andar.

Antonio Machado



No hay camino
que no tenga fin.

Séneca

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

Resumo

O tema principal de esta tese de doutormanento circumscribese principalmente no ámbito da criptografía cuántica. Dentro das tecnoloxías baseadas na óptica cuántica, a criptografía cuántica representa, xunto coa computación cuántica, unha das tecnoloxías en desenvolvemento con maior potencial para transformar a nosa sociedade. Dita tecnoloxía basease no uso das propiedades cuánticas da luz para desenvolver sistemas de comunicación totalmente seguros. Deste xeito, a encriptación cuántica consiste en enviar unidades de información cuantica, denominadas qubits (estados cuanticos $|0\rangle$ y $|1\rangle$), para transmitir una clave de encriptación coa que cifrar as mensaxes. Debido ás propiedades dos estados cuánticos, calquera intento de obter ou copiar un qubit resulta na súa alteración. Isto permite descubrir a presenza dun espía que interfire na comunicación. Esta tecnoloxía non só está en desenvolvemento nos laboratorios, senón que xa se está a aplicar e probar a gran escala. Por exemplo, recentemente, probouse con éxito transmisións cuánticas seguras vía satélite. Aínda que o estudo da seguridade desta área baséase na teoría matemática da información, a súa implementación, baseada na luz, depende enteiramente de diversos campos da óptica, como a fotónica cuántica, a óptica integrada e as fibras ópticas. A óptica cuántica naceu co concepto de fotón introducido por Einstein e estuda as propiedades cuánticas da luz. Este campo non só constitúe a base fundamental do cifrado cuántico a través do estudo dos estados cuánticos da luz, senón que tamén é a orixe de moitas tecnoloxías necesarias para a súa implementación. Por outra banda, as fibras ópticas e a óptica integrada, baseadas na transmisión confinada de luz, constitúen o principal medio de transmisión e procesamento de información de luz respectivamente. Nesta tese abordanse estes campos centradondose na súa aplicación á criptografía cuántica. O obxectivo principal da tese consiste no deseño de novos sistemas de cifrado cuántico autocompensados en alta dimensión. Aumentar a dimensión permite aumentar a seguridade do sistema, mentres que a autocompensación busca resolver os problemas actuais na transmisión. Os obxectivos adicionais da tese son o deseño de dispositivos fotónicos discretos e integrados necesarios para a súa implementación, incluído o desenvolvemento de tecnoloxía para fabricalos neste último caso.

O protocolo base para o cifrado cuántico foi proposto por Bennet e Brassard en 1984 e recibe o nome de BB84 na súa honra. Este protocolo propón usar dous pares de estados cuánticos dun só fotón como qubits pertencentes a dúas bases diferentes pero mutuamente

imparciais. Segundo o protocolo, o remitente de información, comúnmente chamado Alice, envía os seus fotóns codificando os seus bits clave nos diferentes qubits, seleccionando aleatoriamente a base empregada. Ao mesmo tempo, o receptor, chamado Bob, mide os estados de incidencia tamén seleccionando aleatoriamente a base de medida. Teoricamente, sempre que Alice e Bob usen a mesma base para codificar e medir estados, os bits enviados e recibidos deberían ser idénticos. Non obstante, se un espía (Eve) interfire na comunicación, poden aparecer erros. Dado que Eve debe medir os fotóns de Alicia ao azar, sempre que non use a base correcta medirá e reenviará o estado equivocado a Bob o 50 % das veces. Ergo, Alice e Bob poden detectar a presenza de Eve comparando unha fracción dos seus bits e medindo a taxa de erro. No caso de que a comunicación sexa segura, Alice e Bob usan os bits non compartidos para xerar unha clave segura coa que cifrar a información. O BB84 orixinal propón usar fotóns polarizados ortogonalmente como bits usando dúas bases xiradas 45 ° unhas das outras. Outra posibilidade é construír os catro estados cuánticos requiridos mediante diferentes desprazamentos de fase introducidos entre dous modos base. Estes modos poderían ser, por exemplo, modos espaciais dunha fibra, modos desfasados temporalmente ou modos de camiño (modos espaciais de dúas guías diferentes). O BB84 é un dos protocolos de criptografía cuántica máis empregados, pero tamén ten problemas na súa aplicación. Por exemplo, a anisotropía das fibras pode causar erros cando se traballa con modos de polarización, xerando desfases e acoplando enerxía entre os mesmos. Para solucionalo, propuxéronse métodos de autocompensación "plug and play", que buscan corrixir posibles atrasos mediante estratexias de ida e volta. Tamén se empregan recursos como fibras que manteñen a polarización. Non obstante, isto só se fixo para dúas dimensións e con modos de polarización. O BB84 pode ser xeneralizado a máis dimensións. Usar máis dimensións ten a gran vantaxe de que garante unha maior seguridade e que se transfire máis cantidade de información por pulso de sinal. Para xeneralizar o BB84, pódense empregar diferentes estratexias como o uso de estados de luz con momento angular ou, como se propón na tese, modos colineales de fibras de poucos modos ou modos codireccionais de fibras multinúcleo. Os dous tipos de fibras están a ser considerados actualmente para o seu uso en redes ópticas de alta capacidade mediante multiplexación espacial.

Un dos principais problemas en moitas áreas do procesamento de información cuántica, non só na criptografía, está no desenvolvemento de dispositivos que actúen como fontes de estados cuánticos de luz. Especialmente importante é o desenvolvemento de fontes que emitan de forma eficiente estados dun só fotón. Ademais, o estudo de diferentes estados cuánticos permite o desenvolvemento de novas formas de transmitir e procesar información. Este é, pois, o principal obxectivo do capítulo 2 desta disertación: o estudo de elementos ópticos e estados cuánticos que se poidan aplicar na criptografía e así contribuír ao deseño de fontes para xeralos. Deste xeito, o capítulo comeza expoñendo o formalismo cuántico da propagación espacial da luz en guías de onda proposto previamente polo noso grupo e analiza os fundamentos sobre os que se basean as principais fontes de fotóns. Por unha banda, existe a atenuación de feixes coherentes emitidos por láser e con aleatorización de fases, para extraer estados cuánticos de moi poucos fotóns.

Por outra banda, o fenómeno de conversión paramétrica descendente espontánea (SPDC) úsase para producir pares de fotóns enredados, onde se detecta un deles para avisar de que o outro foi emitido. Máis tarde, o capítulo segue presentando o formalismo cuántico dos principais elementos ópticos que se empregarán, non só no capítulo, senón ao longo da tese, para deseñar os nosos sistemas e dispositivos. Deste xeito, introdúcense os diferentes elementos que realizan transformacións SU(2) nas diferentes clases de modos que se poden empregar: láminas de onda para modos de polarización, acopladores direccionais para modos de camiño e convertidores de lentes cilíndricos para modos espaciais. Na parte final do capítulo, estes elementos utilízanse xunto coa SPDC para producir un tipo especial de estado cuántico de luz chamado estados vórtice cuánticos. Estes estados son particularmente interesantes porque son análogos aos vórtices clásicos que levan momento angular. De feito, dependendo da clase de modos empregados, os vórtices cuánticos poden levar impulso físico. Se se utilizan modos de polarización, os vórtices levan momento de xiro (espín). Cos modos espaciais, levan momento angular orbital. Mentres que se se usan modos de camiño, pódese considerar que teñen un momento angular ficticio. Isto é importante, xa que tales estados de momento poden usarse para construír un espazo de Hilbert de alta dimensión útil para varias tecnoloxías de información cuántica. Na tese, analizamos inicialmente como se poden obter estes estados en modos de polarización e espaciais, cunha expansión no anexo, onde se estuda como afecta o grao de compresión ao momento. Máis tarde, estas ideas desenvólvense en dous traballos que adxuntamos. Neles deseñamos dous dispositivos integrados para xerar estes e outros estados cuánticos para o seu posible uso en varias aplicacións. En particular, na tese centrámonos nunha das súas principais aplicacións á criptografía: xerar varios estados cuánticos dun só fotón pertencentes a bases mutuamente imparciais coas que aplicar o protocolo BB84. En particular, vemos como o noso xerador ten a vantaxe de que selecciona aleatoriamente a base do estado e, xunto con outro, o estado tamén se pode obter aleatoriamente. Ademais, o dispositivo pódese estender para xerar bases mutuamente imparciais en dimensións maiores, podendo ser usado para criptografía cuántica de alta dimensión.

O capítulo 3 trata do deseño de sistemas de cifrado cuántico autocompensados para implementar o protocolo BB84 en alta dimensión en fibras de poucos modos colineales. Estas fibras consideráronse como posibles solucións á transmisión óptica mediante multiplexación espacial, polo que é de interese analizar as súas posibilidades nas comunicacións cuánticas. Para xerar un estado cuántico codificado de alta dimensión, proponse o uso dun estado dun fotón que pode estar en distintos modos espaciais. Entre estes modos, que se corresponden cos distintos modos transmitidos por unha fibra de poucos modos, introduciranse diferentes desprazamentos de fase que determinarán o estado cuántico. A dimensión do estado depende trivialmente do número de modos N empregados e as fases deben garantir estados pertencentes a bases mutuamente imparciais. O principal problema que pode xurdir é a aparición de desfases e atrasos entre os modos ao longo das fibras que modifican o estado, así como a existencia de acoplamento entre os modos. Para resolver este último problema, pódense utilizar fibras de núcleo elíptico, xa que reducen o acoplamento espacial. Para o primeiro, este capítulo propón un sistema de autocompensación

baseado na transmisión de estados cuánticos en bucle. Este método consiste no seguinte. Para comezar, Bob xera o estado fundamental e mándao a Alice. Esta usa un dispositivo, ao que chamamos un "espello de Faraday efectivo" (EFM), cuxo propósito consiste en intercambiar modos espaciais de xeito ordenado e, despois, reenvia o estado a Bob. Unha vez máis, Bob reenvía o estado a Alice, xerando un bucle que repite un total de N veces. Dado que en cada viaxe de ida e volta intercambianse os modos, todos eles acaban experimentando os mesmos desfases e atrasos ao completar o proceso e, polo tanto, conséguese unha autocompensación das flutuacións de fase. Nalgúns casos, Bob tamén pode aplicar un EFM, reducindo á metade o número de bucles necesarios. Na última viaxe de ida e volta, Alice codifica a información nos estados desprazando a fase dos diferentes modos, mentres que Bob procede a medir o estado ao recibilo. Non é necesario que cada fotón faga todos os bucles de ida e volta antes de enviar o seguinte, senón que varios fotóns poden viaxar simultaneamente. Para non confundir os estados nos diferentes bucles, pódense empregar diferentes estratexias. Por exemplo, pódese enviar un paquete de fotóns seguido dun espazo en branco mentres se espera a que o primeiro complete o ciclo, ou ben pódense intercalar fotóns (e tamén paquetes) de diferentes bucles. Despois de expoñer o método, o capítulo analiza a seguridade destes sistemas, estudando os principais ataques aos que pode estar suxeito. O primeiro é o ataque *photon number-splitting* (división de número de fotóns) que aproveita a emisión realista de estados de múltiples fotóns dos que se podería extraer un para obter toda a información. Este ataque resólvese introducindo estados *decoy* (señuelo) cos que se pode detectar a presenza do ataque. Posteriormente, dedúcese a seguridade do BB84 de alta dimensión baixo o ataque de clonación cuántica, que busca copiar o estado cuántico o máis fielmente posible, obtendo a taxa de de xeración de chave segura dependente dos erros. Por último, estúdase un ataque específico ao que o noso sistema podería ser vulnerable: o ataque *phase remapping* (mapeado de fase). Este ataque aproveitase do tránsito de Bob a Alice para retrasar os estados, de xeito que, cando Alice os recibe para cifralos, os seus moduladores non aplican o desprazamento de fase desexado. Deste xeito, Alicia enviaría sen sabelo estados modificados que Eve pode interceptar e medir, extraendo máis información que nunha intercepción clásica. Despois, Eve enviaría os estados teóricos sen modificar correspondentes ás súas medidas, polo que Bob non detectaría irregularidades. Na nosa análise vimos que este ataque non obtén mellores resultados para Eve que os que podería obter mediante a clonación cuántica. Polo tanto, o noso sistema de bucle non presenta debilidades maiores que un sistema unidireccional. O atraso dos estados tamén se pode usar para facer que entren nos detectores durante o seu tempo morto, eliminando selectivamente as detección non desexadas. Non obstante, de novo isto non consegue mellores resultados, mesmo cando se combina co ataque anterior. O capítulo remata cun artigo publicado que detalla un sistema de autocompensación que utiliza modos espaciais básicos xunto coa polarización para implementar o BB84 en catro dimensións con só dous ciclos necesarios para conseguir autocompensación. Aínda que o sistema anterior utiliza elementos e dispositivos ópticos discretos en Alice e Bob, é obviamente interesante considerar a posibilidade de usar dispositivos integrados, dada a súa alta robustez óptica e a súa compatibilidade con fibras ópticas, especialmente se

se usa fibras multi-nucleo (MCF). Polo tanto, esta tese plantexa a viabilidade destes dispositivos integrados en plataformas baseadas no intercambio iónico en vidro, o que sería unha excelente solución para comunicacións cuánticas con MCF.

Outro obxectivo desta tese consistiu na fabricación de elementos ópticos integrados que se poden empregar para a criptografía. En particular, o interese estaba na fabricación dos elementos básicos constituíntes dos dispositivos integrados: os acopladores direccionais. Estes elementos pódense empregar como proxectores de estados cuánticos en modos guiados para medir ditos estados, e incluso como xeradores do mesmo. En xeral, nos circuítos fotónicos integrados, as guías de onda están feitas de óxido ou nitruro de silicio sobre un substrato de silicio. No noso laboratorio contamos con tecnoloxía de intercambio iónico en vidro, tecnoloxía que a penas se usou para estes fins, a pesar de que pode chegar a ser máis accesible en certos casos. O capítulo 4 ten como obxectivo demostrar a viabilidade de usar esa tecnoloxía para fabricar acopladores e proxectores para criptografía. Para conseguilo, montouse primeiro un sistema litográfico de foto-redución en dous pasos para poder obter unha imaxe reducida de só un centímetro a partir dun deseño de acopladores impreso de varios decímetros. A imaxe reducida do deseño proxéctase mediante o sistema fotolitográfico sobre unha capa de fotoresina, situada á súa vez sobre unha capa de aluminio que cubre un vidrio. Mediante procedementos químicos (revelado da fotoresina e mordida do aluminio) elimínase a zona iluminada do aluminio, imprimíndose nel o deseño das guías. Posteriormente, estes vidrios cunha máscara protectora gravada son sometidos a un proceso de intercambio iónico nun forno, obtendo guías de canles integradas nos mesmos. Algunhas mostras expuxeronse a un segundo proceso de intercambio para enterrar as guías. Para estes procesos empregáronse sales de prata e potasio. Con estas técnicas litográficas fomos capaces de fabricar guías de onda integradas de menos de 3 micras de ancho, que formaban acopladores. Algunhas mostras experimentaron un segundo proceso de intercambio para enterrar as guías. Para estes procesos empregáronse sales de prata e potasio. Con estas técnicas litográficas fomos capaces de facer guías de onda integradas de menos de 3 micras de ancho, que formaban acopladores. En cada mostra deseñáronse varios bloques de acopladores con diferentes lonxitudes e espazamentos entre guías. A última parte do capítulo está dedicada á caracterización das mostras obtidas mediante dous procedementos. Por unha banda, realizouse unha caracterización mediante microscopía de contraste de interferencia diferencial (DIC). Esta técnica consiste en tomar imaxes das mostras baixo diferentes polarizacións nun microscopio Nomarski. Posteriormente, procesándoas mediante un algoritmo de catro-pasos, pódese obter a compensación introducida polas guías. Deste xeito, podemos medir os principais parámetros experimentais dos acopladores. Por outra banda, para caracterizar o comportamento dos acopladores, configurouse un sistema óptico para introducir luz coherente a través das diferentes guías e medir a saída obtida coa axuda dunha cámara. Analizando os resultados, obtivéronse as curvas de fabricación de acopladores de potasio en vidro para guías de 3 micrómetros, segundo a súa lonxitude e a separación entre guías. Ademais, coa axuda dunha rede de difracción sen orde 0, levouse a cabo un experimento de proxección para verificar a súa posible aplicación como medidores de estados cuánticos en modos

de camiño. Deste xeito, introducíronse dous feixes idénticos a través das entradas dun acoplador de 50-50% e observouse como a saída dependía do cambio de fase entre ambos feixes. Para os desprazamentos de fase de 0 e π, a luz saía igualmente dividida por ambas saídas, mentres que para os desfases de $\pi/2$ e $3\pi/2$, a luz saía totalmente por unha ou outra saída respectivamente.

Finalmente, o capítulo 5 está dedicado ao deseño de novos sistemas de autocompensación mediante dispositivos integrados como os xa analizados. Polo tanto, neste capítulo utilízanse modos de camiño (diferentes guías de onda) para construír un estado cuántico de un só fotón en alta dimensión onde o estado será determinado polos desprazamentos de fase entre os diferentes modos. Para transmitir este tipo de estado, as fibras multi-núcleo son especialmente relevantes, xa que cada núcleo pode usarse para transmitir cada un dos modos guiados nos que se pode atopar o fotón. O acoplamento entre modos transmitidos por diferentes núcleos é moi débil, pero a existencia de flutuacións de fase entre eles segue sendo un problema. No capítulo propóñense dous métodos de autocompensación. Para comezar, o mesmo método de autocompensación de propagación en bucle anterior foi proposto nun artigo publicado. No mesmo, Bob usa un sistema de circuladores ópticos integrados para realizar a permutación modal necesaria para a compensación de fase, mentres que Alice usa circuladores e láminas de media onda para reenviar os estados a Bob compensando as flutuacións de polarización en cada viaxe. Bob usa un sistema de acoplador reconfigurable co que seleccionar se os estados incidentes de Alice van aos circuladores continuando o bucle ou, pola contra, van ao sistema de medición despois de completar todas as voltas. No artigo presentamos algúns dispositivos de proxección integrados para realizar medicións de estados cuánticos en modos guiados de dimensión $N = 2^n$. Estes estados corresponden aos mesmos estados das bases mutuamente imparciais producidas polo noso xerador estendido, propostas no capítulo 2. O segundo método de autocompensación que propoñemos consiste en empregar o fenómeno da conxugación de fases. Trátase dun efecto non lineal que aparece durante a mestura de catro ondas nun cristal non lineal. A interacción de dúas ondas de bombeo xunto cunha terceira incidente produce un cuarta reflectida cuxo campo é o conxugado complexo da terceira. Esta técnica utilizouse en moitas aplicacións para corrixir as fluctuacións dunha imaxe. No capítulo mostramos que a técnica serve para compensar acoplamientos e desfases entre os modos guiados, xa que, cuanticamente, tradúcese nunha conxugación dos operadores que engloban ditos fenómenos. Deste xeito, Alice pode usar un "espello de conxugación de fases" para devolver os estados base enviados por Bob, codificándoos previamente. Este método ten a gran vantaxe sobre o anterior de que só require unha viaxe de ida e volta, pero o uso do devandito espello non é doado.

En conclusión, propuxemos varios sistemas para implementar o protocolo BB84 autocompensado en alta dimensión usando diferentes estratexias. Ao mesmo tempo, deseñamos dispositivos incrustados para xerar e medir estados cuánticos que se poden usar tanto na criptografía como noutras tecnoloxías cuánticas. Finalmente, demostramos a viabilidade de fabricar estes dispositivos con tecnoloxía de intercambio iónico en vidro.

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

Contents

Resumo **xiii**

Contents **xxi**

List of Figures **xxvii**

List of Tables **xxxi**

Abbreviations **xxxiii**

1 Introduction **1**
1.1 Context . . . 2
1.1.1 Quantum Optics . . . 2
1.1.2 Quantum Cryptography . . . 3
1.1.3 Realistic implementation of QKD and problems . . . 7
1.2 Aims and structure . . . 10
1.2.1 Aims . . . 10
1.2.2 Methodology . . . 11
1.2.3 Thesis outline . . . 12
1.3 Works by author . . . 13
1.3.1 List of Publications . . . 13
1.3.2 Conference works . . . 14

2 Quantum States And Devices For Quantum Cryptography **15**
2.1 Quantum light and devices for quantum cryptography . . . 17
2.1.1 Quantization of light spatial propagation . . . 17
2.1.2 Weak coherent state source . . . 19
2.1.3 Generation of biphoton states with SPDC . . . 20
2.1.3.1 SPDC Type I . . . 21
2.1.3.2 SPDC Type II . . . 22
2.2 Bulk and integrated devices for QC . . . 23
2.2.1 Devices for QC with polarization modes . . . 23
2.2.1.1 Polarization beam splitter . . . 23
2.2.1.2 Waveplate . . . 24

2.2.2 Integrated Devices for QC . . . 25
2.2.3 Devices for QC with spatial modes . . . 26
2.2.3.1 Laguerre-Gaussian and Hermite-Gaussian modes . . . 26
2.2.3.2 Quantum transformations between LG and HG modes . . 28
2.2.3.3 Cylindrical lens converters . . . 30
2.2.3.3.1 Gouy phase . . . 30
2.2.3.3.2 Mode converter . . . 30
2.2.3.4 Quantum Transformation Of The Converters . . . 33
2.2.3.4.1 Modes with N=1 . . . 34
2.2.3.5 Mach-Zehnder interferometer with CLC . . . 35
2.3 Quantum states engineering for QC . . . 36
2.3.1 Quantum vortex states with SAM, OAM and FAM . . . 36
2.3.2 Generating quantum vortex states with SPDC . . . 38
2.3.2.1 Generation of SAM vortex states with SPDC . . . 38
2.3.2.1.1 Employing SPDC type I . . . 38
2.3.2.1.2 Employing SPDC type II . . . 41
2.3.2.2 Single-photon-subtracted two-mode squeezed state in OAM 43
2.3.3 Generating quantum vortex squeezed states in integrated devices with FAM . . . 44
2.3.3.1 Non reconfigurable integrated device . . . 44
2.3.3.2 Reconfigurable integrated device . . . 47
2.4 Discrete variable quantum key distribution with vortex states . . . 49
2.4.1 Mutually unbiased basis . . . 49
2.4.2 Generation of single-photon MUBs with our devices to implement DV-QKD . . . 52
2.4.3 Generation of MUBs of higher dimension . . . 54
P1 Generation and Detection of Continuous Variable Quantum Vortex States via Compact Photonic Devices . . . 57
P1.1 Introduction . . . 58
P1.2 Device operation . . . 59
P1.3 Realistic scenario . . . 65
P1.4 Order and handness detection . . . 71
P1.5 Conclusions . . . 74
P2 Engineering continuous and discrete variable quantum vortex states by non-local photon subtraction in a reconfigurable photonic chip . . . 75
P2.1 Introduction . . . 76
P2.2 CV & DV entanglement in a reconfigurable photonic chip . . . 78
P2.2.1 Device operation . . . 78
P2.2.2 CV quantum vortex states . . . 82
P2.2.3 DV quantum vortex states . . . 86
P2.2.4 Discussion . . . 87
P2.3 Non-classicality and entanglement . . . 89

P2.4 Conclusions . . . 93
P2.5 Acknowledgements . . . 93
P2.6 Appendix A . . . 93
A APPENDIX . . . 95
A.1 Generation of quantum vortex squeezed states . . . 95
A.1.1 Generating SAM squeezed vortex states . . . 95
A.1.1.1 Single-photon squeezed state vortex . . . 95
A.1.1.2 Multi-photon squeezed state vortex . . . 97
A.1.2 Generating quantum vortex squeezed states with OAM . . . 98

3 Autocompensating Quantum Cryptography in Few-Mode Fibers 103
3.1 Original BB84 protocol, perturbations and solutions . . . 104
3.1.1 BB84 protocol . . . 105
3.1.2 Quantum States Perturbation in Optical Fibers . . . 109
3.1.2.1 Polarization perturbations and Plug and play systems . . . 110
3.1.2.2 Fiber modes perturbation . . . 112
3.2 Quantum Cryptography Autocompensation by Multi-loop Propagation . . . 114
3.2.1 Effective Faraday Mirror . . . 114
3.2.2 Autocompensating QKD in EC-FMF fibers in high dimension . . . 116
3.2.2.1 Multi-loop system . . . 117
3.2.2.2 Generating the qudits . . . 118
3.2.2.3 Autocompensating process in dimension D . . . 119
3.2.3 Transmission rate limitations . . . 121
3.2.4 Autocompensation in two dimensions . . . 123
3.2.4.1 Generator . . . 124
3.2.4.2 Detector . . . 125
3.2.4.3 Autocompensating system . . . 127
3.2.5 Autocompensation in four dimensions . . . 128
3.3 Cryptographic Security Study under Side Channel Attacks . . . 129
3.3.1 Photon number splitting attack and decoy states protocol . . . 129
3.3.2 Quantum cloning . . . 131
3.3.2.1 No-cloning theorem . . . 132
3.3.2.2 Quantum cloning machine . . . 133
3.3.2.3 Quantum cloning attack on the BB84 protocol . . . 134
3.3.2.4 Security of a HD-QKD system under quantum cloning attacks . . . 135
3.3.3 Phase remapping attack . . . 137
3.3.3.1 Overview . . . 137
3.3.3.2 Application to our four dimensional system . . . 139
3.3.3.2.1 QBER in our system . . . 139
3.3.3.2.2 Minimization of the QBER . . . 141
3.3.3.2.3 Minimization of QBER for the 4-dimensional case 142

3.3.3.3 Generalization to more dimensions . . . 144
3.3.3.3.1 General case . . . 144
3.3.3.3.2 Case $N = 2^m$ . . . 145
3.3.3.4 Detector efficiency mismatch attack . . . 146
3.3.3.4.1 Fake states attack . . . 146
3.3.3.4.2 Generalization for more dimensions . . . 149
3.3.3.4.3 Combination of PR and FS attack . . . 151
P3 Phase auto-compensating high-dimensional quantum cryptography in elliptical-core few-mode fibers . . . 153
P3.1 Introduction . . . 154
P3.2 High-dimensional BB84 Protocol in EC-FMF fibers . . . 156
P3.3 Phase auto-compensating cryptography in EC-FMF fibers . . . 158
P3.3.1 Mode Converter and Mach-Zehnder Interferometers . . . 159
P3.3.2 OFD, MID and RTC . . . 160
P3.3.3 Phase auto-compensating Process and Ququarts . . . 163
P3.4 Random detection system and measurement . . . 164
P3.5 Security analysis . . . 166
P3.6 Conclusions . . . 172

4 Experimental Development of Quantum Projectors 173
4.1 Integrated Quantum Projectors . . . 174
4.1.1 Directional couplers (DC) for SU(N) transformations . . . 174
4.1.2 An introduction to integrated quantum projectors (IQP) . . . 177
4.1.3 Introduction to ion exchange in glass and lithography for IQPs fabrication . . . 180
4.2 Fabrication of IQPs by ionic exchange . . . 181
4.2.1 Ion exchange . . . 181
4.2.1.1 Thermal diffusion . . . 182
4.2.1.2 Experimental setup . . . 183
4.2.1.3 Selection of the fabrication parameters by planar waveguides 186
4.2.1.3.1 Silver salt characterization . . . 187
4.2.1.3.2 Potassium salt characterization . . . 188
4.2.1.3.3 Effective index analysis . . . 188
4.2.1.3.4 Index profile characterization . . . 189
4.2.2 Design of IQPs . . . 191
4.2.2.1 Design parameters for ion exchange . . . 191
4.2.2.1.1 Effective index and WKB approximation . . . 191
4.2.2.1.2 WKB analysis of fabrication parameters . . . 192
4.2.2.1.3 Burying channel waveguides . . . 195
4.2.2.2 Geometrical design of photomasks . . . 196
4.2.3 Fabrication of the metallic motifs of our IQPs . . . 201
4.2.3.1 Substrate cleaning . . . 202

4.2.3.2 Metal layer deposition . . . 202
4.2.3.3 Photoresist deposition and development . . . 203
4.2.3.3.1 Photoresist deposition . . . 204
4.2.3.3.2 Photoresist development . . . 204
4.2.3.4 Photoresist exposition . . . 205
4.2.3.4.1 Printing the original design . . . 205
4.2.3.4.2 First photo-reduction . . . 206
4.2.3.4.3 Second photo-reduction . . . 208
4.2.3.5 Metallic layer etching . . . 211
4.2.4 Cutting and polishing of the IQPs . . . 212
4.2.4.1 Stack . . . 212
4.2.4.2 Cutting of the glass . . . 213
4.2.4.3 Lapping and polishing . . . 213
4.2.4.3.1 Lapping . . . 215
4.2.4.3.2 Polishing . . . 215
4.2.4.4 Sample holder . . . 216
4.3 IQPs characterization . . . 217
4.3.1 Characterization of the IQPs through a four-step phase shifting algorithm . . . 217
4.3.1.1 Description of the polarizing interference microscopy . . . 217
4.3.1.2 Experimental setup and image acquisition . . . 218
4.3.1.3 Four-step phase shifting algorithm . . . 220
4.3.1.4 IQPs analysis . . . 222
4.3.1.4.1 Silver exchanged waveguides . . . 225
4.3.1.4.2 Potassium exchanged waveguides . . . 227
4.3.2 Semi-classical characterization of the IQPs through coherent light . 230
4.3.2.1 Experimental setup . . . 230
4.3.2.2 Coupling analysis . . . 232
4.3.2.2.1 Silver exchanged samples . . . 232
4.3.2.2.2 Potassium exchanged samples . . . 233
4.3.2.3 Projection experiment . . . 240

5 Autocompensating Quantum Cryptography in Multicore Fibers 243
5.1 Autocompensation by multi-loop propagation . . . 244
5.1.1 Multi-loop system with MCFs and integrated devices . . . 244
5.1.2 Proposed autocompensation system . . . 246
5.2 Autocompensation by phase conjugation . . . 247
5.2.1 Phase conjugation of coherent states . . . 247
5.2.1.1 Degenerate four-wave mixing . . . 247
5.2.1.2 Operator propagation equations . . . 248
5.2.1.3 Application to the coherent state . . . 250
5.2.1.4 Phase conjugation . . . 250

5.2.2 Phase conjugation for HD-QKD . . . 251
5.2.2.1 Modal coupling between cores . . . 252
5.2.2.2 Modal and polarization coupling . . . 253
5.2.3 BB84 autocompensating system . . . 254
P4 Phase and polarization autocompensating N-dimensional quantum cryptography in multicore optical fibers . . . 257
P4.1 Introduction . . . 258
P4.2 N-dimensional autocompensating method . . . 259
P4.2.1 Primary quantum state generator . . . 259
P4.2.2 Autocompensating process . . . 260
P4.2.3 Maximum distance and light circulation analysis . . . 262
P4.3 Generation of signal quantum states (Alice System) . . . 264
P4.4 Random projective measurement integrated device (Bob System) . . . 267
P4.4.1 Case $N = 4$ . . . 267
P4.4.2 Case $N = 8$ . . . 270
P4.4.3 Case $N = 2^n$ . . . 271
P4.4.4 Splitter Device . . . 272
P4.5 Security analysis . . . 274
P4.6 Conclusions . . . 280
P5 Fully autocompensating high-dimensional quantum cryptography by optical phase conjugation . . . 281
P5.1 Introduction . . . 282
P5.2 Optical phase conjugator . . . 283
P5.3 Autocompensation with codirectional modes . . . 284
P5.4 Autocompensation with spatial and polarization modes . . . 286
P5.5 General SU($2N$) autocompensation . . . 287
P5.6 Optical fiber setup for HD-QKD . . . 288
P5.7 Free space optical communications . . . 290
P5.8 Summary . . . 290
P5.9 Acknowledgements . . . 290

6 Conclusions **291**

Bibliography **293**

List of Figures

2.2.1 Hermite-Gaussian and Laguerre-Gaussian modes . . . 27
2.2.2 Decomposition of diagonal HG_{nm} modes (a) and LG_{nm} modes (b) modes into linear HG_{nm} modes. . . . 29
2.2.3 Cylindrical lens mode converter . . . 31
2.2.4 MZIC and MZIC demultiplexer . . . 36
2.3.5 Local quantum vortex with $r = 0.5, \phi = 0$. . . . 39
2.3.6 Obtention of a polarization quantum vortex with SPDC I. . . . 40
2.3.7 Global vortex with $r = 0.5, \phi = 0$. . . . 41
2.3.8 Obtention of a polarization quantum vortex with SPDC II. . . . 42
2.3.9 SPDC to generate a vortex state with HG modes. . . . 43
2.3.10 Non reconfigurable vortex integrated device. . . . 45
2.3.11 Plots of probability and phase densities of quantum vortices of order $n = 1$ and $n = 3$ with a squeezing factor $r = 0.25$ . . . 46
2.3.12 Reconfigurable vortex integrated device. . . . 47
2.4.13 Generator system to randomly produce the four states belonging to the MUB of dimension 2. . . . 53
2.4.14 Device for increasing a guided mode vortex state to four (a) and eight (b) dimensions. . . . 55
2.4.15 Device for increasing a guided mode vortex state to 2^m dimensions. . . . 56
P1.1 Sketch of the device proposed for producing CV quantum vortices . . . 60
P1.2 Plots of probability and phase densities of quantum vortices of order 1 and 2 with a squeezing factor $s = 0.25$. . . . 63
P1.3 Plots of the Wigner distribution on the phase space for quantum vortices of order 1 and 2 with a squeezing factor $s = 0.7$ . . . 65
P1.4 Fictitious beam splitter as a model of imperfect detection . . . 67
P1.5 Plots of $-\pi^2 W_{E'}(0,0,0,0)$ and heralding probability $Pr_{on,off}$ for different values of squeezing s, weakly couplers transmission t . . . 68
P1.6 Comparison of the Wigner functions related to quantum vortices obtained by APD heralding and a superposition of ideal Wigner functions for the first two vortex orders . . . 70
P1.7 Plots of $-\pi^2 W_{E'}(0,0,0,0)$ for different values of propagation and coupling losses in the main channels η, total efficiency of ancillary detectors ν and modal purity ζ . . . 70

P1.8 Integrated detection system. The device is made up of a $3\,dB$ DC and two PNRDs. . . . 71
P1.9 Plots of the fidelity $\mathcal{F}$ between the detected state and a quantum vortex $|1_+\rangle$ for a realistic detection system with dark counts of thermal and Poissonian origin. . . . 73
P1.10 Plots of the joint probability distribution of the detected number of photons $Pr_{n_1',n_2'}$ for an input quantum vortex $|1_+\rangle$ with $s = 0.5$ . . . 74
P2.1 Sketch of the photonic circuit proposed for engineering CV entangled quantum states . . . 77
P2.2 Plots of probability and phase densities of a CV circular quantum vortex with squeezing factor $r = 0.3$ and $\eta' = 1$. . . . 82
P2.3 Plots of probability and phase densities of a CV elliptical quantum vortex with squeezing factor $r = 0.3$ and $\eta' = 5$ . . . 83
P2.4 Sketch of the photonic circuit proposed for engineering three-mode CV entangled quantum states . . . 85
P2.5 Plots of probability density of DV quantum vortex states with $\eta' = 1$ and 5 87
P2.6 Plot of the Wigner function related to a CV circular quantum vortex with $r = 0.3$ . . . 90
P2.7 Ratio between the logarithmic negativity of CV vortex states and that corresponding to a two-mode squeezed vacuum over a range of values of the squeezing parameter r and different values of ellipticity given by Φ. . . . 92
A.1 Quantum vortex obtained from a single-photon squeezed state with $r = 0.5, \phi = 0$. . . . 96
A.2 Quantum vortex obtained from a multi-photon squeezed state with $r = 0.5, \phi = 0$. . . . 98
A.3 Squeezed vortex state with three HG modes, with $r = 0.5$, $\phi = 0$. . . . 99
A.4 Squeezed vortex state with three HG modes, with $r = 0.5$, $\phi = 0$. Slides . . 100

3.1.1 Quantum key distribution comprises a quantum channel and a public classical authenticated channel . . . 104
3.1.2 Birefringence diagram. . . . 110
3.2.3 Effective Faraday Mirror system. . . . 116
3.2.4 Sketch of the modal phase autocompensating encryption system . . . 119
3.2.5 Transmission strategy of intercalated states for D=4 . . . 121
3.2.6 Transmission strategy of intercalated groups of states for D=4 . . . 123
3.2.7 X, Y, X', Y', L, D modes . . . 124
3.2.8 Generator device of modes X', L, Y', D. . . . 125
3.2.9 Detector device of modes X', L, Y', D. . . . 126
3.2.10 Plug and play autocompensating system for dimension 2. . . . 127
3.3.11 Bit rate in 2, 4 and 8 dimensions using 2 and $N + 1$ basis. . . . 137
3.3.12 Time response of the phase modulator . . . 138
3.3.13 QBER achieved in a PR attack for different δ in dimension $N = 4$ . . . 143

3.3.14 QBER achieved in a PR attack for different δ in different dimensions N and with n_b basis used. . . . 146
3.3.15 Detectors efficiency mismatch between two SPDs. . . . 147
3.3.16 Detectors efficiency mismatch between four SPDs. . . . 149
3.3.17 QBER achieved in a PR attack combined with a detector attack . . . 152
P3.1 Spatial modes used in this work . . . 157
P3.2 Sketch of the modal phase auto-compensating encryption system . . . 159
P3.3 (a) RTC and (b) OFD. . . . 162
P3.4 Detectors for basis $\bigotimes\oslash$, $\bigodot\bigcirc$, $\bigoplus\bigcirc$ and $\bigodot\ominus$ . . . 164
P3.5 Bit rate in 2 and 4 dimensions using two basis. . . . 167
P3.6 Time response of the phase modulator. The original pulse is time-shifted so it reaches the modulator at time t_δ instead of time t_θ. . . . 168
P3.7 QBER achieved in a PR attack for different δs . . . 170
P3.8 QBER achieved in a PR attack combined with a detector attack . . . 171

4.1.1 General directional coupler for implementing a SU(2) transformation. . . . 175
4.1.2 IQP for dimension 3. . . . 178
4.1.3 IQP for dimension 4. . . . 179
4.2.4 Experimental setup to realize thermal diffusion. . . . 184
4.2.5 Experimental evolution of n_{eff} in function of time for the different modes and for the silver and potassium salts . . . 189
4.2.6 Gaussian and complementary error function fitting of the planar waveguide index n in function of its depth d for the silver and potassium salts . . . 190
4.2.7 IQP unit. . . . 197
4.2.8 Design IQP AC1. . . . 199
4.2.9 Design IQP AC2. . . . 200
4.2.10 Photo-lithographic and ionic exchange processes. . . . 201
4.2.11 Two types of glasses employed in the fabrication process metallized with aluminium and covered by photoresist . . . 203
4.2.12 Experimental setup to implement the first reduction . . . 207
4.2.13 Experimental setup to implement the second photo-reduction. . . . 208
4.2.14 Different elements of the second photo-reduction system . . . 209
4.2.15 Image of the IQPs provided by the second photo-reduction objective . . . 211
4.2.16 Stacking of samples . . . 213
4.2.17 Struers Accutom-2 saw. . . . 214
4.2.18 Lapping and polishing processes . . . 214
4.2.19 Final polished and mounted samples . . . 216
4.3.20 Differential interference contrast (DIC) microscopy . . . 219
4.3.21 Transmitted phase introduced by IQPs in false colour for silver waveguides 223
4.3.22 Transmitted phase introduced by IQPs in false colour for potassium waveguides . . . 223
4.3.23 Aluminium mask of the IQP AC012 as view through an objective Nikon $\times 20$ .224

4.3.24 Linear mean profile of the transmitted phase perpendicular to the waveguides 226
4.3.25 Profile of the transmitted phase along a line perpendicular to the potassium exchanged waveguides . . . 229
4.3.26 Simplified diagram of the optical setup. . . . 230
4.3.27 Experimental optical setup for the IQPs characterization . . . 231
4.3.28 Images of light losses in buried silver waveguides . . . 232
4.3.29 Light modes obtained on the CMOS after introducing TE light in different IQPs . . . 235
4.3.30 Coupling propagation phase in function of the coupler length for different waveguides separation . . . 237
4.3.31 Coupling propagation phase in function of the waveguide separation for different coupler lengths . . . 237
4.3.32 Coupling constant of AC2K2 (potassium diffused buried waveguides) in function of the waveguide separation. . . . 239
4.3.33 Projection system . . . 240
4.3.34 Light intensities in both outputs in function of the displacement of the grating and the introduced phase between beams . . . 242
4.3.35 Light output after introducing two identical light beams from both inputs changing the phase ϕ between them . . . 242

5.1.1 Basic setup of autocompensating high-dimensional cryptography by multi-loop propagation in MCFs . . . 245
5.1.2 Effective Faraday mirror implemented with integrated optical circulators. . 245
5.2.3 Four-wave mixing with two pump waves. . . . 247
5.2.4 Basic setup of autocompensating high-dimensional cryptography by phase conjugation . . . 254
P4.1 Primary quantum state generator from a coherent source . . . 260
P4.2 Sketch of the optical system . . . 261
P4.3 Sketch of an Electro-Optical Attenuator (EOA). . . . 265
P4.4 Projective measurement device for dimension $N = 4$. . . . 268
P4.5 Projective measurement device for dimension $N = 8$. . . . 270
P4.6 Projective measurement device for dimension $N = 2^n$. . . . 272
P4.7 Integrated splitter for dimension $N = 4$ (4D-IS) together with 4D-PMs. . . 273
P4.8 Passive splitter for dimension $N = 2^n$ . . . 274
P4.9 Bit rate in 2, 4 and 8 dimensions using 2 and $N + 1$ basis. . . . 276
P4.10 Time response of the phase modulator . . . 277
P4.11 QBER achieved in a PR attack for different δ in different dimensions N and with n_b basis used. . . . 279
P5.1 Four-wave mixing system . . . 285
P5.2 Basic optical fiber setup for autocompensating HD-QKD by OPC . . . 288

List of Tables

2.1 Examples of values of coefficient $b(x, y, z)$. 28
2.2 Phase values for each MUB fro $D = 4$. 54

3.1 BB84 qubits. 105
3.2 QKD using BB84 without an eavesdropper 107
3.3 QKD using BB84 with eavesdropper 108
3.4 Upper bound on QBER that guarantees security against individual attacks for different dimension and number of basis. 136
3.5 Quantum states represented in notations b, s and k_1, k_2 140
3.6 Minimum eigenvalues of the different quantum states of 4-dimensional MUBs. 143
3.7 Maximum and minimum QBER values under PR attack 145
3.8 Probabilities of Bob's detection for different cases 147
3.9 Probabilities of Bob detection for different cases in four dimensions. Eve sends the same state that she measures. 150
P3.1 Sixteen quantum states of four MUBs used in this work. 156
P3.2 Quantum states represented in notations b, s and k_1, k_2 169

4.1 Salt characterization. Number of modes, Δn and penetration depth in function of time. 187
4.2 Potassium salt characterization for polarization mode TE. Number of modes, Δn and penetration depth in function of time. 188
4.3 Index change. 190
4.4 Upper limits of effective index and penetration depth of monomode waveguides. 194
4.5 Main parameters used to obtain the main samples analysed latter. 195
4.6 IQPs design parameters 197
4.7 Minford design parameters of the IQPs 198
4.8 Main parameters of the IQP AC2D0 with silver superficial waveguides. . . . 225
4.9 Main parameters of the IQP AC2X1 with silver buried waveguides. 225
4.10 Main parameters of the IQP AC2K4 with potassium superficial waveguides. 228
4.11 Main parameters of the IQP AC2K2 with potassium buried waveguides. . . 228
4.12 Coupling measures for superficial potassium IQP AC2K4. Relative light intensity (i_i) in percentage that exits by the outputs 2|3 after enter by input 1(2). 234

4.13 Coupling measures for buried potassium IQP AC2K2. Relative light intensity (i_i) in percentage that exits by the outputs 2|3 after enter by input 1(2). 234
4.14 Coupling measures for buried AC2K4 in terms of phase with unity π. . . . 235
4.15 Coupling measures for buried AC2K2 in terms of phase with unity π. . . . 236
4.16 Fitting parameters of the coupling curves from Figure 4.3.30. 236
4.17 Fitting parameters of the coupling curves from Figure 4.3.31. 236

P4.1 Upper bound on QBER that guarantees security against individual attacks for different dimension and number of basis. 275
P4.2 Maximum and minimum QBER values under PR attack 280

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Abbreviations

- **SPAPD**: avalanche photodiodes.
- **AOS**: Alice's optical system.
- **B92**: Bennett QKD protocol proposed in 1992.
- **BB84**: Bennett and Brassard QKD protocol proposed in 1984.
- **BOS**: Bob's optical system.
- **BS**: beam splitter.
- **BW**: broad bandwidths.
- **CL**: collimating lens.
- **CLC**: cylindrical lens converters.
- **CSG**: coherent states generator.
- **CV**: continuous variable.
- **CW**: continuous wave.
- **DV-QIP**: continuous variable quantum information processing.
- **CV-QKD**: continuous variable quantum key distribution.
- **DC**: directional coupler.
- **DIC**: differential interference contrast (microscopy).
- **DNQ**: diazonaphthoquinone.
- **DS**: detection system.
- **DV**: discrete variable.

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

- **DV-QIP**: discrete variable quantum information processing.
- **DV-QKD**: discrete variable quantum key distribution.
- **EC**: elliptical core.
- **EC-FMF**: elliptical core few-mode fiber.
- **EFM**: effective Faraday mirror.
- **EOA**: electro-optical attenuator.
- **EOR**: electro-optical rotators.
- **EPS**: electro-optical phase shifter.
- **FMF**: few-mode fiber.
- **FS**: fake states (attack).
- **FWM**: four wave mixing.
- **GMCS**: Gaussian modulated coherent state.
- **HD**: high dimension.
- **HD-QKD**: high dimension quantum key distribution.
- **HG**: Hermite-Gauss.
- **HWP**: half-wave plate.
- **IO**: integrated optics.
- **IS**: integrated splitter.
- **IQP**: integrated quantum projector.
- **LG**: Laguerre-Gauss.
- **LN**: lithium niobate.
- **M/DM**: multiplexer/demultiplexer.
- **MCF**: multicore fiber.
- **MDI**: measurement-device-independent.
- **MTF**: modulation transfer function.

- **MZI**: Mach-Zehnder interferometer.
- **MZIC**: Mach-Zehnder interferometer with cylindrical lens converters.
- **OC**: optical circulators.
- **OF**: optical fiber.
- **OFD**: optical fiber delay.
- **OFS**: optical field-strength space.
- **OPC**: optical phase conjugation.
- **PBS**: polarizing beam splitters.
- **PC**: phase conjugation (mirror).
- **PGM**: propylene glycol methyl ether.
- **PL**: photon lantern.
- **PM**: projective measurement (device).
- **PNRD**: photon number-resolving detectors.
- **PNS**: photon number splitting (attack).
- **PPLN**: periodically poling lithium niobate.
- **PR**: phase remapping (attack).
- **POVM**: positive-operator valued measure.
- **PSA**: phase-shifting algorithm.
- **PVD**: Physical Vapour Deposition.
- **QBER**: quantum bit error rate.
- **QC**: quantum cryptography.
- **QCM**: quantum cloning machine.
- **QFT**: quantum field theory.
- **QI**: quantum information.
- **QIP**: quantum information processing.

- **QKD**: quantum key distribution.
- **QLE**: quantum light engineering.
- **QPM**: quasi-phase matching.
- **QSG**: quantum state generator.
- **QVS**: quantum vortex states.
- **QWP**: quarter-wave plate.
- **RDC**: reconfigurable directional couplers.
- **RPS**: relative phase shifter.
- **RTC**: round trip controller.
- **SDM**: space division multiplexing.
- **SG**: state generator.
- **SMF**: single mode optical fiber.
- **SOC**: set of optical circulators.
- **SPAPD**: single-photon avalanche photodiodes.
- **SPDC**: spontaneous parametric down conversion.
- **SSPD**: superconducting single-photon detector.
- **TES**: transition edge sensor.

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

1

Introduction

Light-based technologies have become fundamental part of our current information society. For instance, fiber optics communications have allowed for higher transmission rates, permitting transmission over longer distances, higher bandwidths and lower losses than electrical cables. Thus, optical fibers are behind the internet we use nowadays. The laser, acronym for "light amplification by stimulated emission of radiation", is one of the most important inventions of 20th century and it is used in countless applications like laser printers, fiber-optic and free-space communications, optical disk drives, industrial cutting and welding of materials, manufacturing of micro-electronic devices through photolithography, laser surgery and even for entertainment purpose between many others. Telescopes and light sensors help us to explore space and study the Universe, like mapping the cosmic microwave background of the Big Bang, while it also help us to study our own planet, analysing its atmosphere and predicting the weather. Light-based technologies also have great importance in medicine: medical imagery enables non-intrusive diagnoses and light-based therapies can target cancer cells selectively.

However, perhaps the most promising applications of light lay in the fields of integrated and quantum optics. These fields open the gate to new technologies destined to change our society based on quantum information processing like quantum computing or quantum cryptography, main focus of this thesis. Photonics, the science of photon generation, detection and manipulation, becomes fundamental in the development of quantum computers, able to solve certain computational problems substantially faster than classical computers (quantum supremacy). At the same time, the quantum properties of light enable the design of strategies to transmit data in a secure way. Therefore, it is not an exaggeration to say that photonics will play a role as important in our society in the 21st century as the one electronics played in the 20th century.

1.1 Context

1.1.1 Quantum Optics

The study of light can be traced back to the pioneering work of Ibn Al-Haytham, *Kitab al-Manazir* (Book of Optics), published in 1015. Classical optics began with the discovery of light refraction made by Snell in 1621, and of light diffraction made by Grimaldi in 1660. To explain such effects, Christiaan Huygens proposed the first theory of light in his book *Traité de la lumière* (Treatise on light) published in 1690, where he proposed the notion of light as a wave. However, Isaac Newton challenged this conception and proposed instead a corpuscular theory of light to explain light reflection and refraction, which was published in his book *Opticks*in 1704. This theory became the main theory about the nature of light until Young's double-slit experiment, made in 1801, demonstrated light interference.After that, Augustin-Jean Fresnel worked on the formalization of a new wave theory to explain the new phenomena in 1815 and James Clerk Maxwell described the electromagnetic theory of light propagation in 1865, establishing definitely the main body of classical modern optics. However, in the 20th century our understanding of the fundamental nature of light changed, giving birth to a new field known as quantum optics.

The rise of such field can be traced back to Max Planck's works on the black-body radiation, where he introduced the quantization of energy. He proposed that electromagnetic radiation was emitted in discrete packets of energy, which he called "quanta", and that they were fundamentally indistinguishable [Planck, 1900b, Planck, 1900a]. Based on this, Albert Einstein conceptualized light as being made of this quanta ´´particles´´ and used it to successfully explain the photoelectric effect [Einstein, 1905]. These light quanta received latter the name of *photons*. Planck and Einstein's works became the starting point of the foundation of quantum mechanics. Niels Bohr made also use of the quantization hypothesis of optical radiation to explain the spectrum of discharge emission from hydrogen and propose his theory of the quantized energy levels of atoms [Bohr, 1913]. In 1924, Louis De Broglie suggested that not only light can behave like a particle, but that subatomic particles can behave as waves too, establishing the wave-particle duality [Broglie, 1924]. Following this, Erwin Schrödinger developed an equation to calculate the wave function of a system and how it changes dynamically in time, while Werner Heisenberg formulated his uncertainty principle about the position and momentum of a particle [Heisenberg, 1927]. By 1930, the works of David Hilbert, Paul Dirac, John von Neumann and others had completely unified and formalized quantum mechanics Nonetheless, light-matter quantum interactions were studied more through the point of view of research into matter, rather than research into the nature of light. This changed with the development of laser science.

A few years latter of his revolutionary idea, Einstein explained the interaction of electromagnetic radiation with atoms leading to the idea of *stimulated emission* [Einstein, 1917], which constitutes the basis of the operation of lasers. Moreover, Einstein introduced the concept of entangled quantum states in [Einstein et al., 1935], which eventually has

become fundamental in quantum information processing (QIP). Dirac also contributed to the quantum study of light with his quantization of the electromagnetic field , which lead to the development of the *quantum field theory* (QFT). However, quantum optics would not truly boost until 1950s, with the development of masers by Townes and his group [1], and later the lasers by Townes and Shawlow [2]. The need of good theoretical foundations of the laser, as well as the fruitful research that it generated, led Glauber, Sudarshan and Mandel to apply quantum theory to deeply study photo-detection and the statistics of light, developing the quantum theory of optical coherence [Mandel and Wolf, 1995]. Thus, the concept *coherent state* of light was introduced by Glauber [Glauber, 1963b, Glauber, 1963c], which is the solution of the quantum harmonic oscillator and it is a quantum state closely related to the classical solution of the harmonic oscillator. Both, Sudarshan and Glauber, made use of *quasi-probability distributions* for the study of quantum problems [Sudarshan, 1963, Glauber, 1963a] introducing the *Sudarshan-Glauber P representation* of a quantum system in the phase space. These works reflected that light can not be fully described by classical electromagnetic waves, which led to the study of non-classical states of light, such as the squeezed coherent states [Walls, 1983], and their generation through non-linear optics [Slusher et al., 1985]. The arise of quantum optics has led to remarkable results such as the development of *laser cooling* and *atom traps* [Phillips, 1998], the demonstration of *quantum entanglement* [Freedman and Clauser, 1972, Aspect et al., 1982] and *quantum teleportation* [Bennett et al., 1993, Braunstein and Kimble, 1998], and the generation of *quantum logic gates*. Nowadays, the most interesting areas of research of quantum optics lay in the use of quantum states of light for quantum communications, metrology, sensing and computation, that is technologies based on *quantum information*. Between this technologies, one of the most promising and close to be widely implemented is quantum cryptography.

1.1.2 Quantum Cryptography

In the meantime, another discipline arose as well during the mid-twentieth century. This discipline was *information theory*, which studies the concept of information and tries to mathematically describe the different tasks associated to it such as communication, coding and encryption. Based on the pioneering works of scientists like Alan Turing and John Von Neumann, information theory was formally founded by mathematician Claude E. Shannon with his historical work *A Mathematical Theory of Communication* published in 1948 [Shannon, 1948]. In his paper, Shannon introduces the basic elements of communication (source, transmitter, channel and receiver), defines the concept of *information entropy* and introduced the term *bit* as a unit of information. Information theory main goal is to find the fundamental limits of signal processing and data compression, which can be summed up in obtaining the highest possible transmission rate over a communication channel.

[1] They were developed independently by Basov and Prokhorov.

[2] Also independently developed by Gould.

Shannon also studied cryptography, that is, how information can be coded and transmitted in order to establish secure communications. In cryptography, any message send between a sender, usually called Alice, and a receiver, referred as Bob, must be encrypted by the use of a secret key that supposedly only Alice and Bob can know. Shannon proved that, to ensure perfect security in the information coding, the secret key must be as long as the message to encrypt, although he does not explain how to obtain such a long secret key. This is quite problematic, because Alice and Bob must find a way to confidentially share such a long secret key. Cryptographers have been developing several ways to send encrypted information since the seventies. However, classical ciphers encrypt messages using secret keys much smaller than the message size, which, as Shannon showed compromises perfect security [Van Assche, 2006]. For example, one of the most used public-key cryptography schemes, the RSA scheme, uses two large prime numbers to generate a a secret key. The security of this scheme is justified in the assumption that factoring the product of two large prime numbers is practically impossible with classical computing.

In any case, even if information can be defined as a mathematical concept, any bit of information must necessarily be stored or written in a physical medium and, thus, information is subjected to the laws of physics. Landauer was the first in realize the importance of this and established in his principle that any irreversible manipulation of information must led to an increase of entropy in the physical support [Landauer, 1961]. But this fact had a really interesting implication. Shannon's theory essentially assumes a classical physical support, but if you consider as the physical support of information a medium subjected to the laws of quantum mechanics, like for example a subatomic particle, the behaviour of information is quite different. This led to the rise of *quantum information theory*.

While the unit of information in classical information theory is the bit, whose value can either be 0 or 1, encoding information in a quantum state allows the possibility that the unit of information takes both values simultaneously. Therefore, the unit of information in quantum information theory is the qubit. This became the foundation of quantum computers. In a classical computer, computation is done with bits, while a quantum computer works with qubits. Processing qubits is like processing several combinations of zeroes and ones simultaneously, which leads to an exponential increase in the computation speed. This exceptional speed opens the possibility of solving problems that classical computation is unable to, leading to the so called *quantum supremacy*. One of these problems is the factorization of large integer numbers, which can be done through a quantum computer implementing the *Shor algorithm*. This threatens to make several public-key cryptography schemes, like the RSA one, obsolete. Therefore, it becomes necessary to develop new forms of cryptography that can fulfil Shannon condition.

The first to propose encoding information in a quantum system was Stephen Wiesner with his idea of quantum money [Wiesner, 1983]. This idea consisted of using the spin of particles to design bank notes impossible to forge. As the spin of a particle obeys the uncertainty principle, no forger can perfectly copy its state and will unavoidably make mistakes. Based on Wiesner's idea, Charles Bennett and Gilles Brassard were

the first to realize the high potential of applying quantum mechanics in cryptography in a paper presented at the conference CRIPTO'82 [Bennett et al., 1983]. This was the beginning of *quantum cryptography*, as they coined it. Not long after this, Bennett and Brassard came with the idea of using photons to transmit an arbitrarily long random secret key. They presented their idea in the 1983 *IEEE Symposium on Information Theory* (ISIT), which was published the next year [Bennett and Brassard, 1984]. In their work, Bennett and Brassard took advantage on the quantum property that measuring a quantum state results in the perturbation of such state in order to develop a protocol where any eavesdropper would inevitably be detected. In this way, if a bit of information is encoded in a photon, because of the uncertainty principle, any attempt by an eavesdropper to know the information carried by the photon leads inevitably to the loss of part of the information. Therefore, Alice and Bob can detect the errors caused by an eavesdropper on the transmission line and determinate if the communication is secure [Bennett et al., 1992b].

In essence, Bennett and Brassard had just proposed the first protocol for the distribution of secret keys taking advantage of the principles of quantum mechanics, which has been known since then as the BB84 protocol. This gave birth to *quantum key distribution* (QKD), the principal application of quantum cryptography and the most feasible one of the field of quantum information science [Brassard, 2005]. QKD also relies on techniques from classical information theory in order to correct the errors caused by eavesdropping or by imperfections in the setup. These techniques are referred to as *secret-key distillation*. The ciphering of the message using the key is classical as well. Although current classical encryption systems are nearly unbreakable, their security is not guaranteed forever. Conversely, the security of QKD is guaranteed by the laws of quantum mechanics. Another advantage of QKD respect to classical ways of encryption is that it allows to obtain long secret keys of the same length of the message to encrypt, fulfilling Shannon's condition for a secure coding of the message. Finally, it is important to remark that QKD is perfectly feasible with current technologies, such as commercial lasers and fiber optics.

Nonetheless, interest in the field truly arose with the reinvention of quantum key distribution by Artur Ekert in his paper of 1991 [Ekert, 1991]. In his article, he developed a new protocol based on quantum entanglement [Einstein et al., 1935] and the violation of Bell's theorem [Bell, 1964]. In this wise, the quantum channel shared between Alice and Bob is replaced by a common trusted source emitting entangled photons to both of them. The security of this protocol is based on the impossibility to classically reproduce measurement results on entangled quantum states. The use of quantum entanglement in QKD has proved to be very useful and led to many inventions and improvements like entanglement distillation [Bennett et al., 1996] and quantum privacy amplification [Deutsch et al., 1996].

More QKD protocols were developed over the years. To begin with, in 1992 Bennett refined the original protocol into a new one [Bennett, 1992], called B92, where the four quantum states original required were reduced to two non-orthogonal states. Furthermore, a six-state protocol has been proposed, which greatly reduces Eve's optimal information

gain compared to the BB84 [Bruß, 1998, Bechmann-Pasquinucci and Gisin, 1999]. It is also worth noting Kak's three-stage cryptography protocol [Kak, 2006], where both, Alice and Bob use random polarization rotations to encrypt information. The most interesting thing about this protocol is that it is not actually a QKD protocol, where the ciphering is classical, but instead represents a purely quantum-based cryptography. Anyway, all these protocols tend to use the polarization state of single photons to encode random bits, that is, they work with discrete variables (DC). In order to easily avoid the problem of generate perfect single-photon states, QKD protocols working with continuous variables have also been proposed, like it is the case of the *Gaussian modulated coherent state* (GMCS) protocol [Grosshans et al., 2003]. In this protocol, Alice modulates the amplitude quadrature and phase quadrature of a coherent state with Gaussian distributed random numbers and sends it to Bob, who measures one of the quadratures using homodyne detection. By studying the variance in one quadrature, they can guess the amount of information of the other quadrature gained by a possible eavesdropper and generate a secret key with the Gaussian variables.

The first experimental demonstration of QKD was conducted by Bennett and Brassard in 1989 [Bennett and Brassard, 1989, Bennett et al., 1992a]. The prototype was of about 30 cm. Years later, QKD over long distances in optical fibers was achieved for both, phase-coding [Townsend et al., 1993] and polarization-coding [Muller et al., 1993][3]. Long distances in free space were also achieved [Jacobs and Franson, 1996]. In 1995, Muller et al. carried the first QKD experiment on field, outside the lab, reaching distances over 23 km using polarization-coding [Muller et al., 1995, Muller et al., 1996]. Since them, longer and greater distances have been reached, even recently achieving satellite-to-ground QKD [Liao et al., 2017].

Along with the development of QKD protocols, the study of unconditional security proofs was born to provide their foundation, study their robustness against eavesdropping attacks, determinate the key generation rate of each protocol and even study the post-processing protocol to generate the key [Lo and Zhao, 2008]. Several years after the publication of the BB84 protocol, the first proofs of the unconditional security of QKD protocols were proposed with different approaches by Lo [Lo and Chau, 1999] and Mayers [Mayers, 2001]. A simpler proof of unconditional security was made by Shor and Preskill using entanglement distillation [Shor and Preskill, 2000]. Later, it was demonstrated that using high dimensional quantum states provides greater robustness to noise and a higher level of security in presence of an eavesdropper [Cerf et al., 2002]. The implementation of high dimensional quantum key distribution has become one of the most important areas of study within the field of quantum cryptography [Ding et al., 2017].

[3]Townsend reached distances of over 10 km, while Muller reached 1.1 km.

1.1.3 Realistic implementation of QKD and problems

Even if the above and other QKD protocols can be theoretically proven to be secure, this is always under the assumption of ideal conditions, where Eve has no other way of gaining information that directly eavesdrop the transmission. However, in practice, the devices employed by Alice and Bob (photon source and detectors), as well as the quantum channel (optical fibers or free space), are not ideal. The most basic differences between ideal and realistic devices are the following:

(a) Ideal photon sources always generate single-photon states. Meanwhile, in a realistic source, multi-photon states can also be produced.

(b) Realistic detectors can get detections when there is no actual incoming photon, phenomenon known as *dark counts*. Additionally, once they take a measurement, detectors have a blind time in which they can not detect and may lose incoming photons.

(c) The main problem with realistic communication channels is the noise. Noise can be produced due to birefringence propagation effects, interferences, temperature and pressure variations $\cdots$ and can cause decoherence of the single-photon states leading to errors.

These problems can significantly compromise the fidelity and the security of the protocol, as they can open new ways for Eve to gain information by devising new attacks (*side channel attacks*) that exploit the realistic defects of the devices. The vast majority of research into quantum cryptography today is focused on solving such problems, finding possible new attacks exploiting them and devising new methods against such attacks, in order to ensure security even in non-ideal conditions [Antoniades et al., 2004].

To begin with, in the technological aspect, emphasis has been placed in developing good single photon sources and high efficient detectors. To achieve the first, different generation methods have been proposed like attenuated coherent states [Ribordy, 2006], parametric down conversion [Takeuchi et al., 2004], photon emission of electron-hole pairs in a semiconductor quantum dot [Monat et al., 2006], etc. In the case of detectors, the most used techniques are photomultipliers, avalanche photo-diodes, multichannel plates and superconducting Josephson junctions [Teja et al., 2007]. Regarding transmission, single-mode optical fibers are preferred option, as multi-mode fibers can produce mixed states deteriorating the signal quality. However, if this drawback could be overcome somehow, multi-mode fibers can have great potential for QKD.

In the theoretical aspect, unconditional security proofs with imperfect devices have been studied by people like Gottesman [Gottesman et al., 2004]. In the new security studies, non-ideal effects like dark counts are taken into account to calculate the key rate. Nonetheless, these theoretical studies can not tell us how Eve can take advantage of the devices imperfections and, more importantly, how to protect against it.

And so forth, by taking advantage of the photon source defects (a), a new kind of side channel attack was developed by Huttner and others [Huttner et al., 1995, Yuen, 1996, Lütkenhaus, 2000, Lütkenhaus and Jahma, 2002]. In this attack, called the *photon number splitting* (PNS) attack, Eve could theoretically acquire a copy of the state by splitting the multi-photon state sent by Alice. Hence, Eve can theoretically obtain the full secret key. To solve this, Hwang proposed a new kind of protocol in 2003 [Hwang, 2003]. This method is known as the *decoy state protocol*, because it is based in introducing random fake states (decoys) between signal states (that carry the key bits) that can be used to detect such attack. The decoy-states protocol has been actively developed and implemented over the years [Ma et al., 2005, Curty et al., 2010, Tamaki et al., 2016]. This protocol will be explained in more detail later.

Regarding the photon detector problems (b), a completely new protocol that totally removes any possible side channel attack was proposed by Lo [Lo et al., 2012]. The so called *measure-device-independent* (MDI) protocol involves a third party (Charlie), who performs a Bell state measurement of the signal states sent by Alice and Bob. The entanglement of the measurements of Alice and Bob informs them if Charlie can be trusted. The MDI protocol has been experimentally demonstrated with success [Liu et al., 2013, Yin et al., 2016].

Now, what happens with noise problems in the transmission channel? Eve can not take much advantage of transmission noise to threaten the security. However, noise is still a great problem as it can cause decoherence of single-photon states causing errors and raising the error rate. This would make QKD useless if Alice and Bob were not able to distinguish the origin of the errors. To solve this, Alice and Bob have to measure first the error rate of the channel and thus, they are able to detect Eve through statistical deviations from it. After that, they performs some techniques to correct the errors and to reduce Eve's information down to zero at the cost of reducing their secret key. This processes are known as *error correction* and *privacy amplification* [Bennett et al., 1988, Bennett et al., 1995].

Even if these classical techniques can help to correct errors caused by the noise during transmission, this noise is still a problem that needs to be solved. For this reason, different methods have been proposed to correct transmission fluctuations. For example, Ribordy proposed the implementation of an active feedback control system to make constant measurements of the perturbations and compensate them accordingly, [Ribordy et al., 2000]. However, a more interesting approach was independently developed by Muller [Muller et al., 1997] and Bethune [Bethune and Risk, 2000]. Their idea consists of implementing an autocompensated system or *plug and play* system, that is, a system that naturally compensates perturbations in it. For that they proposed a round-trip system between Alice and Bob: Bob generates the original states and sends them to Alice, who encodes information in them and sends them back to Bob. Birefringence in optical fibers is the main source of noise in polarization-encoding QKD. By using a Faraday mirror, it is possible to compensate all birefringence perturbations caused in the first trip during the back trip [Martinelli, 1989]. The first experiment of autocompensated QKD was made by

Zbinden et al. in 1997 [Zbinden et al., 1997]. Later, Stucki et al. implemented another plug and play system over 67 km of fiber in 2002 [Stucki et al., 2002]. In 2009, Gisin patented a method to synchronize the emitter and the receiver in a plug and play system, while Zavriyev was also patenting a two way QKD system based in active compensation [Zavriyev et al., 2009]. Another autocompensation QKD system using homodyne detection has also been proposed by Xu [Xu et al., 2008]. More recently, an experimental implementation of a plug and play system between six users has been realized [Donkor, 2012]. Other interesting results in the area are the study of synchronization algorithms between the transmitter and receiver in a bidirectional autocompensation QKD system. New autocompensating schemes are still being designed [Duplinskiy et al., 2019].

Nonetheless, further advances in the area were slowed by the preference of using technologies like polarization-maintaining fibers to reduce noise. Interestingly, autocompensation has only been applied for the implementation of protocols like BB84 in two dimensions. But autocompensation can also be extended to high dimension (HD) QKD.

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

1.2 Aims and structure

1.2.1 Aims

As we have seen, quantum cryptography represents the most feasible application of all quantum technologies and it is, as well, the most closely to be widely implemented. For this reason, the overall objective of this thesis is to contribute to the development of discrete and integrated photonic devices in order to implement specific operations for optical communications, and in particular for optical cryptography by using polarization and spatial modes of optical fibers.

In the technological aspect, quantum cryptography relies almost completely on the burgeoning field of quantum optics, as well as integrated and fiber optics. The fundamental study of different states of light, like squeezed states or vortex states, can lead to more robust quantum states. Continuing the previous studies of our group in quantum optics, one of the aims of the thesis is to realize a theoretical analysis and characterization of specific single-photon and multi-photon quantum states excited in polarization or spatial modes, particularly vortex modes or linear combination of vortex modes. Additionally, our aim is the designing of devices for generating such states for possible applications in optical communications and other quantum information technologies. For instance, in quantum cryptography it is essential the use of single-photon sources. Thus, it is of our interest to design such a source based on vortex states.

Moreover, single-photon qudits excited in spatial modes, as those that are transmitted in few-modes optical fibers, constitute a natural way to generalize the BB84 protocol for higher dimensions, improving its security and transmission rate. However, the use of a high number of spatial modes makes them more vulnerable to noise during transmission, due to phase shifts and lags between them, modal coupling and polarization birefringence. This compromises the security of the system because it increments the error rate, making it necessary to correct this noise. Therefore, one of the main aims of this thesis is to design new autocompensating systems able to perform high dimensional quantum key distribution (HD-QKD) in different ways, including the design of the required devices. We are going to introduce different strategies to implement autocompensating HD-QKD based in the use of both few-mode and multicore optical fibers along with discrete and integrated devices respectively.

Finally, one last objective of this thesis consists of manufacturing previously designed integrated devices employing our group's technology and characterise them. In particular, we are interested in the development of quantum integrated projectors that are used to measure quantum states in spatial path modes and basically consist of directional couplers. In our lab, we count with lithographic and ion exchange technology to obtain waveguides in glass. Our aim is to prove the feasibility of this technology to manufacture directional couplers, and thus, any integrated device.

In brief, the main aims can be summed up as follow:

- Study of light squeezed quantum vortex states and design of devices for their generation.
- Development of autocompensating systems to implement HD-QKD.
- Manufacture of integrated devices through lithography techniques and their characterization.

1.2.2 Methodology

The methodology we have used to accomplish the previous aims is the following:

(A) Literature review of the state of the matter and theoretical study of quantum states of light in polarization and spatial modes. This study will allow us to recognize the optical elements required to implement different transformations of quantum states, and thus allow us to design new devices of different purpose.

(B) We will employ the optical elemets studied to design devices for the generation of different quantum states, like vortex states, that can be employed in QKD and others areas of QIP. Quantum simulations of the generated quantum states obtained in different representations will be done, especially one of optical field states, for the purpose of analysing and validating the operation of the devices. Then, the generators will be particularized for generating single-photon qubits for HD-QKD.

(C) Generalization of autocompensating systems to perform HD-QKD. High dimension can be achieved through phase encoding by employing collinear modes of a few-mode fiber (FMF) or codirectional ones in multicore fibers (MCF). To get autocompensation, we examine two new approaches based in two-way communication. Additionally, we will design discrete (for FMF spatial modes) and integrated (for MCF modes) photonic devices for generation and measure of quantum states in the proposed autocompensation systems. Moreover, a security analysis of our proposed system will be made, reviewing different side channels attacks to which our system can be subjected to and study of their behaviour in our HD system.

(D) Manufacture of integrated photonic devices by ion exchange in glass. The optical elements manufactured constitute the basic units of the devices, essentially directional couplers. With regard to manufacturing, first, lithographic techniques will be developed to obtain masks that allow selective ion exchange and give it to the manufacture of directional couplers. Then, the ion exchange process will be characterized to determine the optimal parameters of fabrication. Finally, an optical near-classical characterization with laser of these elements will be made.

1.2.3 Thesis outline

This dissertation is organized in four chapters. Every chapter is dedicated to the study of a particular question in general way. Moreover, published and submitted papers of our group, that explain the details, examples and principal results of our research in each question, are added as sections in the chapters.

In this way, in chapter 2 we first present the quantum background explaining the unitary quantum transformations of the main optical elements that are used in the design of the different devices. Then, we shown a general theoretical study of quantum states and present different discrete devices for their generation. Moreover, two published papers are added, explaining the design of integrated devices for the generation of these states and analysing them. Finally, we explain how our proposed integrated devices can be used to generate qubit states necessary for implementing the BB84 protocol in high dimension.

Chapter 3 is devoted to the design and analysis of autocompensation systems for HD-QKD by using phase encoding employing the spatial modes of a FMF. First, a detailed explanation of the BB84 protocol and the different problems presented during transmission for its correct implementation is done, explaining as well, the autocompensation methods already proposed for the two-dimensional case. Then, we propose our generalization of an autocompensating system for performing the BB84 protocol in high dimension explaining the different details that such a system must fulfil. Afterwards, a general overview of the main results of security studies for practical implementation of HD-QKD is made, followed by a security analysis of our system under a side channel attack which is specific to plug and play systems like ours. Finally, our first published paper about an autocompensation system in four dimensions is presented.

Chapter 4 is dedicated to the manufacturing of integrated devices to perform quantum projections in order to measure vortex states used in our cryptographic system. On this wise, first we introduce the operation of these devices theoretically. Next, we present and explain the different steps of our fabrication process: the characterization of our ion exchange process, the design of devices to manufacture according to the characterized parameters, the set up of a photo-lithographic system to create metallic masks for ion exchange and the final touches of cutting and polishing the samples. At last, we present the characterization of our devices by through different means: using a four-step phase shifting algorithm and through coherent light.

Finally, in chapter 5, we explain two additional and improved ways of implementing our autocompensation QKD by taking advantage of multicore fibers and phase conjugation process. The chapter consists of a general introduction of both methods followed by our published and submitted works on each of them.

1.3 Works by author

1.3.1 List of Publications

The following list indicates the publications derived from this research that were used to create this thesis. The accepted manuscript of the papers are included in it at the end of the specific chapters as an added section. I declare that I am properly authorized to use these articles in this thesis, as specified in the footnotes.

- Barral, D., Liñares, J., and Balado, D. (2016). Engineering continuous and discrete variable quantum vortex states by nonlocal photon subtraction in a reconfigurable photonic chip. *JOSA B*, 33(11):2225–2235, JIF: 2.180, Q2 Optics (Chapter 2) [4]

  ✓ Contribution: collaboration in the design of a reconfigurable integrated vortex states generator device, which can be used for quantum information processing including quantum cryptography.

- Barral, D., Balado, D., and Liñares, J. (2017). Generation and detection of continuous variable quantum vortex states via compact photonic devices. *Photonics*, 4(1):2, JIF: 2.140, Q2 Optics (Chapter 2) [5]

  ✓ Contribution: collaboration in the design of a non-reconfigurable integrated vortex states generator device, which can be used for quantum information processing including quantum cryptography.

- Balado Souto, D., Liñares, J., and Prieto-Blanco, X. (2019). Phase auto-compensating high-dimensional quantum cryptography in elliptical-core few-mode fibres. *Journal of Modern Optics*, 66(9):947–957, JIF: 1.544, Q3 Optics (Chapter 3) [6]

  ✓ Contribution: collaboration in the design of an autocompensating QKD system in four dimensions with discrete devices in few-mode fibers and security analysis.

[4] Published by OSA Publishing. According to the *OSA Copyright Transfer Agreement*, the accepted manuscript is allowed for "Reproduction by authors in a compilation or for teaching purposes short term", as can be consulted in `https://www.osapublishing.org/submit/review/copyright_permissions.cfm` .

[5] Published by MDPI. As an open access journal, the articles are distributed under the *Creative Commons Attribution License*, "which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited", as can be consulted in `https://www.mdpi.com/openaccess` .

[6] Published by Taylor & Francis Group. The sharing policy of the journal allows to post the accepted manuscript in an institutional repository after 12 months of embargo already expired, as can be consulted in `https://authorservices.taylorandfrancis.com/research-impact/sharing-versions-of-journal-articles/` .

- Balado, D., Liñares, J., Prieto-Blanco, X., and Barral, D. (2019). Phase and polarization autocompensating *N*-dimensional quantum cryptography in multicore optical fibers. *JOSA B*, 36(10):2793–2803, JIF: 2.180, Q2 Optics (Chapter 5) [4]

  ✓ Contribution: collaboration in the design of a high dimension autocompensating QKD system with integrated devices in multi-core fibres and security analysis.

- Liñares, J., Prieto-Blanco, X., Balado, D., and Carral, G. M. (2020). Fully autocompensating high-dimensional quantum cryptography by optical phase conjugation. *ArXiv preprint arXiv:2009.13915*, (preprint) (Chapter 5)

  ✓ Contribution: collaboration in the demonstration of autocompensation by phase conjugation with spatial and polarization modes.

1.3.2 Conference works

The following list collects the conferences where the results of our research related to this thesis were presented during these years.

- Balado Souto, D., Liñares Beiras, J., Montero Orille, C., Moreno de las Cuevas, V., Moure Cerijo, D., Nistal Fernández, M. C., and Prieto Blanco, X. (2016). Generación de modos LP con placas de fase producidas por intercambio iónico en vidrio. In *XXXI Simposium Nacional de la Unión Cinetífica Internacional de Radio (URSI 2016)*, Madrid. Escuela Politécnica Superior Universidad Autónoma de Madrid

- Balado, D., Prieto-Blanco, X., and Liñares, J. (2017). Spatial mode quantum cryptography in few-mode optical fibers. In *X Reunión Española de Optoelectrónica (OPTOEL 2017)*, Santiago de Compostela

- Balado, D., Prieto-Blanco, X., Barral, D., and Liñares, J. (2018). Autocompensating high-dimensional quantum cryptography by using integrated photonic devices in multicore optical fiber spatial multiplexing systems. In *International Conference on Integrated Quantum Photonics (ICIQP 2018)*, volume 75

- Liñares-Beiras, J., Prieto-Blanco, X., Balado, D., and Carral, G. M. (2020). Autocompensating high-dimensional quantum cryptography by phase conjugation in optical fibers. In *EPJ Web of Conferences*, volume 238, page 11004. EDP Sciences

2

Quantum States And Devices For Quantum Cryptography

The main objective of this chapter is to introduce and analyse basic aspects of quantum states and devices that can be employed to perform quantum cryptography (QC), as well as employ such devices and states in order to design quantum state generators for QC.

Quantum key distribution (QKD) can be implemented in many ways. For instance the quantum states employed can be excited in polarization modes, in spatial modes or even in different paths. Depending on the way used to implement QKD, the designed systems must employ different kind of devices to perform various operations. In this way, one of the purposes of this chapter is to present the basic quantum formalism of different optic devices that we are going to use throughout this thesis to perform QKD in the different ways.

Another objective of this chapter is the study of a kind of quantum states called quantum vortex states (QVS). These states have great potential for being employed in QC and other quantum information processing (QIP) fields. For instance, squeezed vortex states could be used to implement continuous variable QKD (CV-QKD). In the meantime, single-photon quantum vortex states can also be employed to perform discrete variable QKD (DV-QKD). In fact, the order of the vortexes, which may carry physical meaning according to the used modes, constitutes a natural Hilbert space to implement high dimension QKD (HD-QKD). Besides, these states form an orthonormal base that become the seed to obtain mutually unbiased basis, which are required to implement QKD protocols like the BB84.

The chapter's main interest resides in the design of quantum states generators for QC. The generation of single-photon states is crucial for DV-QKD and other applications of QIP. Protocols like the BB84 require the use of single-photons to be implemented. Not only does the protocol work by considering the mechanical properties of a single photon state, but the use of single photon generators also prevents any possible extraction of information through attacks to get additional photons that could be generated. Moreover, in BB84, single-photon states must be randomly encoded. Most times, this is

done in an active way in the generator, like for example modulating a phase shifter, with pseudo-random algorithms being implemented in the active components. However, these components may be a weakness that can be exploited by an eavesdropper, who could attack them an gain information of the coded state. Therefore, it becomes of special interest to develop passive generators to produce coded states in a fully random way. In this chapter, we include two of our works [Barral et al., 2016,Barral et al., 2017], where we propose two integrated devices for the generation of quantum states, like the previously mentioned quantum vortex states, that can be employed for QKD or other applications.

The structure of this chapter is as follows. First, in section 2.1 we introduce the quantization formalism of light propagation (subsec. 2.1.1) as well as the original basic ways of obtaining single-photon quantum states to be used in discrete variable QIP (DV-QIP). These include the utilization of weak coherent sources with phase randomization (subsec. 2.1.2), and the employment of spontaneous parametric down conversion (SPDC) (subsec. 2.1.3). Next, section 2.2 introduces the quantum formalism of the main optical devices used in this thesis and our published works. These devices consists of both bulk devices for polarization (subsection 2.2.1) and spatial (subsection 2.2.3) modes and integrated devices (subsection 2.2.2). Afterwards, section 2.3 is dedicated to an original study of quantum vortices. In particular, we analyze their physical meaning in terms of their relationship to angular momentum 2.3.1 and ways of generating them in both bulk (subsections 2.3.2 and integrated (subsection 2.3.3) devices. The latter is expanded on our annexed works [Barral et al., 2017] and [Barral et al., 2016] shown in sections P1 and P2 respectively. Both works make use of spontaneous parametric down conversion and integrated directional couplers for the generation of single and multi-photon vortex states. Finally, we explain how we can make use of our designed generators for implementing the BB84 protocol in section 2.4. We introduce the concept of mutually unbiased basis (subsec. 2.4.1) and show how our devices can generate 2-dimensional quantum states for QKD in a random way (subsec. 2.4.2). Moreover, a way of expand this integrated 2-dimensional quantum states to more dimensions and generate mutually unbiased basis is shown in subsection 2.4.3.

2.1 Quantum light and devices for quantum cryptography

In quantum cryptography, the development of single-photon sources and detectors is of the utmost importance. In Quantum Key Distribution (QKD), a message encoded in one degree of freedom of a photon can not be cloned by an eavesdropper without introducing errors.

In this section, we are going to introduce processes for generation of single-photon states after introducing the quantum formalism that describes light propagation.

2.1.1 Quantization of light spatial propagation

The linear momentum of light describes its spatial movement. Thus, it is the quantum magnitude that can describe the quantum spatial propagation of light along direction z. The volume density of linear momentum corresponds to a flux density if $z = ct$, that it is given by the component T^{33} of the Energy-Momentum Maxwell tensor. Therefore, the expression of the Momentum quantum operator is going to be given by the integration of the flux density T^{33} over the cross-section $dxdy$ during a time dt, as explained in [Ben-Aryeh and Serulnik, 1991],

$$\hat{M} = \int\int\int T^{33}(\hat{\boldsymbol{\mathcal{E}}}, \hat{\boldsymbol{\mathcal{H}}}) dx dy c dt, \tag{2.1.1}$$

where the tensor component is written as

$$T^{33}(\hat{\boldsymbol{\mathcal{E}}}, \hat{\boldsymbol{\mathcal{H}}}) = \frac{1}{2}\left[\left(\epsilon_0 n^2(x,y)\hat{\boldsymbol{\mathcal{E}}}_t\hat{\boldsymbol{\mathcal{E}}}_t - \mu_0\hat{\mathcal{H}}_z^2\right) + \left(\mu_0\hat{\boldsymbol{\mathcal{H}}}_t\hat{\boldsymbol{\mathcal{H}}}_t - \epsilon_0 n^2(x,y)\hat{\mathcal{E}}_z^2\right)\right]. \tag{2.1.2}$$

Operators $\hat{\boldsymbol{\mathcal{E}}}$ and $\hat{\boldsymbol{\mathcal{H}}}$ represent the optical field quantum operators, while t and z represent the transversal and propagation components respectively. The propagation medium is characterized by a canonical index profile $n^2(x,y)$. Now, in case that ν modes are propagating across the medium, the total field operators $\hat{\boldsymbol{\mathcal{E}}}, \hat{\boldsymbol{\mathcal{H}}}$ are the superposition of the field operators of each mode, as shown

$$\hat{\boldsymbol{\mathcal{E}}} = \sum_\nu \hat{\boldsymbol{\mathcal{E}}}_\nu = \frac{1}{2}\sum_\nu \left(\hat{\boldsymbol{\mathcal{E}}}_\nu^{(+)} + \hat{\boldsymbol{\mathcal{E}}}_\nu^{(-)}\right), \tag{2.1.3a}$$

$$\hat{\boldsymbol{\mathcal{H}}} = \sum_\nu \hat{\boldsymbol{\mathcal{H}}}_\nu = \frac{1}{2}\sum_\nu \left(\hat{\boldsymbol{\mathcal{H}}}_\nu^{(+)} + \hat{\boldsymbol{\mathcal{H}}}_\nu^{(-)}\right), \tag{2.1.3b}$$

where we have taken into account that each field operator is the semi sum of the positive and negative operators, that may be written in function of the absorption and emission operators as follows

$$\hat{\boldsymbol{\mathcal{E}}}_\nu^{(+)} = \sqrt{\frac{\hbar\omega}{cT}}\,\hat{a}_\nu\,\hat{\boldsymbol{e}}\,e^{-i\omega t}, \quad \hat{\boldsymbol{\mathcal{E}}}_\nu^{(-)} = \left(\hat{\boldsymbol{\mathcal{E}}}_\nu^{(+)}\right)^\dagger \tag{2.1.4a}$$

$$\hat{\boldsymbol{\mathcal{H}}}_{\nu}^{(+)} = \sqrt{\frac{\hbar\omega}{cT}}\,\hat{a}_{\nu}\,\hat{\boldsymbol{h}}\,e^{-i\omega t}, \quad \hat{\boldsymbol{\mathcal{H}}}_{\nu}^{(-)} = \left(\hat{\boldsymbol{\mathcal{H}}}_{\nu}^{(+)}\right)^{\dagger} \tag{2.1.4b}$$

In case we consider modes propagating without interaction in a medium of index n, then we can introduce equations (2.1.3) and (2.1.4) into the tensor component (2.1.2) and make the integrations on both time and the cross section to obtain the Momentum operator (2.1.1) without modal coupling [Liñares and Nistal, 2003, Liñares et al., 2008]

$$\hat{M}_0 = \hbar \sum_{\nu} \beta_{\nu} \hat{a}_{\nu}^{\dagger} \hat{a}_{\nu}, \tag{2.1.5}$$

where β_{ν} represents the propagation constant of mode ν. $\hat{a}$ and $\hat{a}^{\dagger}$ are the photon absorption and emission operators

$$\begin{aligned} \hat{a}\,|n\rangle &= \sqrt{n}\,|n-1\rangle\,, \\ \hat{a}^{\dagger}\,|n\rangle &= \sqrt{n+1}\,|n+1\rangle\,, \end{aligned} \tag{2.1.6}$$

where $|n\rangle$ are the Fock states with n the number of photons. These states are the eigenvectors of operator $\hat{a}_{\nu}^{\dagger}\hat{a}_{\nu}$ and, therefore, they constitute eigenvectors of the free momentum operator (2.1.5) too.

However, we have to take into account that modal coupling can occur, this is, energy exchange between different modes. In order to formalize this, we can assume that several decoupled modes are coupled because of a perturbation that modifies the index of the medium as $n^2(x,y) = n^2 + \Delta n^2$. Thus, the momentum operator (2.1.1) becomes

$$\hat{M} = \hat{M}_0 + \hat{M}_p, \tag{2.1.7}$$

where $\hat{M}_0$ corresponds to the unperturbed case (2.1.5) and the perturbed term is given by

$$\hat{M}_p = \frac{1}{2} \int\int\int \epsilon_0 \Delta n^2 \left(\hat{\boldsymbol{\mathcal{E}}}_t \hat{\boldsymbol{\mathcal{E}}}_t - \hat{\mathcal{E}}_z^2 \right) dxdycdt. \tag{2.1.8}$$

Integrating over time and the spatial cross-section, we have

$$\hat{M}_p = \hbar \sum_{\nu} \sum_{\nu'} \kappa_{\nu,\nu'} \hat{a}_{\nu}^{\dagger} \hat{a}_{\nu'}. \tag{2.1.9}$$

By summing terms (2.1.5) and (2.1.8), we obtain the explicit form of the linear part of the Momentum operator [Liñares and Nistal, 2003, Liñares et al., 2008]

$$\hat{M} = \hat{M}_0 + \hat{M}_p = \hbar \sum_{\nu} \tilde{\beta}_{\nu} \hat{a}_{\nu}^{\dagger} \hat{a}_{\nu} + \hbar \sum_{\nu'} \sum_{\substack{\nu \\ \nu<\nu'}} \kappa_{\nu,\nu'} \left(\hat{a}_{\nu}^{\dagger} \hat{a}_{\nu'} + \hat{a}_{\nu} \hat{a}_{\nu'}^{\dagger} \right), \tag{2.1.10}$$

where $\tilde{\beta}_{\nu}$ are the propagation constants of the modes corrected by self-coupling coefficients and $\kappa_{\nu,\nu'}$ represent the cross-coupling coefficients. This Momentum operator has a general expression and can be used to analyse several multimode optical systems.

Therefore, the Momentum operator (2.1.10) can be used for the obtention of Heisenberg's equations of propagation for a general operator $\hat{\mathbb{O}}$

$$\frac{d\hat{\mathbb{O}}}{dz} = \frac{i}{\hbar}\left[\hat{\mathbb{O}}, \hat{M}\right]. \tag{2.1.11}$$

As a consequence, Heisenberg's propagation equations (2.1.11) give us a way to study the propagation of quantum light in different optical systems by analysing how an operator is propagated. Considering operator $\hat{\mathbb{O}} = \hat{a}$, Heisenberg's equations become

$$-i\frac{d\hat{a}_\nu}{dz} = \tilde{\beta}_\nu \hat{a}_\nu + \sum_{\substack{\nu' \\ \nu' \neq \nu}} \kappa_{\nu,\nu'} \hat{a}_{\nu'}, \tag{2.1.12}$$

which are the fundamental equations for opto-quantum transformations. These equations can be used to describe most optical systems, not only couplers, but also waveplates or beam splitters.

The rigorous quantization analysis of the propagation of coupled modes in integrated optical waveguides was presented by our group for two dimensional [Liñares and Nistal, 2003] and one dimensional waveguides [Liñares et al., 2008], either for linear and non-lineal devices [Liñares et al., 2012].

Now, the propagation of a generic state $|L_0\rangle$ through a device is given by an operator $\hat{U}$, which is an exponential operator of the Momentum operator, as follows

$$|L\rangle = \hat{U}\,|L_0\rangle = e^{\frac{i\theta}{\hbar}\hat{M}}\,|L_0\rangle\,, \tag{2.1.13}$$

where operator $\hat{U}$ fulfils

$$\hat{a}(\theta) = \hat{U}^\dagger \hat{a}(0)\hat{U}. \tag{2.1.14}$$

This quantum light propagation formalism allows us to obtain the quantum behaviour of several devices, as we will see in this and next section. In this one, we will focus in describing the basic forms of single-photon states generation.

2.1.2 Weak coherent state source

The Fock states $|n\rangle$ are the eigenstates of the free momentum operator (2.1.5) and represent quantum states of n photons propagating freely. However, their generation is not trivial.

Until the emergence of quantum optics, the most used way to implement an imperfect single photon source is to employ highly attenuated lasers [Scully and Suhail, 1997]. These kind of sources emit weak coherent states $|\alpha\rangle$, first introduced by [Glauber, 1963b], which are solution to the quantum harmonic oscillator. These states are eigenstates of the absorption operator $\hat{a}$ ($\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$) and consists of a superposition of Fock states

$$|\alpha\rangle = e^{\alpha\hat{a}^\dagger - \alpha^\dagger \hat{a}}\,|0\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle, \tag{2.1.15}$$

where $\alpha = |\alpha|e^{i\epsilon}$, being ϵ the phase of the coherent pulse and $\mu = |\alpha|^2$ the intensity of said pulse. Operator $D(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^\dagger\hat{a}}$ is called the displacement operator, as it displaces a localized state in phase space by α, turning a vacuum state into a coherent one.

In order to generate Fock states of few photons, the laser must be attenuated and its phase randomized [Ma, 2008]. In such manner, if a phase randomization is implemented to each pulse of the laser, then, the density matrix of state (2.1.15) is

$$\rho = \frac{1}{2\pi}\int_0^{2\pi} d\epsilon\, ||\alpha|e^{i\epsilon}\rangle\langle|\alpha|e^{i\epsilon}| \tag{2.1.16}$$

$$= \frac{1}{2\pi}\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\frac{|\alpha|^{n+m}}{\sqrt{n!\,m!}}e^{-\frac{|\alpha|^2}{2}}|n\rangle\langle m|\int_0^{2\pi} d\epsilon\, e^{i(n-m)\epsilon} \tag{2.1.17}$$

$$= \sum_{n=0}^{\infty} P_n(\mu)\,|n\rangle\langle n|. \tag{2.1.18}$$

Thus, we observe that, after phase randomization, state (2.1.15) has been reduced to a Poissonian state, that is, a mixture of Fock states with a Poisson distribution given by

$$P_n = e^{-\mu}\frac{\mu^n}{n!}. \tag{2.1.19}$$

Therefore, the source generates state $|n\rangle$ with probability P_n. The weaker the intensity μ of the source is, the higher the probability of obtaining a single-photon state $|1\rangle$ (and vacuum state $|0\rangle$) with respect to obtaining a multi-photon state $|n\rangle$, $n > 1$. However, such attenuated "single-photon sources" have the problem that the probability of generating a vacuum state is much higher than the probability of generating a single photon. At the same time, the generation of multi-photon states make a QKD system vulnerable to certain attacks like the photon number splitting attack that will be explained latter.

2.1.3 Generation of biphoton states with SPDC

Another way of generate quantum states to implement quantum cryptography is to employ spontaneous parametric down conversion (SPDC). SPDC is a non linear optical process that occurs when a pump beam arrives to a non linear crystal and it is split into two beams in accordance with the law of conservation of energy and the law of conservation of momentum [Klyshko et al., 1970, Burnham and Weinberg, 1970]. Thus, SPDC transforms a photon of high energy into a pair of two photons of lower energy.

In these non linear crystals, the coupling is efficient between modes of the same polarization. The total linear Momentum operator taking into account this interaction is

$$\hat{M} = \hat{M}_0 + \hat{M}_I = \hat{M}_0 + \frac{1}{2}\int \hat{P}(\hat{\boldsymbol{E}})\hat{\boldsymbol{E}}dxdycdt, \tag{2.1.20}$$

where $\hat{M}_0$ is the free Momentum operator (2.1.5) and $\hat{M}_I$ corresponds to the interaction operator. $\hat{P}(\hat{\boldsymbol{E}})$ is the polarization operator of the non linear medium and represents

the interaction or modal coupling. Supposing a non linearity of the second order, this operator has the form

$$\hat{P}(\hat{\boldsymbol{E}}) = \epsilon_0 \chi^2 \hat{\boldsymbol{E}} \hat{\boldsymbol{E}}. \tag{2.1.21}$$

Depending on whether polarization is taken into account in the process, there are two different types of SPDC, as we will see bellow.

2.1.3.1 SPDC Type I

Now, let us consider the SPDC conversion of a pump photon into a pair of photons (signal and idler). Trivially, the laws of conservation of energy and momentum imply

$$\begin{aligned} \omega_p &= \omega_s + \omega_i, \\ \boldsymbol{k}_p &= \boldsymbol{k}_s + \boldsymbol{k}_i. \end{aligned} \tag{2.1.22}$$

Modes s and i refer to the signal and idler, respectively, and have the same polarization, while the pump (p) has orthogonal polarization with respect to them. This kind of condition happens in anisotropic non linear crystals of second order like the KDP or BBO [Ganeev et al., 2004, Eimerl, 1987, Nikogosyan, 1991]. To obtain the Momentum operator, we have to employ the three modes of different frequencies as in equation (2.1.3a), where $\hat{E}_b$ is phase shifted $\pi/2$ by formal reasons. So the Momentum operator that describes the interaction is, according to [Liñares et al., 2012],

$$\begin{aligned} \hat{M}_I &= \frac{1}{2} \int \epsilon_0 \chi^2 \left(\hat{E}_s + \hat{E}_i + \hat{E}_p \right)^3 dxdycdt \\ &= \frac{\epsilon_0 \chi^2}{16} \int \left(\hat{E}_s^{(+)} + \hat{E}_s^{(-)} + \hat{E}_i^{(+)} + \hat{E}_i^{(-)} - i\hat{E}_p^{(+)} + i\hat{E}_p^{(-)} \right)^3 dxdycdt, \end{aligned} \tag{2.1.23}$$

where we have expressed the optical field operators of the modes in complex notation as in (2.1.3a). Ignoring the terms of the temporal integral that are going to become null we have

$$\hat{M}_I = i \frac{\epsilon_0 \chi^2}{8} \int \left(\hat{E}_s^{(+)} \hat{E}_i^{(+)} \hat{E}_b^{(-)} - \hat{E}_s^{(-)} \hat{E}_i^{(-)} \hat{E}_b^{(+)} \right) dxdycdt. \tag{2.1.24}$$

So, the total Momentum operator (2.1.20) is going to be

$$\hat{M} = \hbar k_s \hat{a}_s^\dagger \hat{a}_s + \hbar k_i \hat{a}_i^\dagger \hat{a}_s + i\hbar\xi' \left(\hat{a}_s \hat{a}_i \hat{a}_b^\dagger - \hat{a}_s^\dagger \hat{a}_i^\dagger \hat{a}_b \right). \tag{2.1.25}$$

Finally, considering that the pump is a coherent state and grouping terms, we obtain the final expression of the Momentum operator for SPDC of type I (signal and idler of identical polarization)

$$\hat{M}_I = -i\hbar \left(\xi \hat{a}_s^\dagger \hat{a}_i^\dagger - \xi^* \hat{a}_s \hat{a}_i \right), \tag{2.1.26}$$

where the free momentum has been ignored. The propagator operator of the SPDC of type I is then

$$\hat{S}_I = e^{\frac{i}{\hbar}\hat{M}_I} = e^{\xi \hat{a}_s^\dagger \hat{a}_i^\dagger - \xi^* \hat{a}_s \hat{a}_i}. \tag{2.1.27}$$

Applying this operator to the vacuum we obtain our generated state through this process

$$e^{\frac{i}{\hbar}\hat{M}_I}\left|0_s0_i\right\rangle = \left|0_s0_i\right\rangle + \xi\left|1_s1_i\right\rangle + \cdots \tag{2.1.28}$$

2.1.3.2 SPDC Type II

It is also possible to generate signal and idler photons with orthogonal polarization between them, with the polarization of the pump parallel to one of the formers. This is the SPDC of type II. So, now we must take into account the polarization components when calculating the interaction Momentum operator as

$$\hat{M}_I = \frac{1}{2}\int \epsilon_0\chi^2\left(\hat{E}_{1H} + \hat{E}_{2H} + \hat{E}_{1V} + \hat{E}_{2V} + \hat{E}_p\right)^3 dxdycdt. \tag{2.1.29}$$

Proceeding the same way as before, we can obtain the final expression for the interaction Momentum operator

$$\hat{M}_I = -i\hbar\left(\xi\hat{a}^\dagger_{1H}\hat{a}^\dagger_{2V} + \xi\hat{a}^\dagger_{1V}\hat{a}^\dagger_{2H} - \xi^*\hat{a}_{1H}\hat{a}_{2V} - \xi^*\hat{a}_{1V}\hat{a}_{2H}\right), \tag{2.1.30}$$

where the free momentum has been ignored. The propagator operator of the SPDC of type II is then

$$\hat{S}_I = e^{\frac{i}{\hbar}\hat{M}_I} = e^{\xi\hat{a}^\dagger_{1H}\hat{a}^\dagger_{2V} - \xi^*\hat{a}_{1H}\hat{a}_{2V}}e^{\xi\hat{a}^\dagger_{1V}\hat{a}^\dagger_{2H} - \xi^*\hat{a}_{1V}\hat{a}_{2H}}. \tag{2.1.31}$$

Now, using again the propagator into the vacuum to obtain the generated state we have

$$e^{\frac{i}{\hbar}\hat{M}_I}\left|00\right\rangle = \left|00\right\rangle + \xi\left(\left|1_H1_V\right\rangle + \left|1_V1_H\right\rangle\right) + \cdots \tag{2.1.32}$$

The solution at first order is one of Bell quantum states. By making use of waveplates, it is possible to obtain any of the four Bell states, which are given by

$$\left|\Psi^\pm\right\rangle = \frac{1}{\sqrt{2}}\left(\left|1_{1H}\right\rangle\left|1\right\rangle_{2V} \pm \left|1_{1V}\right\rangle\left|1\right\rangle_{2H}\right), \tag{2.1.33a}$$

$$\left|\Phi^\pm\right\rangle = \frac{1}{\sqrt{2}}\left(\left|1_{1H}\right\rangle\left|1\right\rangle_{2H} \pm \left|1_{1V}\right\rangle\left|1\right\rangle_{2V}\right). \tag{2.1.33b}$$

These states are of great important in many of quantum applications, like quantum computing or quantum teleportation. But they also are of great use in quantum cryptography. For instance, Bell states are the basis to implement the Ekert protocol [Ekert, 1991] as well as the MDI protocol [Lo et al., 2012].

2.2 Bulk and integrated devices for QC

In this section, we are going to introduce the quantum formalism of the different devices that are employed in this and further chapters in order to work with different types of modes, like polarization, integrated or spatial modes. In many cases, according to the *correspondence principle*, the quantum operator transformations (solutions to Heisenberg's equations) corresponds to the classical field transformations [Gerry et al., 2005].

To begin with, taking into account the quantum field operators (2.1.4a) and the correspondence with classical optics, a basic optical element like a beam splitter (BS), can be quantized as [Fearn and Loudon, 1987]

$$\begin{aligned} \hat{a}_t &= T^{1/2}\hat{a}_{i1} - R^{1/2}\hat{a}_{i2}, \\ \hat{a}_r &= R^{1/2}\hat{a}_{i1} + T^{1/2}\hat{a}_{i2}, \end{aligned} \tag{2.2.34}$$

where modes t and r refer to the transmitted and reflected modes, $i1$ and $i2$ make reference to the incident ones and T and R are the transmission and reflection coefficients, which can be expressed as $\sqrt{T} = \cos\omega$ and $\sqrt{R} = \sin\omega$. These transformations can also be obtained from equations (2.1.12). For the simple case of a 50/50 beam splitter the transformation matrix of operators can be written as

$$B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}. \tag{2.2.35}$$

The propagator operator (2.1.13) of the general BS can be written as

$$\hat{B} = \exp\left\{ \frac{\theta}{2} \left(a_t^\dagger a_r - a_t a_r^\dagger \right) \right\}, \tag{2.2.36}$$

where $\theta = \frac{\pi}{2}$ for the case (2.2.35)

2.2.1 Devices for QC with polarization modes

2.2.1.1 Polarization beam splitter

A regular BS would act the same way over both polarization modes, but introducing a phase shift π. A polarization beam splitter (PBS) is a BS that acts in a different way for each polarization mode. They can be implemented by anisotropic mediums. The quantum transformation of operators of these devices can be written as

$$\begin{pmatrix} \hat{a}_{tH} \\ \hat{a}_{rH} \\ \hat{a}_{tV} \\ \hat{a}_{rV} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} \hat{a}_{i1H} \\ \hat{a}_{i2H} \\ \hat{a}_{i1V} \\ \hat{a}_{i2V} \end{pmatrix}, \tag{2.2.37}$$

where H and V refer to horizontal and vertical polarizations. Trivially, single-photon states of different polarization coming by the same direction would leave by different ones.

The propagator operator of the general PBS is a product of BS operators (2.2.36) for the different polarizations

$$\hat{P} = \exp\left\{\frac{\theta_H}{2}\left(a_{tH}^\dagger a_{rH} - a_{tH}a_{rH}^\dagger\right)\right\}\exp\left\{\frac{\theta_V}{2}\left(a_{tV}^\dagger a_{rV} - a_{tV}a_{rV}^\dagger\right)\right\}, \tag{2.2.38}$$

where $\theta_H = 0$ and $\theta_V = \pi$ for the case (2.2.37)

2.2.1.2 Waveplate

The most fundamental optical devices while working with polarization modes are waveplates. In a general way, if we have a retarder that introduces a phase shift δ between two polarizations H' and V' that are rotated an angle θ respect to polarization modes H and V, then, applying the correspondence principle with classical optics, the quantum transformations of operators can be deduced to be [Agarwal, 2012]

$$\begin{pmatrix} \hat{a}_H \\ \hat{a}_V \end{pmatrix} = \begin{pmatrix} \cos^2\theta e^{-i\frac{\delta}{2}} + \sin^2\theta e^{i\frac{\delta}{2}} & \sin\theta\cos\theta\left(e^{-i\frac{\delta}{2}} - e^{i\frac{\delta}{2}}\right) \\ \sin\theta\cos\theta\left(e^{-i\frac{\delta}{2}} - e^{i\frac{\delta}{2}}\right) & \cos^2\theta e^{i\frac{\delta}{2}} + \sin^2\theta e^{-i\frac{\delta}{2}} \end{pmatrix}\begin{pmatrix} \hat{a}_{H0} \\ \hat{a}_{V0} \end{pmatrix}. \tag{2.2.39}$$

The transformation matrix can be denoted as $W_{\delta,\theta}$ and can be achieved by solving Heisenberg equations (2.1.12) in system ν' rotated respect to the lab system ν, where $\nu = H, V$. The most interesting cases are those were the phase shift is π ($\lambda/2$) and $\pi/2$ ($\lambda/4$), this is, a half-waveplate (HWP) and a quarter-waveplate (QWP) respectively. The transformations then, are

$$H_\theta = W_{\pi,\theta} = -i\begin{pmatrix} -\cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}, \tag{2.2.40}$$

$$Q_\theta = W_{\frac{\pi}{2},\theta} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 - i\cos 2\theta & -i\sin 2\theta \\ -i\sin 2\theta & 1 + i\cos 2\theta \end{pmatrix}. \tag{2.2.41}$$

For the case where $\theta = \frac{-\pi}{4}$ we have

$$H_{\frac{\pi}{4}} = W_{\pi,\frac{\pi}{4}} = i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2.2.42}$$

$$Q_{\frac{\pi}{4}} = W_{\frac{\pi}{2},\frac{\pi}{4}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}. \tag{2.2.43}$$

Note that these transformations correspond to Pauli-X and $\sqrt{X}$ quantum gates [Nielsen and Chuang, 2002].

2.2.2 Integrated Devices for QC

A directional coupler (DC) is, as known, an integrated device that allows to couple energy between two directional spatial modes. Considering a directional coupler formed by two linear monomode waveguides, the Momentum operator (2.1.10) takes the form

$$\hat{M} = \hbar\beta_1 \hat{a}_1^\dagger \hat{a}_1 + \hbar\beta_2 \hat{a}_2^\dagger \hat{a}_2 + \hbar\kappa_{12} \left(\hat{a}_1^\dagger \hat{a}_1 \hat{a}_2^\dagger \hat{a}_2 \right). \tag{2.2.44}$$

Now, introducing this operator into Heisenberg's spatial equations (2.1.11), we obtain the following equation system

$$\begin{aligned} -i\frac{\partial \hat{a}_1}{\partial z} &= \beta_1 \hat{a}_1 + \kappa_{12} \hat{a}_2, \\ -i\frac{\partial \hat{a}_2}{\partial z} &= \kappa_{12} \hat{a}_1 + \beta_2 \hat{a}_2. \end{aligned} \tag{2.2.45}$$

Solving this differential equation system, the operators transformation matrix for DCs is easily obtained

$$\begin{aligned} \hat{a}_1 &= e^{i\frac{\beta_1+\beta_2}{2}z} \left[\hat{a}_{1_0} \cos\left(\frac{1}{2}\sqrt{(\beta_1-\beta_2)^2 + 4\kappa^2}\, z \right) + \hat{a}_{2_0} i \sin\left(\frac{1}{2}\sqrt{(\beta_1-\beta_2)^2 + 4\kappa^2}\, z \right) \right] \\ \hat{a}_2 &= e^{i\frac{\beta_1+\beta_2}{2}z} \left[\hat{a}_{2_0} \cos\left(\frac{1}{2}\sqrt{(\beta_1-\beta_2)^2 + 4\kappa^2}\, z \right) + \hat{a}_{1_0} i \sin\left(\frac{1}{2}\sqrt{(\beta_1-\beta_2)^2 + 4\kappa^2}\, z \right) \right] \end{aligned} \tag{2.2.46}$$

Considering the synchronous case $\beta_1 = \beta_2$, we obtain the operator transformation matrix

$$\begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} = e^{i\beta z} \begin{pmatrix} \cos\kappa z & i\sin\kappa z \\ i\sin\kappa z & \cos\kappa z \end{pmatrix} \begin{pmatrix} \hat{a}_{1_0} \\ \hat{a}_{2_0} \end{pmatrix}. \tag{2.2.47}$$

We can label this matrix $C_{\kappa z}$. The propagator operator of this is

$$\hat{C}_{\kappa z} = e^{i\frac{\kappa z}{\hbar}\hat{M}} = e^{i\frac{\kappa z}{\hbar}\left(\hat{a}_1^\dagger \hat{a}_1 - \hat{a}_2^\dagger \hat{a}_2\right)}. \tag{2.2.48}$$

It is important to note that any system that exchanges energy between different modes is a coupler. In this way, a BS is a coupler between the transmitted and reflected modes, while a waveplate is a coupler between polarization modes. Applying selective phase transformations to matrix (2.2.47) we can obtain the most general unitary transformation for group SU(2)

$$\begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} = e^{i\beta z} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta_f} \end{pmatrix} \begin{pmatrix} \cos\kappa z & i\sin\kappa z \\ i\sin\kappa z & \cos\kappa z \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta_i} \end{pmatrix} \begin{pmatrix} \hat{a}_{1_0} \\ \hat{a}_{2_0} \end{pmatrix}. \tag{2.2.49}$$

2.2.3 Devices for QC with spatial modes

A interesting way to implement QKD in high dimension is to make use of spatial modes to construct a high dimensional Hilbert space. This could be done, for example, by directly using different modes of a certain order, being those transmitted through free space or by a few-modes optical fiber, as the different transmitted qudits. Along with devices to implement transformations between them and using different basis is possible to implement HD-QKD protocols. Besides, the different modes transmitted by a few-modes optical fiber or in different cores of a multicore fiber can be used as base modes to implement phase encoding protocols in high dimension, as we are going to see in the next chapters 3 and 5.

Another possibility, compatible with the previous ones, is using the orbital angular momentum (OAM) of light as a high dimensional Hilbert space. OAM is carried by optical vortices of light, which are light modes with a field distribution of the form $F(r)\exp(il\phi)$. This distribution means that the field intensity tends to zero as $r \to 0$ whereas the phase shift in one cycle around the origin is $2\pi l$. The azimuthal index l is directly related to the OAM of the light and it means that the vortex carries an orbital angular momentum of $l\hbar$ per photon [Allen et al., 1992].

2.2.3.1 Laguerre-Gaussian and Hermite-Gaussian modes

The most physically realizable optical vortices are the Laguerre–Gaussian (LG) beam modes. These modes are solutions to Helmholtz's equation and their field amplitude is given by [Agarwal, 2012]

$$v_{nm}(x,\omega) = \sqrt{\frac{2}{\pi\omega}\frac{(-1)^p p!}{\sqrt{n!\,m!}}}\left(\frac{2r^2}{\omega^2}\right)e^{i\frac{r^2}{\omega^2}}\left(\frac{r\sqrt{2}}{\omega}\right)^{|n-m|} L_p^{|n-m|}e^{-i\theta(n-m)}, \tag{2.2.50}$$

where the azimuthal mode index is $l = n - m$ and $p = min(n, m)$. $r = \sqrt{x^2+y^2}$ and $\theta = \arctan\frac{y}{x}$ are the polar coordinates and $L_p^{|l|}$ is the generalized Laguerre polynomial

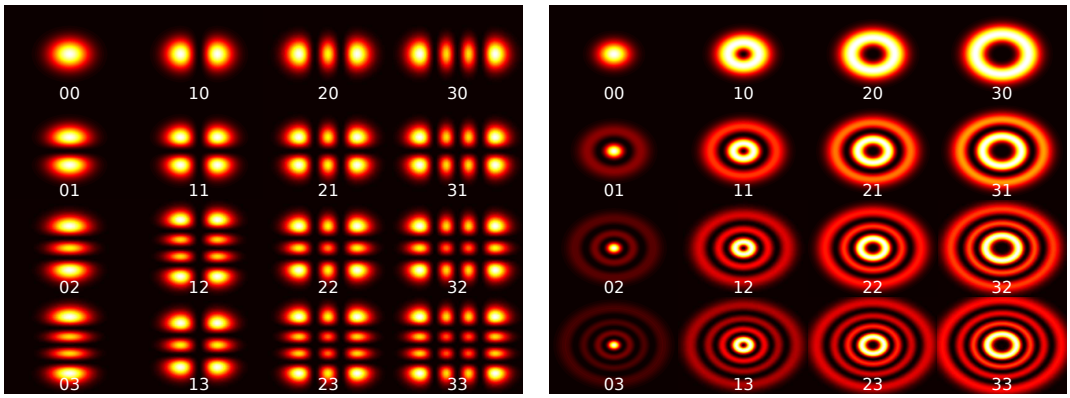
$$L_p^l(x) = \sum_{i=0}^{p}(-1)^i\begin{pmatrix} p+l \\ p-i \end{pmatrix}.\frac{x^i}{i!} \tag{2.2.51}$$

LG modes can be obtained by combination of the Hermite-Gaussian (HG) modes that most lasers emit and constitute the propagation modes of most optical fibers. HG modes are solutions to the Helmholtz's equation in Cartesian coordinates with rectangular symmetry along the propagation axis and their field amplitude is given by

$$u_{nm}(x,y,\omega) = u_n(x,\omega)u_m(y,\omega), \tag{2.2.52}$$

where

$$u_n(x,\omega) = \sqrt{\sqrt{\frac{2}{\pi}}\frac{1}{2^n n!\,\omega}}H_n\left(\frac{\sqrt{2}x}{\omega}\right)e^{-\frac{x^2}{\omega^2}}, \tag{2.2.53}$$



(a) HG_{nm}. (b) LG_{lp}.

Figure 2.2.1: Hermite-Gaussian (a) and Laguerre-Gaussian (b) modes. HG modes index are n, m, while LG index are $l = n - m$ and $p = min(n, m)$.

and $H_n(x)$ is the Hermite polynomial

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}. \tag{2.2.54}$$

As both types of modes are solutions to Helmholtz's equation, they are linearly dependent. By analysing expressions (2.2.50) and (2.2.52), it can be proved [Beijersbergen et al., 1993, Agarwal and Banerji, 2006, Agarwal, 2012] that a LG mode v_{nm} can be decomposed in a lineal combination of HG modes u_{nm} as follows

$$v_{nm}(x, y, z) = \sum_{k=0}^{n+m} i^k b(n, m, k) u_{n+m-k,k}(x, y, z). \tag{2.2.55}$$

Factor i^k represents a relative phase shift of $\pi/2$ between successive HG modes of the linear combination, while $b(x, y, z)$ are real coefficients whose value is given by

$$b(n, m, k) = \sqrt{\frac{(n + m - k)!}{2^{n+m} n!\, m!\, k!}} \frac{d^k}{dt^k} \left[(1 - t)^n (1 + t)^m\right]_{t=0}. \tag{2.2.56}$$

Different values of this coefficient are shown on Table 2.1

An important property about HG modes is the fact that it is possible to decompose them into a linear combination of HG modes of a basis rotated 45° respect the basis of the original ones [Agarwal and Banerji, 2006]. This decomposition works the same way as LG decomposition (2.2.55) without the existence of the phase shift $\pi/2$ between successive modes. So, a diagonal HG mode, this is, rotated -45° respect the main cartesian axis, can be written as

$$u_{nm}\left(\frac{x - y}{2}, \frac{x + y}{2}, z\right) = \sum_{k=0}^{n+m} b(n, m, k) u_{n+m-k,k}(x, y, z). \tag{2.2.57}$$

Table 2.1: Examples of values of coefficient $b(x, y, z)$.

n	**m**	$k=0$	1	2	3
0	0	1			
0	1	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$		
1	0	$\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}}$		
0	2	$\frac{1}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$	
1	1	$\frac{1}{\sqrt{2}}$	0	$-\frac{1}{\sqrt{2}}$	
2	0	$\frac{1}{2}$	$-\frac{1}{\sqrt{2}}$	$\frac{1}{2}$	
0	3	$\frac{1}{\sqrt{8}}$	$\sqrt{\frac{3}{8}}$	$\sqrt{\frac{3}{8}}$	$\frac{1}{\sqrt{8}}$
1	2	$\sqrt{\frac{3}{8}}$	$\frac{1}{\sqrt{8}}$	$-\frac{1}{\sqrt{8}}$	$-\sqrt{\frac{3}{8}}$
2	1	$\sqrt{\frac{3}{8}}$	$-\frac{1}{\sqrt{8}}$	$-\frac{1}{\sqrt{8}}$	$\sqrt{\frac{3}{8}}$
3	0	$\frac{1}{\sqrt{8}}$	$-\sqrt{\frac{3}{8}}$	$\sqrt{\frac{3}{8}}$	$-\frac{1}{\sqrt{8}}$

2.2.3.2 Quantum transformations between LG and HG modes

The relations between HG and LG modes can be transcribed to quantum formalism. In this way, if we have a single-photon state in, for example, a LG mode, that state is equivalent to a superposition of single photon states in HG modes. So, according to the correspondence principle, relation (2.2.55) can be expressed in terms of emission operators as

$$\hat{a}^{\dagger}_{LG_{nm}} = \sum_{k=0}^{n+m} i^k b(n,m,k) \hat{a}^{\dagger}_{HG'_{n+m-k,k}}, \tag{2.2.58}$$

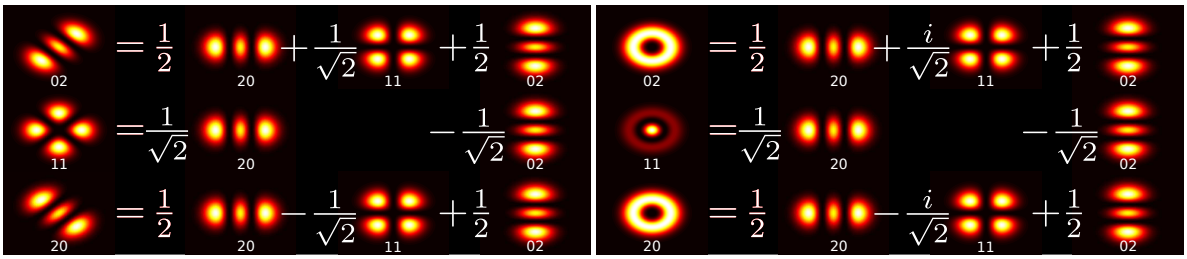
while relation (2.2.57) becomes

$$\hat{a}^{\dagger}_{HG_{nm}} = \sum_{k=0}^{n+m} b(n,m,k) \hat{a}^{\dagger}_{HG'_{n+m-k,k}}, \tag{2.2.59}$$

where modes HG' are rotated 45° respect to HG ones.

Equations (2.2.58) and (2.2.59) compose two groups of equation systems. Solving these systems we can obtain the transformation matrices of operators. So, if we have modes HG, HG' and LG of order $N = n + m$ whose operators are

$$\mathcal{X}_{N+1} = \begin{pmatrix} \hat{a}_{HG_{N,0}} \\ \vdots \\ \hat{a}_{HG_{N-i,i}} \\ \vdots \\ \hat{a}_{HG_{0,N}} \end{pmatrix}, \quad \mathcal{X'}_{N+1} = \begin{pmatrix} \hat{a}_{HG'_{N,0}} \\ \vdots \\ \hat{a}_{HG'_{N-i,i}} \\ \vdots \\ \hat{a}_{HG'_{0,N}} \end{pmatrix}, \quad \mathcal{L}_{N+1} = \begin{pmatrix} \hat{a}_{LG_{N,0}} \\ \vdots \\ \hat{a}_{LG_{N-i,i}} \\ \vdots \\ \hat{a}_{LG_{0,N}} \end{pmatrix}, \tag{2.2.60}$$



(a) (b)

Figure 2.2.2: Decomposition of diagonal HG_{nm} modes (a) and LG_{nm} modes (b) modes into linear HG_{nm} modes.

then, the transformation matrices between the three basis are given by

$$\mathcal{X}_{N+1} = B \cdot \mathcal{X'}_{N+1}, \tag{2.2.61}$$

$$\mathcal{L}_{N+1} = B \cdot G^{\dagger}_{\frac{\pi}{2}} \cdot \mathcal{X'}_{N+1}, \tag{2.2.62}$$

$$\mathcal{L}_{N+1} = B \cdot G^{\dagger}_{\frac{\pi}{2}} \cdot B^{T} \cdot \mathcal{X}_{N+1}, \tag{2.2.63}$$

where we have defined matrices

$$B_{jk} = b_{jk} = b(N+1-j, j-1, k), \tag{2.2.64a}$$

$$G_{\frac{\pi}{2}\,jk} = g_{jk} = i^{j-1}\delta_{jk}, \tag{2.2.64b}$$

and taken into account that these matrices fulfil the inversion relationships $B^{-1} = B^{T}$, $G^{-1}_{\frac{\pi}{2}} = G^{\dagger}_{\frac{\pi}{2}}$. The transformation matrix in (2.2.63) can be reduced to

$$\left(B \cdot G^{\dagger}_{\frac{\pi}{2}} \cdot B^{T}\right)_{jk} = \sum_{m} i^{m-1} b_{jm} b_{km} = e^{i\frac{\pi}{4}N} i^{k-j} b_{jk}. \tag{2.2.65}$$

Particularising for order $N = 1$, this is, for a two dimensional case, we have

$$\mathcal{X}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \mathcal{X'}_2, \tag{2.2.66}$$

$$\mathcal{L}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \mathcal{X'}_2, \tag{2.2.67}$$

$$\mathcal{L}_2 = \frac{e^{-i\frac{\pi}{4}}}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \mathcal{X}_2, \tag{2.2.68}$$

where

$$\mathcal{X}_2 = \begin{pmatrix} \hat{a}_{HG_{10}} \\ \hat{a}_{HG_{01}} \end{pmatrix}, \quad \mathcal{X'}_2 = \begin{pmatrix} \hat{a}_{HG'_{10}} \\ \hat{a}_{HG'_{01}} \end{pmatrix}, \quad \mathcal{L}_2 = \begin{pmatrix} \hat{a}_{HG_{10}} \\ \hat{a}_{HG_{01}} \end{pmatrix}. \tag{2.2.69}$$

2.2.3.3 Cylindrical lens converters

2.2.3.3.1 Gouy phase

By observing equations (2.2.55) and (2.2.57) we can see that it is possible to transform a HG mode into a LG mode, and the other way, by means of adding a phase shift $\pi/2$ between the successive HG modes, into which we can decompose our original mode. This can be achieved thanks to the Gouy phase [Liñares et al., 2017c, Beijersbergen et al., 1993]. The Gouy phase consists of the phase difference acquired by a gaussian beam of light when crossing the waist of the beam with respect to a plane wave.

For an isotropic gaussian beam, this is, its waist is in the same position for all the cross direction, the Gouy phase is given by

$$\varphi_{G_{nm}} = (n + m + 1)\,\varphi_G(z), \tag{2.2.70}$$

with $\Phi_G = \arctan z/z_R$, where the waist is situated in $z = 0$ and z_R is the Rayleigh length. If the beam is astigmatic the phase shift is a bit different. Using a cylindrical lens, an astigmatic beam can be generated and the Gouy phase presents two contributions corresponding to each of the transversal directions of the lens

$$\varphi_{G_{nm}} = \left(n + \frac{1}{2}\right)\varphi_{G_x}(z) + \left(m + \frac{1}{2}\right)\varphi_{G_y}(z), \tag{2.2.71}$$

being

$$\begin{aligned} \varphi_{G_x} &= \arctan \frac{z - z_{0x}}{z_{Rx}}, \\ \varphi_{G_y} &= \arctan \frac{z - z_{0y}}{z_{Ry}}, \end{aligned} \tag{2.2.72}$$

where z_{0x} and z_{0y} are the position of the beam waist in x and y axis respectively, and z_{Rx} and z_{Ry} are the corresponding Rayleigh lengths in said axis.

2.2.3.3.2 Mode converter

In order to generate phase shifts between modes using the Gouy phase [Beijersbergen et al., 1993], it is necessary to convert an incident isotropic Gaussian beam into an astigmatic one within a cavity, so that the same isotropic mode exits. The phase shift between HG modes oriented along the astigmatism axes must be generated in this cavity. Let's consider an astigmatic beam with waists located in the same place, but with different Rayleigh range, z_{Rx} and z_{Ry}. If we place a cylindrical lens in the position where the transverse radius of the beam coincide, then the outgoing beam will be isotropic. Placing symmetrically another cylindrical lens at the same distance from the waist of the beam, we would have that the beam is astigmatic in the region covered by the lenses, while it is isotropic outside them.

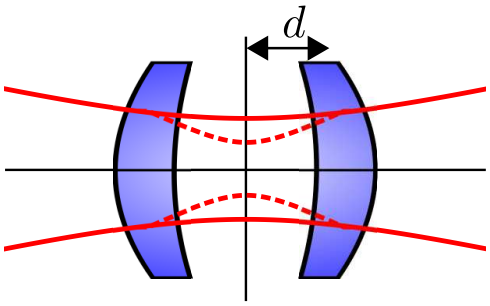


Figure 2.2.3: Cylindrical lens mode converter. The solid and dashed lines represent the different widths of the light beam in orthogonal axis.

The condition for the transversal radius of the beam to be equal at $z = d$ results in

$$\frac{z_{Rx}^2 + d^2}{z_{Rx}} = \frac{z_{Ry}^2 + d^2}{z_{Ry}}, \tag{2.2.73}$$

and, at the same time, the beam must meet the lens equation

$$\frac{1}{f} = \frac{1}{R_x(d)} - \frac{1}{R_y(d)} = \frac{d}{z_{Rx}^2 + d^2} - \frac{d}{z_{Ry}^2 + d^2}. \tag{2.2.74}$$

Equations (2.2.73) and (2.2.74) form an equation system that can be solved to obtain the Rayleigh ranges

$$z_{Rx} = dp, \tag{2.2.75}$$
$$z_{Ry} = d/p, \tag{2.2.76}$$

where

$$p = \sqrt{\frac{1 - d/f}{1 + d/f}}. \tag{2.2.77}$$

The difference in the Gouy phase between the lenses would be

$$\Delta\varphi_G = \varphi_G(d) - \varphi_G(-d) = (n + m + 1)\,\frac{\Delta\varphi_{Gx} + \Delta\varphi_{Gy}}{2} + (n - m)\,\frac{\Delta\varphi_{Gx} - \Delta\varphi_{Gy}}{2}, \tag{2.2.78}$$

where

$$\Delta\varphi_{Gi} = \varphi_{Gi}(d) - \varphi_{Gi}(-d) = 2\arctan\frac{d}{z_{Ri}} \quad i = x, y. \tag{2.2.79}$$

If a HG mode strikes a lens system whose main axis are rotated 45° with respect to the mode axis, then, its component modes in the lens main axis, are going to experiment phase shifts between them as a consequence of the Gouy phase difference (2.2.78). If the

incident diagonal HG mode is of order $N = n + m$, it is composed of $N + 1$ HG modes in the lens axis and the phase difference between successive modes is given by

$$\Phi = \Delta\varphi_{GN-k,k} - \Delta\varphi_{GN-k-1,k+1} = 2\left[\arctan\frac{1}{p} - \arctan p\right], \tag{2.2.80}$$

where $k = 0, ..., N$.

Consequently, the phase difference introduced between the modes is function of the focal of the lenses f and the distance between $D = 2d$ and its range of values goes from 0 to π. This system is denominated a cylindrical lens converter (CLC) and it works in a similar way to retarder plates for polarization. The general transformation that a CLC implements is

$$u_{nm}(\frac{x-y}{2}, \frac{x+y}{2}, z) \to \sum_{k=0}^{n+m} e^{ik\Phi} b(n, m, k) u_{n+m-k,k}(x, y, z). \tag{2.2.81}$$

There are two more relevant CLCs that are equivalent to half-wave plated (HWP) and a quarter-wave plate (QWP) for polarization:

- $\pi/2$ *converter*. If the phase shift between successive modes (2.2.78) is $\Phi = \frac{\pi}{2}$, then a factor i^k is introduced in each correspondent term of the HG mode decomposition (2.2.57), obtaining in a LG mode of the same order. The converter also can implement the inverse transformation, transforming LG modes in HG ones. The condition to obtain this phase shift is $p = -1 + \sqrt{2}$, which means that the distance between lenses D must be

  $$D = \sqrt{2} f \tag{2.2.82}$$

  This way, the transformation is

  $$u_{nm}(\frac{x-y}{2}, \frac{x+y}{2}, z) \to v_{nm}(x, y, z) = \sum_{k=0}^{n+m} i^k b(n, m, k) u_{n+m-k,k}(x, y, z). \tag{2.2.83}$$

- π *converter*. If the phase shift between successive modes (2.2.78) is $\Phi = \pi$, the introduced factor in in each correspondent term of the HG mode decomposition (2.2.57) is $(-1)^k$. If a LG_{nm} mode is introduced in this converter, the phase shift results in the inversion of said mode to mode LG_{mn}, which physically means that the angular momentum is inverted $l \leftrightarrow -l$. The condition for this phase shift is $p = 0$, which means that the distance between lenses D must be

  $$D = 2f \tag{2.2.84}$$

  This way, the transformation is

  $$u_{nm}(\frac{x-y}{2}, \frac{x+y}{2}, z) \to u_{mn}(\frac{x-y}{2}, \frac{x+y}{2}, z) = \sum_{k=0}^{n+m} (-1)^k b(n, m, k) u_{n+m-k,k}(x, y, z). \tag{2.2.85}$$

2.2.3.4 Quantum Transformation Of The Converters

We can develop the quantum formalism of the CLCs. Let us denote as $\hat{a}_{nm}$ the absorption quantum operator of a photon excited in a HG mode aligned with basis $\mathcal{X}$ ($\bigoplus$); and we also denote $\hat{a}'_{nm}$ as the absorption quantum operator of a photon excited in a HG mode aligned with a base $\mathcal{X}'$ ($\bigotimes$), which is rotated an angle of $+45°$ respect to base $\mathcal{X}$. So, considering equation (2.2.81), the quantum transformation between operators is going to be

$$\hat{a}_{HG_{nm}} = \sum_{k=0}^{n+m} e^{ik\Phi} b(n,m,k) \hat{a}_{HG'_{n+m-k,k}}. \tag{2.2.86}$$

Now, we can solve this group of equation systems as done previously in subsubsection 2.2.3.2 to obtain the propagation transformation matrices of the operators. Alternatively, we now that the these matrices for basis HG' given by $C^{N+1}_{\frac{\pi}{2},0} = G_{\frac{\pi}{2}}$ and $C^{N+1}_{\pi,0} = G_{\pi}$ for converters $\frac{\pi}{2}$ and π respectively, where the former is given by equation (2.2.64b) and the latter is given by

$$G_{\pi jk} = (-1)^{j-1}\delta_{jk}, \tag{2.2.87}$$

that fulfils $G^{-1}_{\pi} = G_{\pi}$. Thus, using basis transformation (2.2.61) we can obtain our desired transformations.

Therefore, matrix transformation of a $\pi/2$ converter rotated $45°$ is

$$C^{N+1}_{\pi/2,\pi/4} = B \cdot G_{\frac{\pi}{2}} \cdot B^T, \tag{2.2.88}$$

where $C^{N+1}_{\pi/2,\pi/4} = e^{i\frac{\pi}{4}N} i^{k-j} b_{jk}$. Employing also basis transformation (2.2.63) we can ascertain how this converter turns HG modes into LG ones and vice versa

$$\begin{aligned} \mathcal{L}_{N+1} &= \mathbb{I} \cdot \mathcal{X}_{N+1_0}, \\ \mathcal{X}_{N+1} &= \mathbb{U} \cdot \mathcal{L}_{N+1_0}, \end{aligned} \tag{2.2.89}$$

where subindex 0 refer to the original base prior the CLC, $\mathbb{I}$ is the identity matrix and

$$\mathbb{U} = \begin{pmatrix} 0 & \cdots & 1 \\ \vdots & \iddots & \vdots \\ 1 & \cdots & 0 \end{pmatrix}. \tag{2.2.90}$$

On the other hand, for a π converter we have the transformation matrix

$$C^{N+1}_{\pi,\pi/4} = B \cdot G_{\pi} \cdot B^T = \mathbb{U} \tag{2.2.91}$$

And employing also basis transformation (2.2.62) we can see that this converter inverts LG modes

$$\mathcal{L}_{N+1} = \mathbb{U} \cdot \mathcal{L}_{N+1_0}. \tag{2.2.92}$$

2.2.3.4.1 Modes with N=1

Let us examine the case for $N = 1$ more closely. If we suppose that HG basis $\mathcal{X}'$ is rotated an arbitrary angle α, instead of 45°, respect to base $\mathcal{X}$, the decomposition of a single-photon state into both HG modes of the latter base is trivially

$$\begin{aligned} |1_X\rangle &= \cos\alpha\,|1_{X'}\rangle - \sin\alpha\,|1_{Y'}\rangle\,, \\ |1_Y\rangle &= \sin\alpha\,|1_{X'}\rangle + \cos\alpha\,|1_{Y'}\rangle\,, \end{aligned} \tag{2.2.93}$$

where modes X and Y design modes HG_{10} and HG_{01} respectively. Now, if any of the former states crosses a CLC whose main axis are aligned with base $\mathcal{X}'$, they are transformed as

$$\begin{aligned} |1_{X0}\rangle &\to \cos\alpha\,|1_{X'}\rangle - \sin\alpha\,e^{i\Phi}\,|1_{Y'}\rangle\,, \\ |1_{Y0}\rangle &\to \sin\alpha\,|1_{X'}\rangle + \cos\alpha\,e^{i\Phi}\,|1_{Y'}\rangle\,, \end{aligned} \tag{2.2.94}$$

Expressing them into operator form and putting everything into base $\mathcal{X}$ considering (2.2.93), we have

$$\begin{pmatrix} \hat{a}^\dagger_{X0} \\ \hat{a}^\dagger_{Y0} \end{pmatrix} = \begin{pmatrix} \cos^2\alpha + e^{i\Phi}\sin^2\alpha & \left(1-e^{i\Phi}\right)\sin\alpha\cos\alpha \\ \left(1-e^{i\Phi}\right)\sin\alpha\cos\alpha & \sin^2\alpha + e^{i\Phi}\cos^2\alpha \end{pmatrix} \begin{pmatrix} \hat{a}^\dagger_X \\ \hat{a}^\dagger_Y \end{pmatrix}. \tag{2.2.95}$$

Therefore, the general transformation of a CLC for HG modes with $N = 1$ $\hat{C}_{\phi,\alpha}$ is given by

$$\begin{pmatrix} \hat{a}_X \\ \hat{a}_Y \end{pmatrix} = e^{i\frac{\Phi}{2}} \begin{pmatrix} \cos\frac{\Phi}{2} - i\sin\frac{\Phi}{2}\cos 2\alpha & -i\sin\frac{\Phi}{2}\sin 2\alpha \\ -i\sin\frac{\Phi}{2}\sin 2\alpha & \cos\frac{\Phi}{2} + i\sin\frac{\Phi}{2}\cos 2\alpha \end{pmatrix} \begin{pmatrix} \hat{a}_{X0} \\ \hat{a}_{Y0} \end{pmatrix}. \tag{2.2.96}$$

This transformation corresponds to the waveplate transformation (2.2.39) for polarization modes, thus, a CLC implements the general SU(2) transformation for HG modes with $N = 1$. Just like in the wave plate, the matrices for π and $\frac{\pi}{2}$ converters are

$$C_{\pi,\alpha} = \frac{1}{\sqrt{2}} \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}, \tag{2.2.97}$$

$$C_{\pi/2,\alpha} = \frac{e^{i\frac{\pi}{4}}}{\sqrt{2}} \begin{pmatrix} 1 - i\cos 2\alpha & -i\sin 2\alpha \\ -i\sin 2\alpha & 1 + i\cos 2\alpha \end{pmatrix}. \tag{2.2.98}$$

For the case $\alpha = \frac{\pi}{4}$, we have again quantum gates X and $\sqrt{X}$

$$C_{\pi,\pi/4} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.2.99}$$

$$C_{\pi/2,\pi/4} = \frac{e^{i\frac{\pi}{4}}}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \tag{2.2.100}$$

2.2.3.5 Mach-Zehnder interferometer with CLC

Let us considerate a Mach-Zehnder interferometer (MZI) that, as known, is formed by two BS two mirrors and a phase element. In this case, let us introduce as the phase element a π CLC converter (MZIC) and we can see how does the interferometer behaves when a single-photon state in mode HG of order $N = 1$ is introduced. The transformation of the quantum operators is as follows

$$\begin{pmatrix} \hat{a}_{hX} \\ \hat{a}_{vX} \\ \hat{a}_{hY} \\ \hat{a}_{vY} \end{pmatrix} = B \otimes \mathbb{I} \cdot \mathbb{M} \otimes \mathbb{I} \cdot \mathbb{C}_{\pi,0} \cdot \mathbb{M} \otimes \mathbb{I} \cdot B \otimes \mathbb{I} \cdot \begin{pmatrix} \hat{a}_{h0X} \\ \hat{a}_{h0X} \\ \hat{a}_{h0Y} \\ \hat{a}_{v0Y} \end{pmatrix}, \tag{2.2.101}$$

where matrix B is the BS matrix (2.2.35), $\mathbb{I}$ is the identity matrix, $\mathbb{M} = -\mathbb{U}^2$ represents the phase shift π introduced by the mirrors and the direction interchange and the matrix of the converter is

$$\mathbb{C}_{\pi,0} = \text{diag}\,(1, 1, -1, 1) \tag{2.2.102}$$

Thus, the transformation produced by the MZIC for case $N = 1$ is

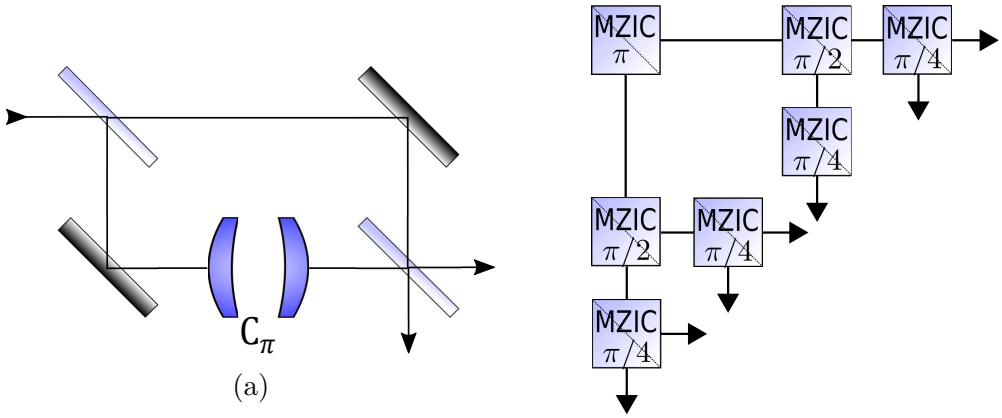
$$\mathcal{M}_\pi = \begin{pmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{2.2.103}$$

which is essentially a system equivalent to PBS (2.2.37) for polarization modes, this is, the MZIC separates single-photon states in modes X and Y by different directions.

For a general $N = n + m$, the MZIC $\mathcal{M}_\pi$ would separate the $N + 1$ possible states into two groups, as it only separate modes that follows the succession $\text{HG}_{n,m} \leftrightarrow \text{HG}_{n-2,m+2}$. Now, a $\frac{\pi}{2}$ converter actually generates phase shifts π into that succession of modes, so a MZIC $\mathcal{M}_{\frac{\pi}{2}}$ can separate the each group into another pair of groups. By the same logic, if we want to keep separating modes, we have to employ successive MZICs at the outputs of each previous one with successive phases $\frac{\pi}{2^m}$, until $m = 1 - \lceil \log_2 N + 1 \rceil$. Mathematically,

$$\mathcal{M}_\pi^{[1]} \cdot \mathcal{M}_{\frac{\pi}{2}}^{[2]} \cdot \ldots \cdot \mathcal{M}_{2^m\pi}^{[m]}, \tag{2.2.104}$$

where $[i]$ represents the number of MZIC of such kind needed. Thus, a HG modal demultiplexer can be implemented. Additionally, if we combine two π converters rotated 45° between each other ($\mathbb{C}_{\pi,\pi/4}$ and $\mathbb{C}_{\pi,0}$), a MZIC $\mathcal{M}_\pi^{(LG)}$ (2.2.103) for LG modes is obtained (after compensating a global phase $\pi/2$ generated by the lenses). Therefore, by following the same strategy than (2.2.104), a demultiplexer for LG modes can be implemented as well.



(a) (b)

Figure 2.2.4: Figure (a) shows the basic configuration of a MZIC_π. Figure (b) shows the scheme of a demultiplexer based in MZICs for the cases $N = 4, 5, 6, 7$.

2.3 Quantum states engineering for QC

In this section, we are going to develop devices in order to generate special quantum states that can be employed into quantum cryptography. In particular, we are going to study the quantum states known as quantum vortex states (QVS).

2.3.1 Quantum vortex states with SAM, OAM and FAM

Quantum vortex states, originally proposed in [Agarwal et al., 1997], are analogous to classical vortices explained in subsection (2.2.3.1), but in the optical field-strength space (OFS). Thus, a quantum state $|\phi\rangle$ will be a vortex state when it has the form

$$\langle x, y|\psi\rangle \approx (x \pm iy)^n \, e^{-\left(x^2+y^2\right)/2\sigma}, \tag{2.3.105}$$

where $|x, y\rangle$ is the eigenvector to the quadrature operator representing the optical field-strength

$$\hat{\mathcal{E}}_i = \frac{1}{\sqrt{2}}\left(\hat{a}_i^\dagger + \hat{a}_i\right), \tag{2.3.106}$$

with $i = x.y$, and analogously, the second quadrature is [Schleich, 2001]

$$\hat{\mathcal{P}}_i = \frac{i}{\sqrt{2}}\left(\hat{a}_i^\dagger - \hat{a}_i\right), \tag{2.3.107}$$

As we saw, classical light vortices, this is, LG modes, carry orbital angular momentum (OAM). However, vortex states are abstract vortices displayed in the OFS of the different modes x, y of light used. Thus, any physical meaning of the vortex is going to be related to the kind of modes that we are working with.

In first case, if we employ two orthogonal polarization modes $(\hat{a}_H, \hat{a}_V)$, vortex states become a representation of the spin momentum carried by our light state. In [Liñares and Nistal, 2009], our group made a quantum mechanical derivation of the spin operator in integrated isotropic and anisotropic photonic waveguides, starting from the first principles of the electromagnetic theory and conservation laws. Spin operator is given by

$$\hat{L}_s = \hbar\left(\hat{n}_+ - \hat{n}_-\right) = \hbar\left(\hat{a}_H^\dagger \hat{a}_V - \hat{a}_H \hat{a}_V^\dagger\right). \tag{2.3.108}$$

For example, if we have a state of n photons horizontally polarized and m photons vertically polarized $|n_H, m_V\rangle$, we can obtain a vortex state by making the state cross a 45° rotated QWP. Trivially, the spin of this vortex will be given by

$$\langle L_s\rangle = \langle n_H, m_V|\,\hat{Q}^\dagger_{\pi/4}\hat{L}_s\hat{Q}_{\pi/4}\,|n_H, m_V\rangle = \langle n_+, m_-|\,\hat{L}_s\,|n_+, m_-\rangle = (n-m)\hbar. \tag{2.3.109}$$

where $\hat{Q}_{\pi/4}$ is the operator of the QWP (2.2.41). The order of the vortex $n-m$ determines the spin of the state.

If we employ classical Hermite-Gauss (HG) modes in our quantum states, quantum vortex states will be similar to classical light vortices they will represent the OAM carried by the state. The OAM operator is given by

$$\hat{L} = \hbar\sum_{l,p} l\,\hat{n}_{l,p}. \tag{2.3.110}$$

where $l = n - m$ and $p = \min(n, m)$ are the indexes of classical $\mathrm{LG}_{l,p}$ modes and n and m are the indexes of classical HG_{nm}. As we previously explained, CLCs are required to work with HG and LG modes. In this case, employing a $\pi/4$ converter rotated 45°, if we make state $|\psi_{HG}\rangle = |n_{HG_{N,0}}\rangle \otimes |n_{HG_{N-1,1}}\rangle \otimes \ldots |n_{HG_{N/2,N/2}}\rangle \ldots \otimes |n_{HG_{1,N-1}}\rangle \otimes |n_{HG_{0,N}}\rangle$ cross the CLC, we will obtain a high dimensional vortex state who carries a OAM of

$$\langle L\rangle = \langle\psi_{HG}|\,\hat{C}^*\hat{L}\hat{C}\,|\psi_{HG}\rangle = \hbar\sum_{i=0}^{N+1}(N-2i)n_{N-2i}. \tag{2.3.111}$$

Now, in any other different case, like for example, when using path modes of different waveguides, the quantum vortex will not carry any physical angular momentum. However, we can consider that it carries a fictitious orbital momentum (FAM) that will work in the same way as OAM (2.3.110).

$$\hat{L}_F = \hbar\sum_{l,p} l_F\,\hat{n}_{l,p}. \tag{2.3.112}$$

In this case, couplers are required to employ the SU(2) transformation from before (2.3.111).

The most important point about this, it is the fact that both OAM and FAM from vortex quantum states allow to generate an infinite dimensional Hilbert space to encode quantum information. This results in that quantum vortex states open great possibilities in DV- and CV-QC

2.3.2 Generating quantum vortex states with SPDC

We have already shown how a QWPs and CLCs rotated 45° ($\hat{Q}_{\pi/4}$) can be used to obtain a vortex state in polarization and spatial modes. Now we are going to analyse how to generate them when using squeezed sources. As well, we are going to study how squeezing affects the momentum of the vortex state.

It is known that single mode squeezed states can be generated by degenerate parametric oscillation in an optical parametric oscillator [Wu et al., 1987], or using four-wave mixing [Slusher et al., 1987]

$$|\xi\rangle = \hat{S}(\xi)\,|0\rangle = e^{\frac{1}{2}\left(\xi^*\hat{a}^2 - \xi\hat{a}^{\dagger 2}\right)}\,|0\rangle = \frac{1}{\sqrt{\cosh r}}\sum_{n=0}^{\infty}\left(-e^{i\phi}\tanh r\right)^n \frac{\sqrt{2n!}}{2^n n!}\,|2n\rangle, \tag{2.3.113}$$

where $\xi \equiv \eta = re^{i\phi}$ is the squeezing parameter, while a two mode squeezed states are generated through SPDC

$$|\xi_{12}\rangle = \hat{S}_{12}(\xi)\,|0\rangle = e^{\frac{1}{2}\left(\xi^*\hat{a}_1\hat{a}_2 - \xi\hat{a}_1^\dagger\hat{a}_2^\dagger\right)}\,|0\rangle = \frac{1}{\cosh r}\sum_{n=0}^{\infty}\left(-e^{i\phi}\tanh r\right)^n |n,n\rangle. \tag{2.3.114}$$

In this subsection, we are going to focus on the second method. A theoretical study of squeezed vortex generation with single-mode squeezed states is added in appendix A.1 of this chapter.

2.3.2.1 Generation of SAM vortex states with SPDC

2.3.2.1.1 Employing SPDC type I

One way of engineering squeezed vortex states employing spontaneous parametric down-conversion (SPDC) has been shown in [Agarwal, 2011]. Unlike the analysis shown in appendix A.1 it studies a bimodal squeezed state and it consists of the subtraction of a single photon in one arm of a type I SPDC process

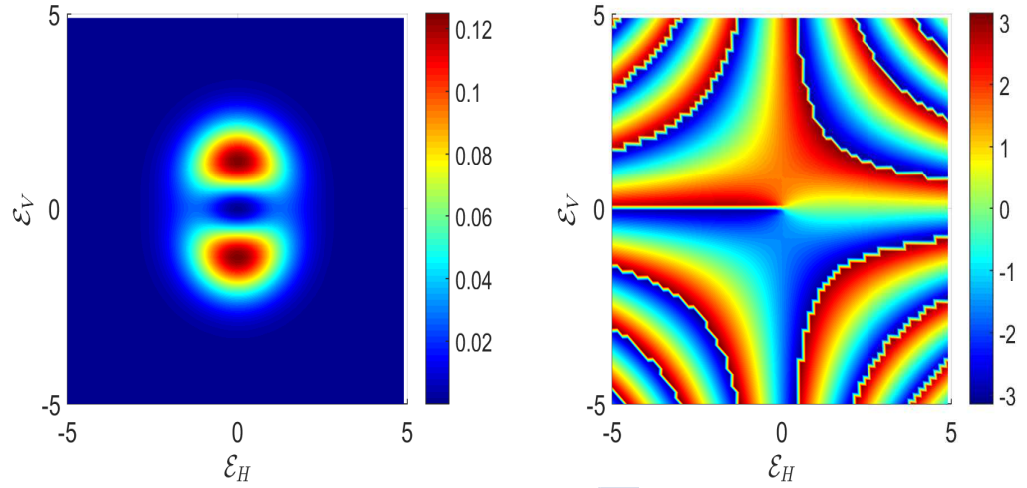
$$|\Psi\rangle = \hat{a}_2\,\hat{S}_{12}(\xi)\,|0\rangle\,. \tag{2.3.115}$$

If we want to use polarization modes we can employ a half wave plate (HWP) in order to change the polarization of one of the modes and then employ a polarisation beam splitter (PBS) to join both modes. According to [Agarwal, 2011], the quadrature distribution of this state (2.3.115) in our polarization modes is

$$\Psi(x_H, x_V) = \frac{\sqrt{2}e^{i\phi}\left(x_H - \eta x_V\right)}{\left(1-\eta^2\right)^{3/2}\pi^{1/2}\cosh^2 r}\exp\left\{\frac{2x_H x_{a2}\eta - \left(x_H^2 + x_V^2\right)\eta^2}{1-\eta^2} - \frac{1}{2}\left(x_H^2 + x_V^2\right)\right\}, \tag{2.3.116}$$

where $\eta = re^{i\phi}$ represents the squeezing in the OFS space.

For $\eta = i|\eta|$ this has the structure of an elliptical vortex. We can see this in Figure 2.3.5 where we observe its elliptical shape around the singularity.



(a) Probability density. (b) Phase density.

Figure 2.3.5: Local quantum vortex with $r = 0.5, \phi = 0$.

However, if we calculate the spin momentum carried by the stage

$$\langle L_z \rangle = \int\int \Psi^* L_z \Psi \, dx_H \, dx_V = 0, \tag{2.3.117}$$

we see that it does not carry an average spin. This is logical as state (2.3.116) is only a vortex under the condition

$$\eta = i|\eta| \iff \phi = \frac{\pi}{2} + k\pi. \tag{2.3.118}$$

This means that the state is only a vortex in certain periodic planes. Thus, we can refer to state (2.3.116) as a *local* vortex state.

If we want for the state to carry spin, we can add a QWP, rotated 45° respect the polarization, at the output of the PBS, as shown in Figure 2.3.6. So, we have the following state

$$|\Psi\rangle = \hat{L}_{\left(\frac{\pi}{2},\frac{\pi}{4}\right)} \hat{P}_{BS} \hat{L}_{1\left(\pi,\frac{\pi}{4}\right)} \hat{a}_2 \hat{S}_{12}(\xi) \, |0\rangle \, . \tag{2.3.119}$$

Now, state (2.3.119) can be calculated in the OFS from (2.3.116) by means of Feynman propagation [Hibbs and Feynman, 1965, Liñares et al., 2012], as follows

$$\Psi_F(x,y) = \int\int K(x,y,x_0,y_0,z,0)\Psi(x_0,y_0)dx_0dy_0, \tag{2.3.120}$$

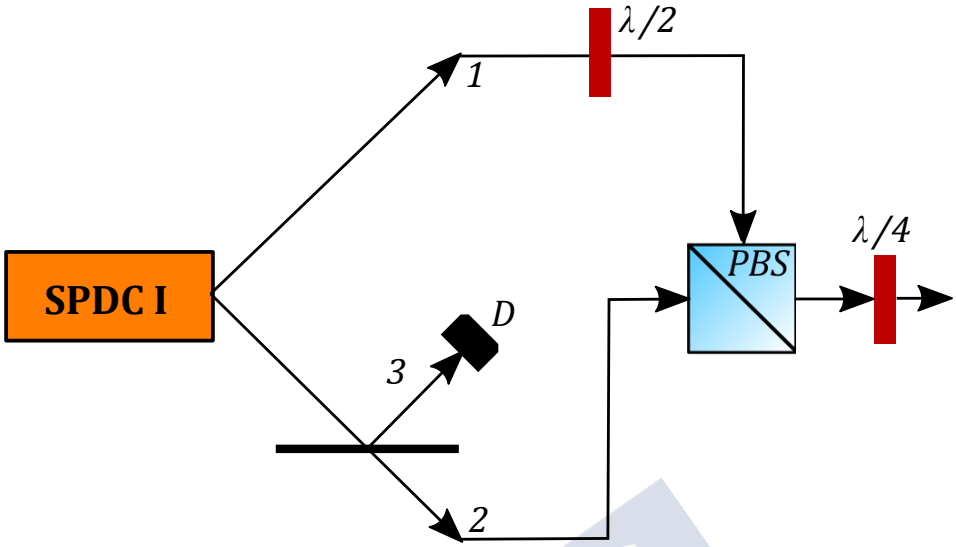


Figure 2.3.6: Obtention of a polarization quantum vortex with SPDC I.

where $K(x,y,x_0,y_0,z,0)$ is Feynman's propagation constant

$$K(x,y,x_0,y_0,z,0)=\frac{i}{2\pi}\frac{1}{\sqrt{\sin(\beta_x z)\sin(\beta_y z)}}\exp\left\{\frac{-i}{2}\left[\frac{x^2+x_0^2}{\tan(\beta_x z)}-\frac{2x_0x}{\sin(\beta_x z)}\right]\right\}$$
$$\exp\left\{\frac{-i}{2}\left[\frac{y^2+y_0^2}{\tan(\beta_y z)}-\frac{2y_0y}{\sin(\beta_y z)}\right]\right\}. \quad (2.3.121)$$

To obtain the propagation through a QWP rotated 45°, we select the phase propagation difference to be $\beta_y z-\beta_x z=\pi/2$, and we use the rotated axis of the QWP as the coordinate system

$$\begin{pmatrix} x_H \\ x_V \end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}. \quad (2.3.122)$$

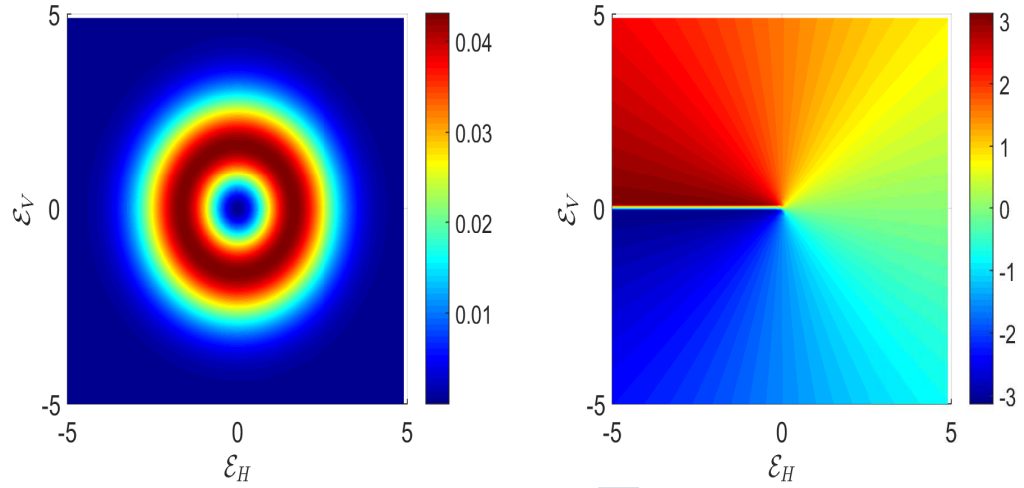
Therefore, calculating the propagation integral (2.3.120), we obtain the following state

$$\Psi(x_H,x_V)=\frac{1}{\sqrt{\pi}}\frac{x_H-ix_V}{\cosh 2r-\cos\phi\sinh 2r}\exp\left\{-\frac{1}{2}\frac{1-\eta}{1+\eta}\left(x_H^2+x_V^2\right)\right\}. \quad (2.3.123)$$

Unlike the local vortex, this state is always a vortex, regardless of the propagation plane. So we have a *global* vortex state. If we calculate its spin,

$$\langle L_z\rangle=\int\int\Psi^* L_z\Psi\,dx_H\,dx_V=-\hbar, \quad (2.3.124)$$

we see that it carries actual momentum and that it is independent of the squeezing.



(a) Probability density. (b) Phase density.

Figure 2.3.7: Global vortex with $r = 0.5, \phi = 0$.

2.3.2.1.2 Employing SPDC type II

Since we are working with polarization modes, type II SPDC can also be employed to obtain our vortex state, as shown in Figure 2.3.8. Using a beam splitter with low reflectivity followed by a PBS and two detectors, we can subtract a single photon in a polarization mode. In this way,

$$\hat{P}\,\hat{B}_H\,\hat{B}_V\,\hat{S}_{1H2V}(\xi)\,\hat{S}_{1V2H}(-\xi)\,|0\rangle\,, \tag{2.3.125}$$

where $\hat{S}_{1H2V}(\xi)\,\hat{S}_{1V2H}(-\xi)$ is the SPDC type II operator (2.1.31), $\hat{B}_i$ is the BS operator for (2.2.36) different polarizations and $\hat{P}$ is the PBS operator (2.2.38). The BS operator can be approximated as

$$\hat{B}_i = e^{-\tan\frac{\theta}{2}\hat{a}_{2i}\hat{a}^\dagger_{3i}} e^{-\ln\left(\cos^2\frac{\theta}{2}\right)\left(\hat{a}^\dagger_{3i}\hat{a}_{3i}-\hat{a}^\dagger_{2i}\hat{a}_{2i}\right)} e^{-\tan\frac{\theta}{2}\hat{a}^\dagger_{2i}\hat{a}_{3i}} \approx e^{-\tan\frac{\theta}{2}\hat{a}_{2i}\hat{a}^\dagger_{3i}} t^{\hat{a}^\dagger_{2i}\hat{a}_{2i}}, \tag{2.3.126}$$

and so, if the BS has a very low reflection coefficient ($t \approx 1$), the BS operators can be approximated to order one as

$$\hat{B}_H \cdot \hat{B}_V = \left(1 - \frac{r}{t}\hat{a}^\dagger_{2H}\hat{a}_{2H}\right)\left(1 - \frac{r}{t}\hat{a}^\dagger_{2V}\hat{a}_{2V}\right) \approx 1 - \frac{r}{t}\left(\hat{a}^\dagger_{2H}\hat{a}_{2H} + \hat{a}^\dagger_{2V}\hat{a}_{2V}\right). \tag{2.3.127}$$

Taking into account the PBS in the detectors ($\hat{a}^\dagger_{2H} = \hat{a}^\dagger_{3H}$, $\hat{a}^\dagger_{2V} = \hat{a}^\dagger_{4V}$), we have

$$|\Psi\rangle \approx \left[1 - \frac{r}{t}\left(\hat{a}^\dagger_{3H}\hat{a}_{2H} + \hat{a}^\dagger_{4V}\hat{a}_{2V}\right)\right]\hat{S}_{1H2V}(\xi)\,\hat{S}_{1V2H}(-\xi)\,|0\rangle\,. \tag{2.3.128}$$

Now, if we employ another PBS to join both modes (as shown in Figure 2.3.8), we are going to obtain a local vortex like (2.3.115) in one of the PBS outputs, while we obtain

squeezed vacuum in the other. Depending which detector (D_H or D_V) makes click, the generated states will be

$$\langle 1_{3H}|\Psi\rangle = \hat{a}_{bH}\hat{S}_{a(H,V)}(\xi)\,\hat{S}_{b(H,V)}(-\xi)\,|0\rangle\,, \tag{2.3.129a}$$

$$\langle 1_{4V}|\Psi\rangle = \hat{a}_{aV}\hat{S}_{a(H,V)}(\xi)\,\hat{S}_{b(H,V)}(-\xi)\,|0\rangle\,. \tag{2.3.129b}$$

For example, if we detect a photon in detector D_V (2.3.129b) we obtain the state

$$\Psi = \frac{\sqrt{2}e^{i\phi}\left(x_{aH}-\eta_a x_{aV}\right)}{\left(1-\eta_a^2\right)^{3/2}\pi^{1/2}\cosh^2 r}\exp\left\{\frac{2x_{aH}x_{aV}\eta_a-\left(x_{aH}^2+x_{aV}^2\right)\eta_a^2}{1-\eta_a^2}-\frac{1}{2}\left(x_{aH}^2+x_{aV}^2\right)\right\}$$
$$\cdot\frac{1}{\sqrt{(1-\eta_b^2)\pi\cosh^2 r}}\exp\left\{\frac{2x_{bH}x_{bV}\eta_b-\left(x_{bH}^2+x_{bV}^2\right)\eta_b^2}{1-\eta_b^2}-\frac{1}{2}\left(x_{bH}^2+x_{bV}^2\right)\right\}. \tag{2.3.130}$$

Like we did before, using QWPs, rotated 45° respect the polarization axis, in both outputs and applying propagation we get the global vortex

$$\Psi_F = \frac{1}{\sqrt{\pi}}\frac{x_{bH}\pm ix_{bV}}{\left(\cosh 2r-\cos\phi\sinh 2r\right)^{3/2}}\exp\left\{-\frac{1}{2}\frac{1+\eta}{1-\eta}\left(x_{aH}^2+x_{aV}^2+x_{bH}^2+x_{bV}^2\right)\right\}. \tag{2.3.131}$$

As we can see, in output B we obtain a global vortex state with polarization modes, just like with SPDC I (2.3.123), while from output A, squeeze vacuum comes out. If we measure a photon in detector D_H, trivially the states come out by the opposite outputs.

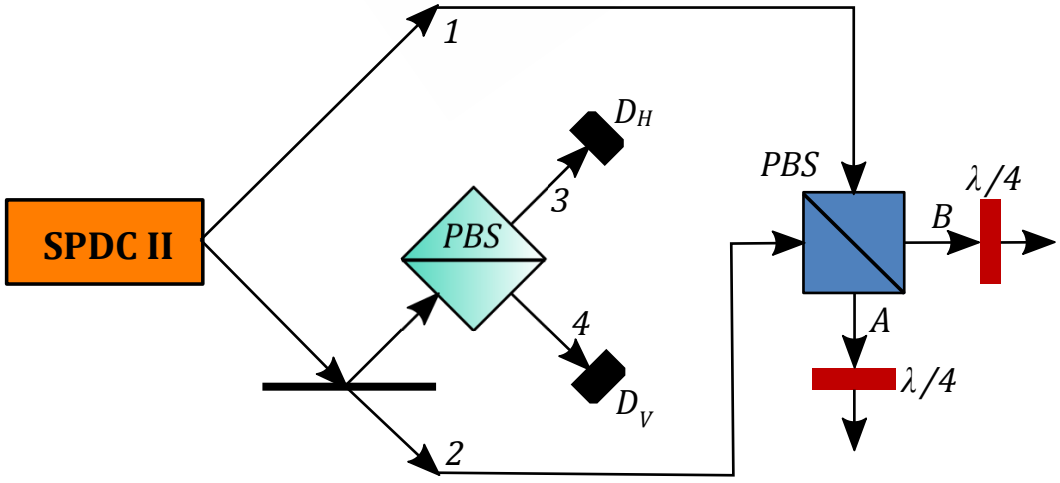


Figure 2.3.8: Obtention of a polarization quantum vortex with SPDC II.

2.3.2.2 Single-photon-subtracted two-mode squeezed state in OAM

The SPDC process shown in subsection 2.3.2.1 can also be used with OAM states generating two modes with opposed moment l. Employing CLCs we can work with HG modes to obtain a squeezed vortex carrying orbital angular momentum.

The scheme of the system is shown on Figure (2.3.9). So, using two CLCs $C_{\pi/2}$ we can convert our LG modes, originated in the SPDC process, to HG modes. Then, instead of a PBS, we can make use of a Mach-Zehnder interferometer with a CLC C_π (MZIC), which allows us to separate two HG modes like the HG_{10} and HG_{01} by introducing a phase difference of π between both. In this way we can extract one photon to one of the modes generating state (2.3.130). Finally, we can join both modes in the same propagation direction using another MZIC and generate a global vortex carrying OAM employing a final CLC ($C_{\pi/2}$). So, we obtain state (2.3.131) but with HG modes $\Psi(x_{10}, x_{01})$.

As we saw before, our state will carry an OAM of $\langle L \rangle = \pm l\hbar$. Case $l = 1$ will be like equation (2.3.124).

In the case that we generate two LG modes of $l = \pm 2$ with SPDC, the first CLC converters turn the into modes HG_{20} and HG_{02}. Extracting a photon in one mode and joining both modes with a MZIC, we will obtain the local vortex $\Psi(x_{20}, x_{02})$ in one of the outputs (A or B) given by equation (2.3.130), excluding squeezed vacuum. In this case, the MZIC should have a $C_{\pi/2}$ instead to introduce a phase shift π between both modes. If this state crosses a CLC $C_{\pi/2}$ rotated $\pi/4$ respect to the HG modes, we can apply the basis change in equation (A.18) and use Feynman propagation (2.3.120) and we obtain the following state

$$\Psi(x_{20}, x_{11}, x_{02}) = N\left(x_{20} - i\sqrt{2}x_{11} - x_{02}\right)\exp\left\{\frac{1-\eta}{1+\eta}x_{20}x_{02}\right\}. \tag{2.3.132}$$

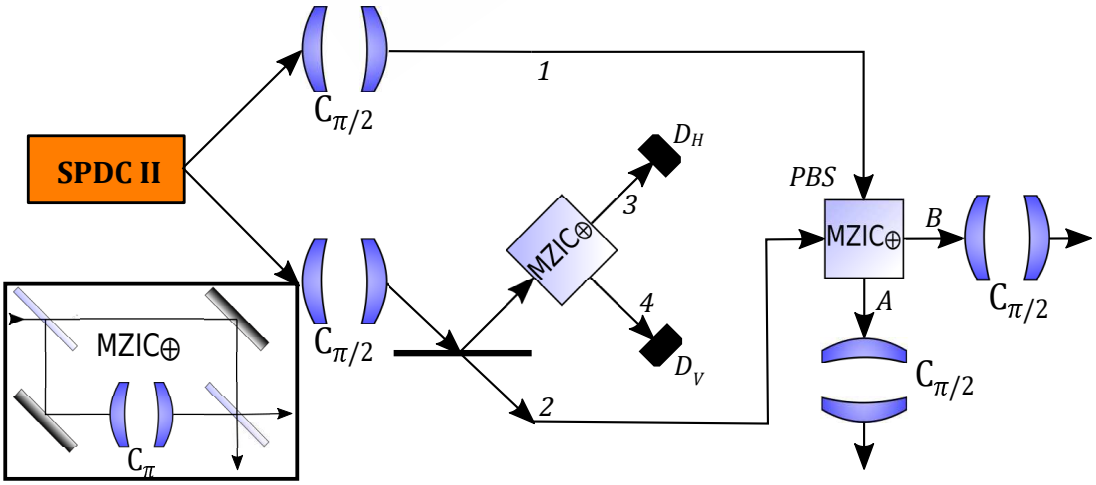


Figure 2.3.9: SPDC to generate a vortex state with HG modes.

2.3.3 Generating quantum vortex squeezed states in integrated devices with FAM

The major research of our group has been focused on integrated optics [Liñares Beiras et al., 2011]. In the last years, several theoretical and applied quantum studies have been made about both linear and non-linear integrated optical devices. To begin with, our group has previously realized quantum analysis of the generalized polarization properties of multimode single-photon states [Liñares et al., 2011] and multi-photon states [Barral et al., 2013] in directional couplers. They are based on the OFS probability distributions in such a way that generalized polarization is understood as a significant confinement of the probability distribution along certain regions of the multidimensional OFS space. These states can constitute FAM vortex states in the OFS space. Besides, it has been theorised how to obtain a perfect quantum optical vortex [Barral and Liñares, 2017] within a non-linear medium suitably engineered.

Moreover, a reconfigurable integrated device for manipulation and detection of two-mode spatial quantum states of light through the reconstruction of the OFS probability distribution via homodyne detection [Barral et al., 2015] has been proposed. Another integrated device designed to generate both coherent and squeezed Bell-like states was proposed in [Barral and Liñares, 2016]. Both devices have great potential for quantum information processing purposes, including cryptography.

In this section, we are going to present two novelty works about integrated devices for the generation of vortex quantum states that have been published [Barral et al., 2016,Barral et al., 2017]. In them, we basically employ a similar process to the one shown in section 2.3.2 to generate vortex states in integrated devices. To achieve this we have to use a periodic poled grating to generate a squeezed state.

2.3.3.1 Non reconfigurable integrated device

An integrated device that works in a identical way to the bulk devices explained before, but with integrated waveguide modes was proposed in the article *Generation and Detection of Continuous Variable Quantum Vortex States via Compact Photonic Devices* published on *Photonics* **4** in 2017, that is annexed as section P1 [Barral et al., 2017].

The device is shown in Figure 2.3.10. This device can be divided in two stages. The first stage is devoted to the generation of the quantum state and pump suppression. A pump is introduced in the integrated device through a waveguide. Then a Y junction separates the pump into two modes, which cross a periodically poled zone generating two single-mode squeezed states (1 & 2). Then, the pump is filtered by means of two wavelength-dependent directional couplers (F_1 & F_2). So, at the end of this stage we have state

$$|\Psi\rangle = \hat{S}_1(r)\hat{S}_2(r)|0_1\,0_2\rangle. \tag{2.3.133}$$

As we need a bimodal squeezing between modes as in previous sections, a directional coupler is required in order to entangle both modes (C_1). Next, we employ two weak

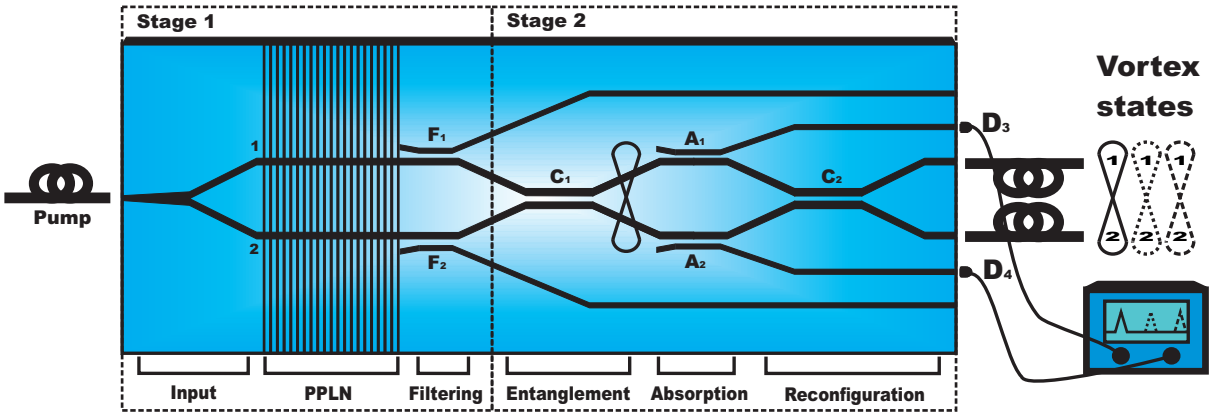


Figure 2.3.10: Non reconfigurable vortex integrated device.

couplers (A_1 & A_2) to subtract a single or n photons of any of the modes. This will give us a local vortex of order n

$$|\Psi\rangle \propto \hat{a}^n_{1|2}\hat{S}_{12}(r)|0_1\,0_2\rangle. \tag{2.3.134}$$

To obtain a global vortex, one last coupler is required to reconfigure the state as we have already seen previously

$$|\Psi\rangle \propto \left(\hat{a}^\dagger_1 \pm i\hat{a}^\dagger_1\right)^n \hat{S}_1(r)\hat{S}_2(r)|0_1\,0_2\rangle. \tag{2.3.135}$$

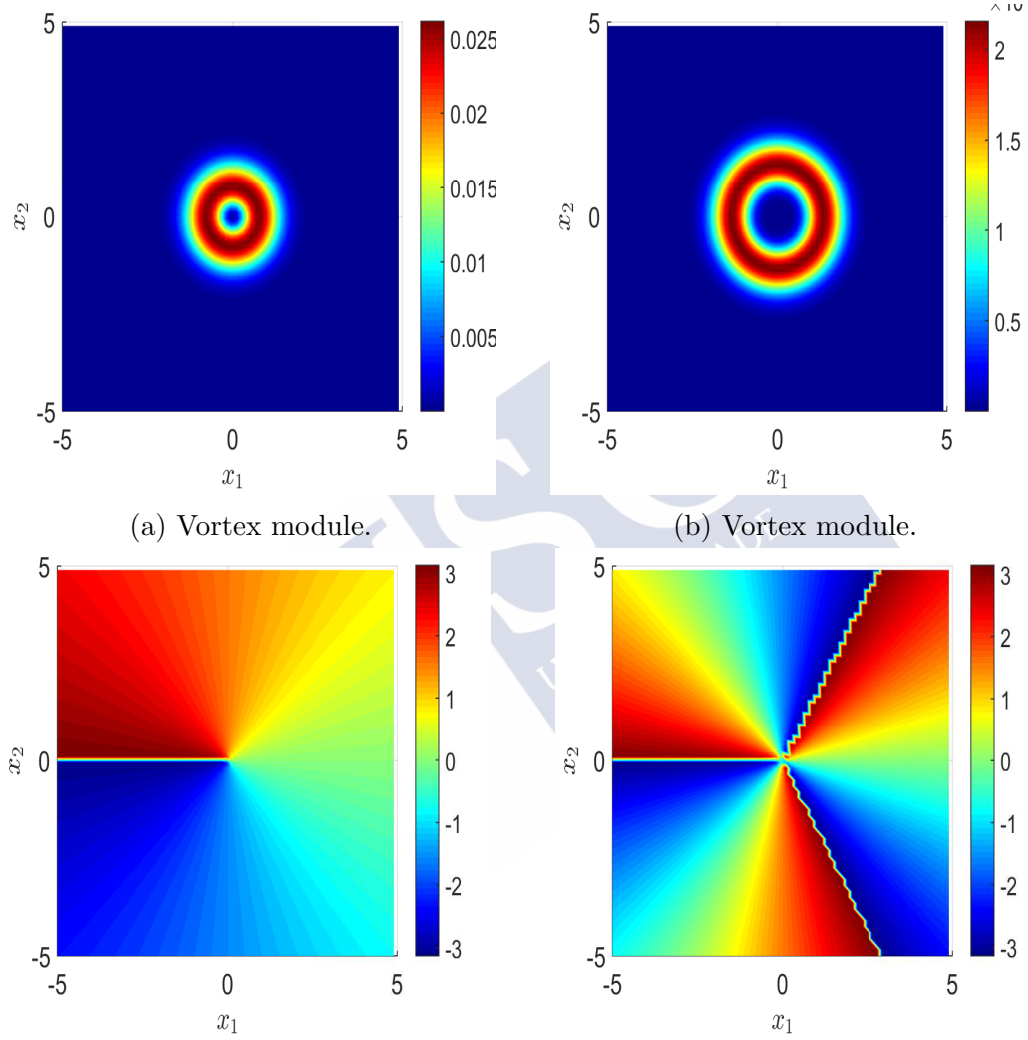
So we are going to obtain the following generic vortex state of order n

$$\Psi_{n_\pm}(x_1,x_2) = \langle x_1\,x_2|\Psi_E\rangle = \frac{1}{\sqrt{\pi\,n!\;e^{2(1+n)r}}}(x_1 \pm ix_2)^n e^{-\frac{x_1^2+x_2^2}{2e^{2r}}}. \tag{2.3.136}$$

We represent state (2.3.136) for orders $n = 1$ and $n = 3$ in Figure. 2.3.11. In the figure, we can observe how the size of the vortex grows with the order. At the same time, the order is manifested in the number of 2π cycles that the phase completes by 2π rotation in the azimuthal angle. Moreover, calculating the FAM of this state, we can see that it depends of the order as well:

$$\langle L_F\rangle = \int\int \Psi^* L_F \Psi\, dx_H\, dx_V = \pm n\hbar, \tag{2.3.137}$$

The full analysis of this device can be shown in the published article that is annexed as section P1.



(a) Vortex module.

(b) Vortex module.

(c) Vortex phase.

(d) Vortex phase.

Figure 2.3.11: Plots of probability (upper) and phase (lower) densities of quantum vortices of order $n = 1$ (left) and $n = 3$ (right) with a squeezing factor $r = 0.25$.

2.3.3.2 Reconfigurable integrated device

Another integrated device for generating vortex states, but designed to be actively reconfigurable and not passive, was proposed in the article *Engineering continuous and discrete variable quantum vortex states by non-local photon subtraction in a reconfigurable photonic chip* published on *Journal of the Optical Society of America B* **33** (11) in 2016, that is annexed as section P2 [Barral et al., 2016].

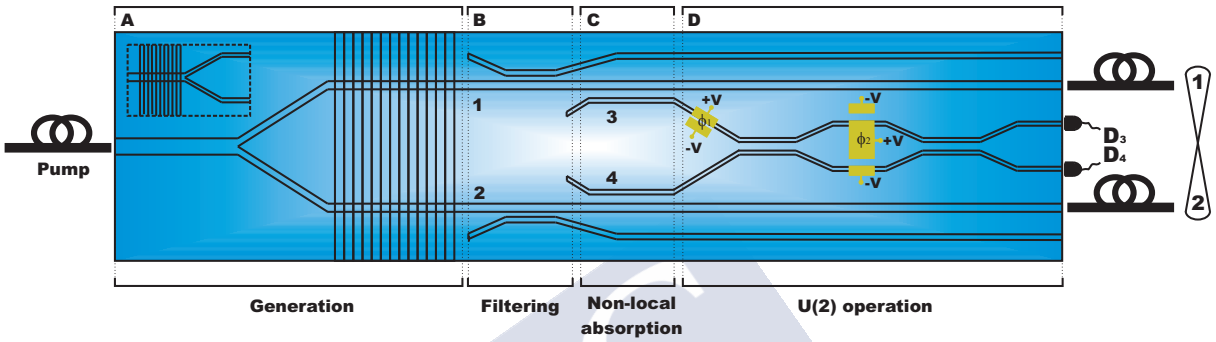


Figure 2.3.12: Reconfigurable vortex integrated device.

The device is shown in Figure. 2.3.12. It is quite similar to the device explained in the previous section but with some differences. Stages A and B from 2.3.12 correspond to stage 1 from 2.3.10, where the quantum state is generated by squeezing a pump divided in two modes through a periodically poled grating (A) and being filtered by two DCs (B). Once again we obtain state (2.3.133)

$$|\Psi_B\rangle = \hat{S}_1(\xi)\hat{S}_2(\xi)|0_\xi\, 0_2\rangle. \tag{2.3.138}$$

Stage 2 is, however, different in both devices. While in the previous one we have an entanglement DC before the DCs destined to absorb photons, in this device stage C consists of two DCs of high transmitivity that absorb single photons from channels 1 and 2 to the auxiliary waveguides 3 and 4 respectively.

$$|\Psi_C\rangle = \hat{C}_{\kappa z_{13}}\hat{C}_{\kappa z_{24}}\hat{S}_1(\xi)\hat{S}_2(\xi)|0_1\, 0_2\, 0_3\, 0_4\rangle \propto \hat{a}_{1|2}\hat{a}^\dagger_{3|4}\hat{S}_1(\xi)\hat{S}_2(\xi)|0_1\, 0_2\, 0_3\, 0_4\rangle, \tag{2.3.139}$$

where $\hat{C}_{\kappa z}$ is given by (2.2.48).

Finally, an entanglement operation in the auxiliary channels is made in stage D. This stage is a MZI in auxiliary waveguides 3 and 4, consisting of two DCs alternated between two phase shifters (ϕ_1 and ϕ_2) consists of two DCs forming a MZI in waveguides 3 and 4, with followed by two detectors to detect the extracted photon. Thus, we have state

$$|\Psi_D\rangle = \hat{U}_{34}\hat{C}_{\kappa z_{13}}\hat{C}_{\kappa z_{24}}\hat{S}_1(\xi)\hat{S}_2(\xi)|0_1\, 0_2\, 0_3\, 0_4\rangle, \tag{2.3.140}$$

where the MZI operator can be written as

$$\hat{U}_{34} = e^{i\frac{\phi_2}{2}i(\hat{a}_3\hat{a}_4^\dagger - \hat{a}_3^\dagger\hat{a}_4)}e^{i\frac{\phi_1}{2}(\hat{a}_3^\dagger\hat{a}_3 - \hat{a}_4^\dagger\hat{a}_4)}. \tag{2.3.141}$$

As channels 1 and 3, as well as, 2 and 4, are respectively entangled. The U(2) entanglement operation in channels 3 and 4 also generates an entanglement between main channels 1 and 2.

As explained in detail in subsections P2.2.1 and P2.2.2 respectively of our paper P2, using the disentangling theorem [Kim, 2008] and the Bogoliubov transformation [Agarwal, 2012], we can calculate expression (2.3.140). Depending in which single-photon detector (3 or 4) makes a measure, we will obtain the states (P2.17)

$$\langle 1_3 0_4|\Psi_D\rangle = |1_{\xi 1} 0_{\xi 2}\rangle - \eta \tan(\phi_2/2) e^{-i\phi_1} |0_{\xi 1} 1_{\xi 2}\rangle , \tag{2.3.142a}$$

$$\langle 0_3 1_4|\Psi_D\rangle = |1_{\xi 1} 0_{\xi 2}\rangle - \eta \cot(\phi_2/2) e^{-i\phi_1} |0_{\xi 1} 1_{\xi 2}\rangle , \tag{2.3.142b}$$

where $|0_\xi\rangle = \hat{S}(\xi)|0\rangle$ is the vacuum squeezed state and $|1_\xi\rangle = \hat{S}(\xi)|1\rangle$ is a single-photon squeezed state. Moreover, by lowering the original pump, it is possible to obtain single-photon states, which are very useful in discrete variable QKD, as we are going to see in next section.

Establishing $\phi_1 = (2n-1)\pi/2$, we will have an elliptical squeezed vortex state that, in the case that we detect a photon on detector 3 (2.3.142a) is given in the OFS by

$$\Psi(x_1, x_2) = \sqrt{\frac{2}{\pi \left(1 + \eta^2 \tan(\phi_2/2)^2\right) e^{4r}}} (x_1 - i\eta \tan(\phi_2/2) x_2) e^{-\frac{x_1^2 + x_2^2}{2e^{2r}}} . \tag{2.3.143}$$

If we choose $\phi_2 = 2 \arctan \eta^{-1}$ we obtain the quantum vortex state generated by our previous device for $n = 1$ (2.3.136), which is shown on Figure 2.3.11.

The full analysis of this device can be shown in the published article that is annexed as section P2.

2.4 Discrete variable quantum key distribution with vortex states

In the previous subsections, we studied the properties and how to generate quantum vortex states of light. These entangled states present high potential in different applications of QIP. For instance, as squeezed states they could be employed in continuous variable quantum key distribution (CV-QKD) [Cerf et al., 2001, Gottesman and Preskill, 2003, García-Patrón and Cerf, 2009]. Moreover, as quantum vortex are analogous to spatial classical vortex (and can actually coincide with them, as shown before), these states can constitute a high dimensional Hilbert base to implement discrete variable quantum key distribution (DV-QKD), making use of their vorticity order and abstract handedness, as done with OAM states [Mafu et al., 2013].

However, in the rest of this thesis, we are going to focus on single-photon DV-QKD Specifically, we are going to implement high dimensional BB84 protocols. Vortex states fulfil an important role in such protocol as they constitute the basis to generate mutually unbiased basis (MUBs), which are required to implement it. As we will see, our devices proposed in [Barral et al., 2017] (section P1) and [Barral et al., 2016] (section P2) can operate as natural generators of all possible single-photon states belonging to any of the MUBs.

2.4.1 Mutually unbiased basis

The BB84 protocol is based in the utilization of quantum states belonging to mutually unbiased bases (MUBs). A MUB set is a collection of K quantum state bases for a Hilbert space of dimension D,

$$\left\{ |\varphi\rangle_{1(k)}, ..., |\varphi\rangle_{D(k)} \right\}, \tag{2.4.144}$$

with $k = 1, ..., K$ and $2 \leq K \leq D$, whose inner product between any of the possible $K \cdot D$ states satisfies

$$|\langle \varphi_{i(k)} | \varphi_{j(k')} \rangle|^2 = \begin{cases} \frac{1}{D} & \text{if} \quad k \neq k' \quad \forall\, i,j = 1, ..., D \\ \delta_{ij} & \text{if} \quad k = k' \quad \forall\, i,j = 1, ..., d \end{cases} \tag{2.4.145}$$

Theoretically, for dimension D there can be a maximum of $D + 1$ MUBs that can be created simultaneously [Bengtsson, 2007, Bengtsson et al., 2007].

Vortex states can be used as one of the MUBs for dimension $D = 2$ while using a linear basis as the other. In this way, and taking into account [Klappenecker and Rötteler, 2003], a MUB set for $D = 2$ will be

$$\mathcal{B}_1^{(2)} = \left\{ \frac{1}{\sqrt{2}}(1,1);\ \frac{1}{2}(1,-1) \right\}, \tag{2.4.146a}$$

$$\mathcal{B}_2^{(2)} = \left\{ \frac{1}{\sqrt{2}}(1,i);\ \frac{1}{2}(1,-i) \right\}, \tag{2.4.146b}$$

where $\mathcal{B}_1^{(2)}$ is the linear base and $\mathcal{B}_2^{(2)}$ is the vortex base for dimension $D = 2$.

It has been shown [Klappenecker and Rötteler, 2003, Tselniker et al., 2009] that it is possible to obtain MUBs of higher dimensions, in particular, MUBs for dimension $D = 2^n$, by using tensorial products and some phase shifts between the 2-dimensional basis (2.4.146). In this way, for dimension $D = 4$ we have the following MUB set

$$\mathcal{B}_1^{(4)} = \mathcal{B}_1^{(2)} \otimes \mathcal{B}_1^{(2)} = \left\{ \frac{1}{2}(1,1,1,1);\ \frac{1}{2}(1,-1,1,-1);\ \frac{1}{2}(1,1,-1,-1);\ \frac{1}{2}(1,-1,-1,1) \right\}, \tag{2.4.147a}$$

$$\mathcal{B}_2^{(4)} = \mathcal{B}_2^{(2)} \otimes \mathcal{B}_2^{(2)} = \left\{ \frac{1}{2}(1,i,i,-1);\ \frac{1}{2}(1,-i,i,1),\ \frac{1}{2}(1,i,-i,1);\ \frac{1}{2}(1,-i,-i,-1) \right\}, \tag{2.4.147b}$$

$$\mathcal{B}_3^{(4)} = \Gamma \cdot \mathcal{B}_1^{(2)} \otimes \mathcal{B}_2^{(2)} = \left\{ \frac{1}{2}(1,i,1,-i);\ \frac{1}{2}(1,-i,1,i);\ \frac{1}{2}(1,i,-1,i);\ \frac{1}{2}(1,-i,-1,-i) \right\}, \tag{2.4.147c}$$

$$\mathcal{B}_4^{(4)} = \Gamma \cdot \mathcal{B}_1^{(2)} \otimes \mathcal{B}_2^{(2)} = \left\{ \frac{1}{2}(1,1,i,-i);\ \frac{1}{2}(1,-1,i,i);\ \frac{1}{2}(1,1,-i,i);\ \frac{1}{2}(1,-1,-i,-i) \right\}, \tag{2.4.147d}$$

where Γ is a phase shift matrix given by

$$\Gamma = \operatorname{diag}(1,1,1,-1)\,. \tag{2.4.148}$$

Going up to dimension $D = 8$, a set of eight MUBs can be constructed as follows

$$\begin{aligned}
\mathcal{B}_1^{(8)} &= \mathcal{B}_1^{(2)} \otimes \mathcal{B}_1^{(2)} \otimes \mathcal{B}_1^{(2)}, \\
\mathcal{B}_2^{(8)} &= \mathcal{B}_2^{(2)} \otimes \mathcal{B}_2^{(2)} \otimes \mathcal{B}_2^{(2)}, \\
\mathcal{B}_3^{(8)} &= \Gamma_1 \cdot \mathcal{B}_1^{(2)} \otimes \mathcal{B}_1^{(2)} \otimes \mathcal{B}_2^{(2)}, \\
\mathcal{B}_4^{(8)} &= \Gamma_1 \cdot \mathcal{B}_2^{(2)} \otimes \mathcal{B}_2^{(2)} \otimes \mathcal{B}_1^{(2)}, \\
\mathcal{B}_5^{(8)} &= \Gamma_2 \cdot \mathcal{B}_1^{(2)} \otimes \mathcal{B}_2^{(2)} \otimes \mathcal{B}_1^{(2)}, \\
\mathcal{B}_6^{(8)} &= \Gamma_2 \cdot \mathcal{B}_2^{(2)} \otimes \mathcal{B}_1^{(2)} \otimes \mathcal{B}_2^{(2)}, \\
\mathcal{B}_7^{(8)} &= \Gamma_3 \cdot \mathcal{B}_1^{(2)} \otimes \mathcal{B}_2^{(2)} \otimes \mathcal{B}_2^{(2)}, \\
\mathcal{B}_8^{(8)} &= \Gamma_3 \cdot \mathcal{B}_2^{(2)} \otimes \mathcal{B}_1^{(2)} \otimes \mathcal{B}_1^{(2)},
\end{aligned} \tag{2.4.149}$$

where Γ_i represents phase shifts

$$\begin{aligned}
\Gamma_1 &= \operatorname{diag}(1,1,1,1,1,-1,-1,1)\,, \\
\Gamma_2 &= \operatorname{diag}(1,1,1,-1,1,-1,1,1)\,, \\
\Gamma_3 &= \operatorname{diag}(1,1,1,-1,1,1,-1,1)\,.
\end{aligned} \tag{2.4.150}$$

For example, the MUB pair formed by the direct tensorial product of the 2-dimensional basis (2.4.146) would be

$$\mathcal{B}_1^{(8)} = \mathcal{B}_1^{(2)} \otimes \mathcal{B}_1^{(2)} \otimes \mathcal{B}_1^{(2)} = 2^{-3/2} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}, \quad (2.4.151a)$$

$$\mathcal{B}_2^{(8)} = \mathcal{B}_2^{(2)} \otimes \mathcal{B}_2^{(2)} \otimes \mathcal{B}_2^{(2)} = 2^{-3/2} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ i & -i & i & -i & i & -i & i & -i \\ i & i & -i & -i & i & i & -i & -i \\ -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ i & i & i & i & -i & -i & -i & -i \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ -i & i & i & -i & i & -i & -i & i \end{pmatrix}, \quad (2.4.151b)$$

where each column is a vector of the basis $\mathcal{B}_1^{(8)}$ and $\mathcal{B}_2^{(8)}$.

Finally, any MUB set of dimension $D = 2^n$ can be created following the same method and obtaining by the MUB properties (2.4.145) the appropriated Γ_i. It is important to note that the BB84 protocol does not require to employ all the possible basis for dimension D and instead, while using them improves security, it also decreases the transmission rate as the number of times that Alice and Bob use the same basis (only case that allows to generate key) is reduced. Therefore, two basis can be perfectly employed and, as we have seen, basis $\mathcal{B}_1^{(2^n)}$ and $\mathcal{B}_2^{(2^n)}$ of dimension $N = 2^n$ can always be factorized as follows

$$\mathcal{B}_1^{(2^n)} = \mathcal{B}_1^{(2)} \otimes \mathcal{B}_1^{(2)} \otimes ... \otimes \mathcal{B}_1^{(2)}, \quad (2.4.152a)$$

$$\mathcal{B}_2^{(2^n)} = \mathcal{B}_2^{(2)} \otimes \mathcal{B}_2^{(2)} \otimes ... \otimes \mathcal{B}_2^{(2)}, \quad (2.4.152b)$$

where $\mathcal{B}_i^{(2)}$ is the corresponding basis in two dimensions (2.4.146).

2.4.2 Generation of single-photon MUBs with our devices to implement DV-QKD

In our works P1 and P2, we designed two devices to generate quantum vortex states of light with integrated path modes, as shown in subsection 2.3.3. These vortex states (2.3.142) can be reduced to single-photon states. As explained in subsection P2.2.3 of our paper P2, by lowering the power of the input pump, our device generates the states P2.25

$$\langle 1_3 0_4 | \Psi_D \rangle \propto |1_1 0_2\rangle - \eta \, \tan(\phi_2/2) e^{-i\phi_1} |0_1 1_2\rangle, \tag{2.4.153a}$$

$$\langle 0_3 1_4 | \Psi_D \rangle \propto |1_1 0_2\rangle + \eta \, \cot(\phi_2/2) e^{-i\phi_1} |0_1 1_2\rangle. \tag{2.4.153b}$$

Now, if we fix the second phase shifter of the device in such a way that it always applies a phase $\phi_2 = 2 \arctan(\eta^{-1})$ (or $\phi_2 = 2 \arctan(\eta)$) we will be generating state

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|1_1 0_2\rangle \pm e^{i\phi_1} |0_1 1_2\rangle \right), \tag{2.4.154}$$

where the sign $\mp$ depends on detection of detectors 3 and 4 from Figure P2.1 respectively. To ensure that we always obtain this state independently of the detection there should be no squeezing on the generation ($r = 0$) $\eta = 1$, which means that the second phase shifter should introduce $\phi_2 = \pi/2$. Therefore, the device would only have an active phase shifter (ϕ_1).

By adjusting the applied phase ϕ_1, we can generate the four states that constitute two MUBs for dimension 2 (2.4.146). These states could be obtained by implementing phases $\phi_1 = \left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$. However, the device itself already randomly applies a phase π, as explained and seen in (2.4.154). This an important fact because it means that our device is generating totally random qubits $|0\rangle = \left(|1_1\rangle + e^{i\phi_2} |1_2\rangle\right)/\sqrt{2}$ and $|1\rangle = \left(|1_1\rangle - e^{i\phi_2} |1_2\rangle\right)/\sqrt{2}$ on its own without the emitter (Alice) having to randomly select them. Instead, in order to apply the BB84 protocol, phase ϕ_1 has to be randomly modified between values 0 or $\pi/2$. This selects the basis where the qubits are encoded, either the vortex basis or the linear one.

Hence, between its many possible applications, our proposed device in [Barral et al., 2016] can work as a generator of single-photon qubit states in spatial path modes to implement DV-QKD. Its operation has several advantages. To begin with, it warns every time that a new state is generated. Moreover, if photon number resolving (PNR) detectors are used in it, we know if the emitted state is truly single-photon or if a multi-photon state has been emitted instead. This is advantageous because it allow us to prevent against possible attacks like the photon-number splitting attack [Lütkenhaus and Jahma, 2002]. Another advantage of our device resides in the already mentioned random generation of qubits $|0\rangle$ and $|1\rangle$. Thus, it is not necessary to use a pseudo-random algorithm or even true random number generators [Bahadur et al., 2016] to generate bits, although one for basis choice is still needed. Besides, this randomness in the bit coding helps as well

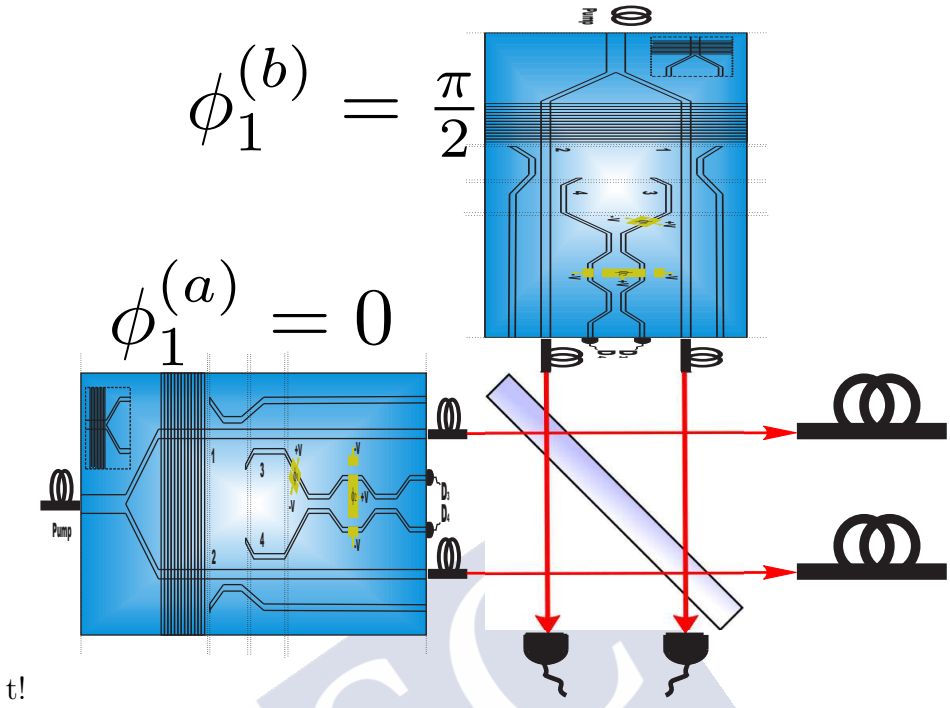


Figure 2.4.13: Generator system to randomly produce the four states belonging to the MUB of dimension 2.

to protect against possible side channel attacks that an eavesdropper can implement on the the generator to gain information by, for example, attacking the phase shifter with a bright pulse and analysing its effects [Jain et al., 2014]. If the eavesdropper could know the phase used to encode a bit, the bit itself would be known. In our generator, only the base is encode through a phase shift, which still would give the eavesdropper enough information to perform a measure. However, in our case, the phase shifter ϕ_1 is located in the auxiliary waveguides of the device and so, it is not easily accessible. Thus, it becomes difficult for an eavesdropper to perform a trojan-horse attack on the generator.

Furthermore, if we want to generate the four different states (2.4.146) in a truly random way, two devices with fixed phase shifts of $\phi_1^{(a)} = 0$ and $\phi_1^{(b)} = \pi/2$ could be arranged at the inputs of a beam splitter system, with detectors and fibers in the outputs, as shown on Figure 2.4.13. In this way, each device generates states in its particular base which are then sent, or not, through the fiber. We know the state generated by the click obtained in one of the four detectors in our devices. Half of the total states generated are going to get lost in the beam splitter. By putting detectors in the unused output of the BS, we can detect the lost states to discern them from the actually sent ones. Nonetheless, with two identical pump pulses in each device, twice as many states are also being generated and so, the effective generation rate is similar to the single case. Thus, this scheme is able to generate the four states (2.4.146) in a fully random way without loss of generation rate.

In conclusion, our designed device explained in paper P2 is a useful generator of single-photon qubits to perform the BB84 protocol. In addition, SAM and OAM vortex generators proposed in subsection 2.3.2 could be used as MUBs generators in a similar way, by lowering the pump and actively modifying the final waveplates and CLCs respectively.

2.4.3 Generation of MUBs of higher dimension

Now, if we want to generate MUBs in more dimensions, we will need to make use of directional couplers in order to rise the dimension of our vortex state. So, if we take into account the quantum transformation of a coupler (2.2.49) for the case $\kappa z = \frac{\pi}{4}$, we have that a single-photon state in waveguide A will be transformed by a DC between waveguides A and B like

$$|1_{A0}\rangle = \frac{1}{\sqrt{2}}\left(|1_A\rangle + ie^{i\phi_2'}|1_B\rangle\right), \tag{2.4.155}$$

where $\delta_f = \phi_2'$ is the phase added at output B from the detector. Therefore, taking (2.4.155) into our generated state (2.4.154) for both waveguides 1 and 2, we obtain

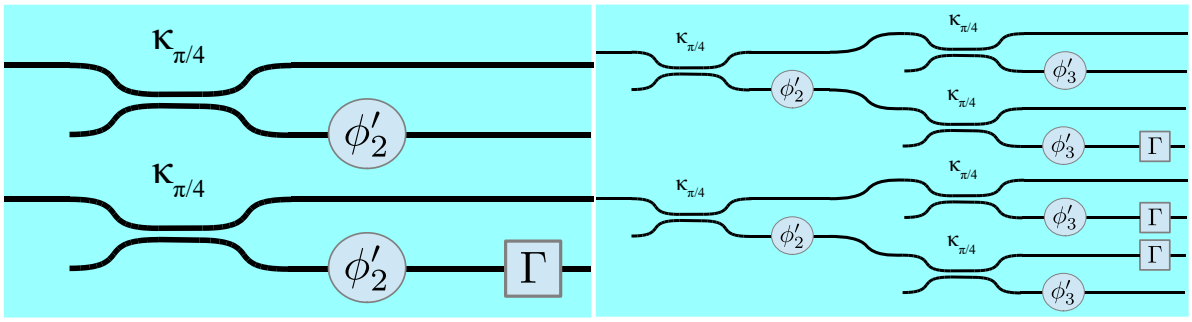
$$|\Psi\rangle = \frac{1}{2}\left(|1_{1A}\rangle + ie^{i\phi_2'}|1_{1B}\rangle \pm e^{-i\phi_1}|1_{2A}\rangle \pm ie^{i(\phi_2'-\phi_1+\gamma)}|1_{2B}\rangle\right), \tag{2.4.156}$$

where γ is an additional phase introduced in the last waveguide which can take values $0, \pi$, corresponding to the phase shifter Γ (2.4.148). Modifying phases ϕ_1 and ϕ_2', it is possible to generate the set of four MUBs in four dimensions (2.4.147). The required phases to obtain these four basis are shown on Table 2.2, while the device is shown on Figure 2.4.14(a).

Table 2.2: Phase values for each MUB fro $D = 4$.

	$\mathcal{B}_1^{(4)}$	$\mathcal{B}_2^{(4)}$	$\mathcal{B}_3^{(4)}$	$\mathcal{B}_4^{(4)}$
ϕ_1	$0, \pi$	$\mp\frac{\pi}{2}$	$0, \pi$	$\mp\frac{\pi}{2}$
ϕ_2'	$\pm\frac{\pi}{2}$	$0, \pi$	$0, \pi$	$\pm\frac{\pi}{2}$
γ	0	0	π	π

By fixing γ, each of the four possible pairs of values from phases ϕ_1 and ϕ_2' corresponds to each of the states from (2.4.147). However, due to the random π phase that generates our original device, phase shift ϕ_1 only needs to change between values $\{0, \pi/2\}$. Therefore, phase γ selects between two pairs of bases (so it can be fixed if only a pair is used), while phase ϕ_1 is responsible of the basis selection and phase ϕ_2' chooses between two pair of states. Once again, the randomness in state generation contributes to the security of the generator device. Moreover, assuming that only two basis are used, the same strategy of designing two different generators for each basis explained in previous subsection 2.4.2 could be employed to add more randomness in the generation process.



(a) Four dimensions. (b) Eight dimensions.

Figure 2.4.14: Device for increasing a guided mode vortex state to four (a) and eight (b) dimensions.

If we go up to dimension $D = 8$, a new set of couplers implementing (2.4.155) are needed, as shown in Figure 2.4.14(b). In this case, we obtain state

$$\begin{aligned} |\Psi\rangle &= |1_{1AA}\rangle + ie^{i\phi'_3}\,|1_{1AB}\rangle + ie^{i(\phi'_2+\gamma_a)}\,|1_{1BA}\rangle - e^{i(\phi'_2+\phi'_3)}\,|1_{1BB}\rangle \\ &\pm e^{-i\phi_1}\,|1_{2AA}\rangle \pm ie^{i(\phi_3-\phi_1+\gamma_b)}\,|1_{2AB}\rangle \pm ie^{i(\phi'_2-\phi_1+\gamma_c)}\,|1_{2BA}\rangle \mp e^{i(\phi'_3+\phi'_2-\phi_1)}\,|1_{2BB}\rangle\,, \end{aligned} \quad (2.4.157)$$

where phases γ_j with $j = a, b, c$ are phases introduced to generate more MUBs,and are dependant of the Γ_i (2.4.150) used. By modifying all the phases ϕ_1, ϕ'_2 and ϕ'_3, as well, as the phase shift Γ_i if required, the MUB set (2.4.149) can be obtained.

Finally, for a general dimension $D = 2^m$, we need to employ a device like the one showed in Figure 2.4.15, which will give us state

$$\begin{pmatrix} 1 \\ \pm e^{-i\phi_1} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ ie^{i\phi'_2} \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 1 \\ ie^{i\phi'_m} \end{pmatrix}. \quad (2.4.158)$$

Like before, the Γ devices shown in Figure 2.4.15 allow to generate all the possible MUBs for the desired dimension. However, they are not needed in case we use the MUB pair $\mathcal{B}_1^{(2^n)}$ and $\mathcal{B}_2^{(2^n)}$ (2.4.152).

A symmetrical pyramidal scheme of coupler arrangement can also be used instead of what is shown on Figures 2.4.14 and 2.4.15. However the different phases of the modes are not going to be ordered following state (2.4.158).

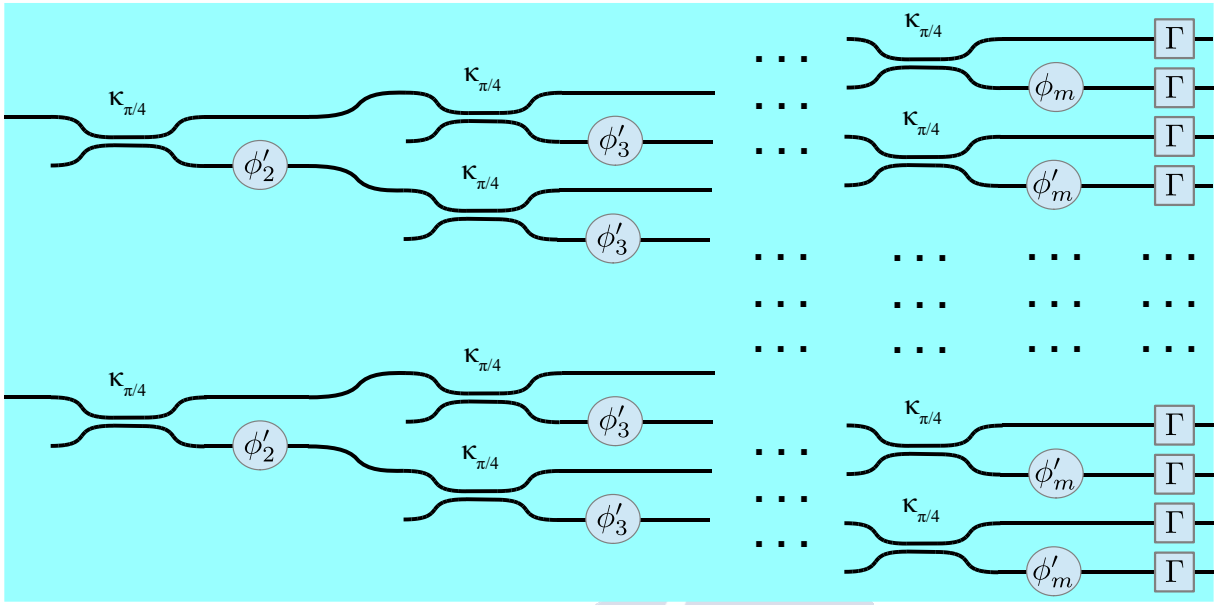


Figure 2.4.15: Device for increasing a guided mode vortex state to 2^m dimensions.

P1 Generation and Detection of Continuous Variable Quantum Vortex States via Compact Photonic Devices

PHOTONICS
VOL. 4 NO. 1 PAGE 2
ISSN: 2304-6732 (ONLINE)
doi: https://doi.org/10.3390/photonics4010002

PUBLISHED 3 JAN 2017

BY DAVID BARRAL[1], DANIEL BALADO[1] & JESÚS LIÑARES[1]

[1] UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Abstract: *A quantum photonic circuit with the ability to produce continuous variable quantum vortex states is proposed. This device produces two single-mode squeezed states which go through a Mach-Zehnder interferometer where photons are subtracted by means of weakly coupled directional couplers towards ancillary waveguides. The detection of a number of photons in these modes heralds the production of a quantum vortex. Likewise, a measurement system of the order and handedness of quantum vortices is introduced and the performance of both devices is analyzed in a realistic scenario by means of the Wigner function. These devices open the possibility of using the quantum vortices as carriers of quantum information.*

P1.1 Introduction

In recent years there has been an increasing interest in the processing of quantum information (QIP) with continuous variables (CV-QIP) [Braunstein and Van Loock, 2005]. CV-QIP protocols are based on gaussian states as resource of entanglement. However, the use of non-gaussian states have been shown to be essential in certain quantum protocols, like the entanglement distillation [Eisert et al., 2002, Fiurášek, 2002, Giedke and Cirac, 2002, Takahashi et al., 2010]. These states are obtained from gaussian states through non-gaussian operations, like the subtraction and addition of photons [Kim, 2008]. This area of research has led to table-top ground-breaking demonstrations like the transition from classical to quantum states by photon addition [Agarwal and Tara, 1991, Zavatta et al., 2004] and the generation of Schrödinger-cat-like states via photon absorption [Dakna et al., 1997, Neergaard-Nielsen et al., 2006], as well as opened new roads in quantum computation and communications [Neergaard-Nielsen et al., 2010, Lee et al., 2011].

However, it is unlikely that any eventual quantum-light-based mainstream technology will be build upon the current bulk optics-based optical circuits. Instead, that technology will be based on practical, low cost, interlinked and tunable components, as those which constitute fiber and integrated optics (IO) [Tanzilli et al., 2012]. In this regard, IO shows unique features for QIP as sub-wavelength stability, essential for quantum interference [Politi et al., 2008]; great miniaturization, indispensable as the level of complexity of the circuit increases [Carolan et al., 2015]; and the optical properties of the waveguide substrates, which enable the generation of quantum states on-chip by means of their enhanced non-linear features [Krapick et al., 2013, Jin et al., 2014, Dutt et al., 2015], its manipulation by means of their thermo-, electro- and strain-optic properties [Martin et al., 2012, Humphreys et al., 2014, Setzpfandt et al., 2016], and the integration of detectors in the circuit [Sahin et al., 2014, Najafi et al., 2015]. In this regard, the implementation of CV-QIP in IO is taking its first steps. Demonstrations of on-chip squeezing up to -4.1 dB in the pulsed wave (PW) regime and -1.83 dB in the continuous wave (CW) regime have been reported [Eto et al., 2008, Kaiser et al., 2016], as well as the first demonstration of CV entanglement on-chip has been recently presented [Masada et al., 2015].

Likewise, the bits of quantum information can be encoded in many different degrees of freedom such as polarization, spatial mode, path, time, orbital angular momentum (OAM) and so on. Due to the continuous nature of the OAM, which gives access to an infinite dimensional Hilbert space, and its easy tailoring with light, the use of single-photon optical vortices for QIP have attracted great attention over the past decades [Molina-Terriza et al., 2007, Fickler et al., 2012]. These quantum states have an analogous in the optical field-strength space: the quantum vortex states, originally proposed in [Agarwal et al., 1997]. These are entangled, non-gaussian and non-classical quantum states, as well as eigenstates of the z component of the abstract angular momentum operator $\hat{L}_z$, in analogy with the quantum eigenstates of the spatial OAM operator, showing order and handedness, therefore with possibilities in DV- and CV-QIP [Barral and Liñares, 2016]. Other quantum vortices with different properties and symmetries have been also proposed, like the SU(2)-

transformed Fock states [Agarwal and Banerji, 2006], the generalized quantum vortices [Bandyopadhyay and Singh, 2011, Bandyopadhyay et al., 2011, Agarwal, 2011, Banerji et al., 2014], the Bessel-Gauss quantum vortex states [Zhu et al., 2012a, Zhu et al., 2012b] and the Hermite polynomial quantum vortices [Li et al., 2015].

Taking into account all the above, our main motivation is to sketch a monolithic IO chip able to produce quantum vortex states of light by means of non-linear waveguides, directional couplers (DC) and conditional measurement, as well as to introduce a measurement device which can detect their order and handedness. As we will show, a quantum vortex state would be heralded by the detection of a number of photons subtracted by a weakly coupled directional coupler from an entangled squeezed state propagating in a Mach-Zehnder interferometer. Furthermore, we present a realistic approach based on the Wigner function, where the propagation losses, the non-unity efficiency of the heralding detectors and the modal purity of the states are considered. Besides, a vorticity integrated detection system is introduced. We analyze the theoretical basis of this device and present a realistic model based on the inefficient operation of the number-resolving detectors. These devices together open the possibility of using the quantum optical vortices in QIP protocols.

The article is organized as follows: Section 2 presents a scheme of the ideal generation of quantum vortices on-chip, studying their field-strength probability and phase distributions as well as their Wigner distribution on the phase space. A realistic model of the states produced with this scheme is presented in Section 3. In Section 4, a vortex - order and handedness measurement device is proposed and its inefficient operation is studied. Finally, the main results of this article are summarized in Section 5.

P1.2 Device operation

The proposed device is shown in Figure P1.1. It is composed of two stages. The purpose of the first stage is to generate two single-mode squeezed states. Materials like lithium niobate (LN) or potassium titanyl phosphate (KTP) are suitable to be chosen as material substrate. We will focus on the first one due to its appealing properties related to the production of squeezed states on chip, where large conversion efficiencies ($\approx 10^7$ photon pairs $\mathrm{mW^{-1}nm^{-1}s^{-1}}$ in the telecom C and L bands), broad bandwidths (BW) in the CW regime ($\approx$ 10 THz) and transmission losses as low as 0.1 dB $\mathrm{cm^{-1}}$ have been reported [Alibart et al., 2016].

The first stage is composed by an integrated taper, where a slow transition between single- and two-mode parts of the input waveguide is designed in order to maximize the coupling of an input coherent field to the following symmetric splitter. The power of the pump is halved and these two pumps propagating within waveguides 1 and 2 cross two areas specially engineered in order to maximize the non-linear effect of the substrate. A large conversion efficiency between the pump and the daughter fields is obtained by tailoring the non-linearity of the material by periodically poled (PPLN), enabling quasi-phase matching of the propagation constants (QPM) [Suhara, 2009]. The period of the

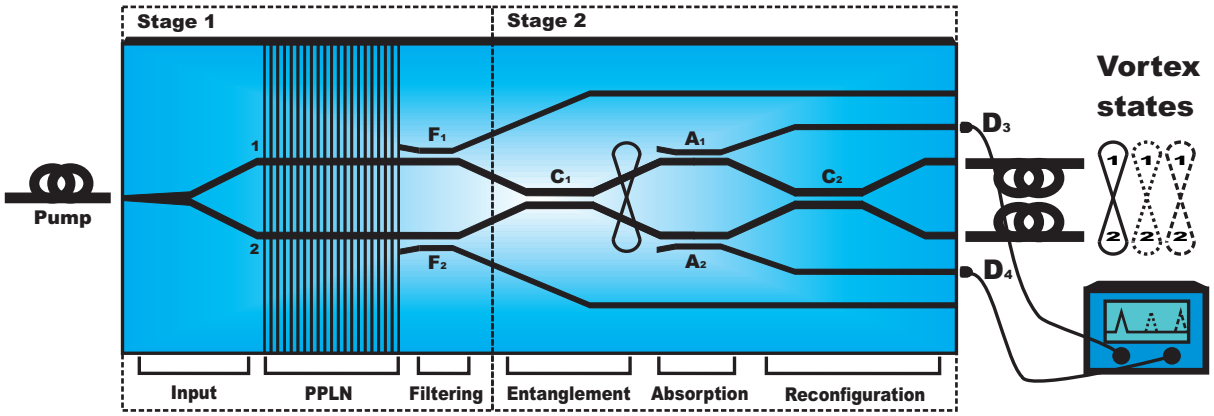


Figure P1.1: Sketch of the device proposed for producing CV quantum vortices. The first stage is devoted to the generation of the quantum state and pump supresion. Two single-mode squeezed states (1 & 2) are produced in the periodically poled zone and the pump is filtered by means of wavelength-dependent DCs (F_1 & F_2). The second stage is made up of an integrated Mach-Zehnder interferometer with two weakly coupled DCs in its arms. The two single-mode squeezed states are first mixed in a 3 dB DC (C_1) in order to generate an entangled two-mode squeezed state. Next, the two weakly coupled DCs (A_1 & A_2) leak photons to a pair of ancillary waveguides (3 & 4). Finally, the second 3 dB DC (C_2) mixes again the states. The detection of n photons in the ancillary modes will herald a n-order quantum vortex.

grating Λ is tailored such that

$$\Delta\beta \equiv \beta(\omega_p) - \beta(\omega_s) - \beta(\omega_i) = \frac{2\pi}{\Lambda}, \tag{P1.1}$$

where $\Delta\beta$ represents the propagation constants mismatch between a pump photon (p) and its daughters photons, labelled signal (s) and idler (i), caused by dispersion. Likewise, type-0 spontaneous parametric down conversion (SPDC) is chosen, coupling the interacting fields along the extraordinary axis of the crystal through the higher component of its second order non-linear tensor, d_{33} [Alibart et al., 2016].

From the quantum field theory it is known that the generator of the temporal evolution of the quantum states is the Hamiltonian operator $\hat{H}$, while their spatial propagation is best described by the momentum operator $\hat{M}$ [Huttner et al., 1990, Toren and Ben-Aryeh, 1994]. Therefore, the generation of quantum light in waveguides can be also described by this operator [Liñares et al., 2008, Liñares et al., 2012], which in this case is given by

$$\hat{M}_j = \frac{1}{2}\iiint \epsilon_0\, d^{(2)}_{eff}(\sum_k \hat{E}_{j,k})^2\, dxdydt, \tag{P1.2}$$

with $j = 1, 2$ and $k = i, s, p$; ϵ_0 is the vacuum permittivity, $d^{(2)}_{eff}$ the second order effective non-linearity in the poled area, the integral is performed over the transverse area of the

waveguide and the period of the waves, and $\hat{E}_{j,k}$ are the quantum optical fields given by

$$\hat{E}_{j,k} \propto \hat{a}_{j,k}\, e^{i\beta_j(\omega_k)z}\, e^{-i\omega_k t}\, \mathbf{e}_{j,k}(x,y) + h.c., \tag{P1.3}$$

with $\hat{a}_{j,k}$ and $\mathbf{e}_{j,k}(x,y)$ the absorption operators and the normalized transverse vector amplitudes related to each mode j,k, respectively. Setting the pump as a strong classical field and applying the above fields into Equation $(P1.2)$ we obtain the following momentum corresponding to the waveguide j

$$\hat{M}_j(\kappa) = -\frac{i\hbar}{2}(\kappa \hat{a}_j^{\dagger 2} - \kappa^* \hat{a}_j^2), \tag{P1.4}$$

where we have considered QPM and conservation of energy, in such a way that the signal and idler waves are degenerated in frequency ($\omega_p = 2\omega_s = 2\omega_i$), and where κ is the nonlinear coupling constant which depends on $d^{(2)}_{eff}$, the pump intensity, the mode mismatch and the QPM. These momentum operators lead to two degenerated single-mode squeezed vacuum states given by

$$|\Psi_A\rangle = \hat{S}_1(s)\hat{S}_2(s)|0_1\, 0_2\rangle, \tag{P1.5}$$

where $\hat{S}_j(s) = e^{\frac{i}{\hbar}\hat{M}_j L_p} = e^{\frac{s}{2}(\hat{a}_j^{\dagger 2} - \hat{a}_j^2)}$ is the single-mode squeezing operator and $s = \kappa L_p$ the squeezing parameter generated in a poled area of length L_p, which we have chosen real in order to simplify [Suhara, 2009].

Next, the pump is filtered by means of suitably designed wavelength dependent DCs (F_1 and F_2 in Figure P1.1). Quantum-mechanically, a DC working at frequency ω is given by $\hat{U}_{jl}(\theta_j(\omega)) = e^{-i(\theta_j(\omega)/2)\hat{\sigma}_x}$, or in matrix form by

$$U(\theta_j(\omega)) = \begin{pmatrix} \cos(\theta_j(\omega)/2) & i\sin(\theta_j(\omega)/2) \\ i\sin(\theta_j(\omega)/2) & \cos(\theta_j(\omega)/2) \end{pmatrix}, \tag{P1.6}$$

with $\theta_j(\omega) \equiv 2\kappa(\omega)L_D$, $\kappa(\omega)$ is the frequency-dependent coupling strength of a DC of length L_D and $\hat{\sigma}_x$ is the corresponding Pauli operator [Campos et al., 1989]. $\hat{U}_{jl}$ stands for a DC with effective reflectivity $r_j = \sin(\theta_j(\omega)/2)$ and transmittivity $t_j = \cos(\theta_j(\omega)/2)$. Since the DCs F_1 and F_2 are designed to filter the pumps, they fully reflect the pump ($\theta(\omega_p) = \pi$) towards ancillary waveguides l and transmit the squeezed vacua ($\theta(\omega_s) = 2\pi$) through the signal waveguides $j = 1, 2$. These dispersive couplers have been experimentally demonstrated in SPDC on a LN chip showing a pump suppression of ≈ 30 dB [Jin et al., 2014] and, recently, they have been proposed as new tools for quantum state control showing functionalities without equivalent in bulk optics [Marchildon and Helmy, 2016].

The second stage consist of a Mach-Zehnder interferometer made up of two 3 dB DCs at the signal frequency (C_1 and $C2$ in Figure P1.1) and two single-mode waveguides. These guides are also weakly coupled to two ancillary waveguides, in such a way that photons are leaked into them from the main modes.

The quantum state Eq. $(P1.5)$ after the directional coupler $C1$ is transformed into the following EPR state [Agarwal, 2012]

$$|\Psi_B\rangle = \hat{U}_{12}(\pi/2)\hat{S}_1(s)\hat{S}_2(s)|0_1\, 0_2\rangle = \hat{S}_{12}(is)|0_1\, 0_2\rangle, \tag{P1.7}$$

where $\hat{S}_{12}(is) = e^{is(\hat{a}_1^\dagger \hat{a}_2^\dagger + \hat{a}_1 \hat{a}_2)}$ stands for the two-mode squeezed operator. Then, the quantum state (P1.7) founds two weakly coupled DCs (A_1 and A_2 in Figure P1.1) which couple the main waveguides with two ancillary ones (3 and 4). These directional couplers cause the following mixing of the modes

$$|\Psi_C\rangle = \hat{U}_{13}(\theta_1)\hat{U}_{24}(\theta_2)\hat{S}_{12}(is)|0_1\,0_2\,0_3\,0_4\rangle. \tag{P1.8}$$

As input modes 3 and 4 are in the vacuum, using the disentangling theorem for the SU(2) group [Kim, 2008], Equation (P1.8) can be written as

$$|\Psi_C\rangle = e^{-i\tan(\theta_1/2)\hat{a}_1\hat{a}_3^\dagger}\, t_1^{\hat{a}_1^\dagger \hat{a}_1}\, e^{-i\tan(\theta_2/2)\hat{a}_2\hat{a}_4^\dagger}\, t_2^{\hat{a}_2^\dagger \hat{a}_2}\, \hat{S}_{12}(is)|0_1\,0_2\,0_3\,0_4\rangle. \tag{P1.9}$$

The measurement operator related to the subtraction of n photons from the mode j is given by [Vidrighin et al., 2013]

$$\hat{G}_l(n) = \langle n_l|\hat{U}_{jl}(\theta_j)|0_l\rangle = (-i)^n \frac{\tan^n(\theta_j/2)}{\sqrt{n!}} \hat{a}_j^n t_j^{\hat{a}_j^\dagger \hat{a}_j}. \tag{P1.10}$$

Considering high transmittivity ($t_{1,2} \to 1$ or equally $\theta_{1,2} \to 0$) and moderate squeezing, the detection of n photons in the mode 3 is given by

$$|\Psi_D\rangle = \langle n_3\,0_4|\Psi_C\rangle = \hat{G}_3(n)\hat{G}_4(0)|\Psi_B\rangle \approx (-i)^n \frac{(\theta_1/2)^n}{\sqrt{n!}} \hat{a}_1^n\, \hat{S}_{12}(is)|0_1\,0_2\rangle. \tag{P1.11}$$

A similar result would be obtained detecting n photons in the mode 4. It should be outlined that the measurement operator can be carried out by using photon number-resolving detectors (PNRDs) [Namekata et al., 2010]. In the case of using avalanche photodiodes (APDs), they do not distinguish between one or several photons impinging on it at the same time, so the "click" event projects the state into a statistical mixture. We will study that case in the following section. Moreover, bearing in mind that $[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}$, by using the two-mode squeezing Bogoliubov transformation $\hat{S}_{12}^\dagger(s)\hat{a}_1\hat{S}_{12}(s) = \cosh s\, \hat{a}_1 + \sinh s\, \hat{a}_2^\dagger$ Equation (P1.11) can be rewritten as

$$|\Psi_D\rangle \approx (-i)^n \sinh^n(s) \frac{(\theta_1/2)^n}{\sqrt{n!}} \hat{S}_{12}(is)\hat{a}_2^{\dagger n}|0_1\,0_2\rangle. \tag{P1.12}$$

Finally, this quantum state finds the second 3 dB DC (C_2 in Figure P1.1) designed in such a way that it performs the unitary $\hat{U}_{12}(3\pi/2)$. Hence, the detection of n photons in the leaky modes, would herald the following quantum state

$$|\Psi_E\rangle \propto \hat{S}_1(s)\hat{S}_2(s)(\hat{a}_1^\dagger \pm i\hat{a}_2^\dagger)^n|0_1\,0_2\rangle, \tag{P1.13}$$

where we have used the similarity transformation $\hat{U}\,\hat{a}^{\dagger n}\,\hat{U}^\dagger = \hat{U}\,\hat{a}^\dagger\,\hat{U}^\dagger\,\hat{U}\,\hat{a}^\dagger\,\hat{U}^\dagger \ldots \hat{U}\,\hat{a}^\dagger\,\hat{U}^\dagger = (\hat{U}\,\hat{a}^\dagger\,\hat{U}^\dagger)^n$ [Mandel and Wolf, 1995] and the plus and minus signs appear after the detection of photons in the modes 3 and 4, respectively. This is a quantum vortex state

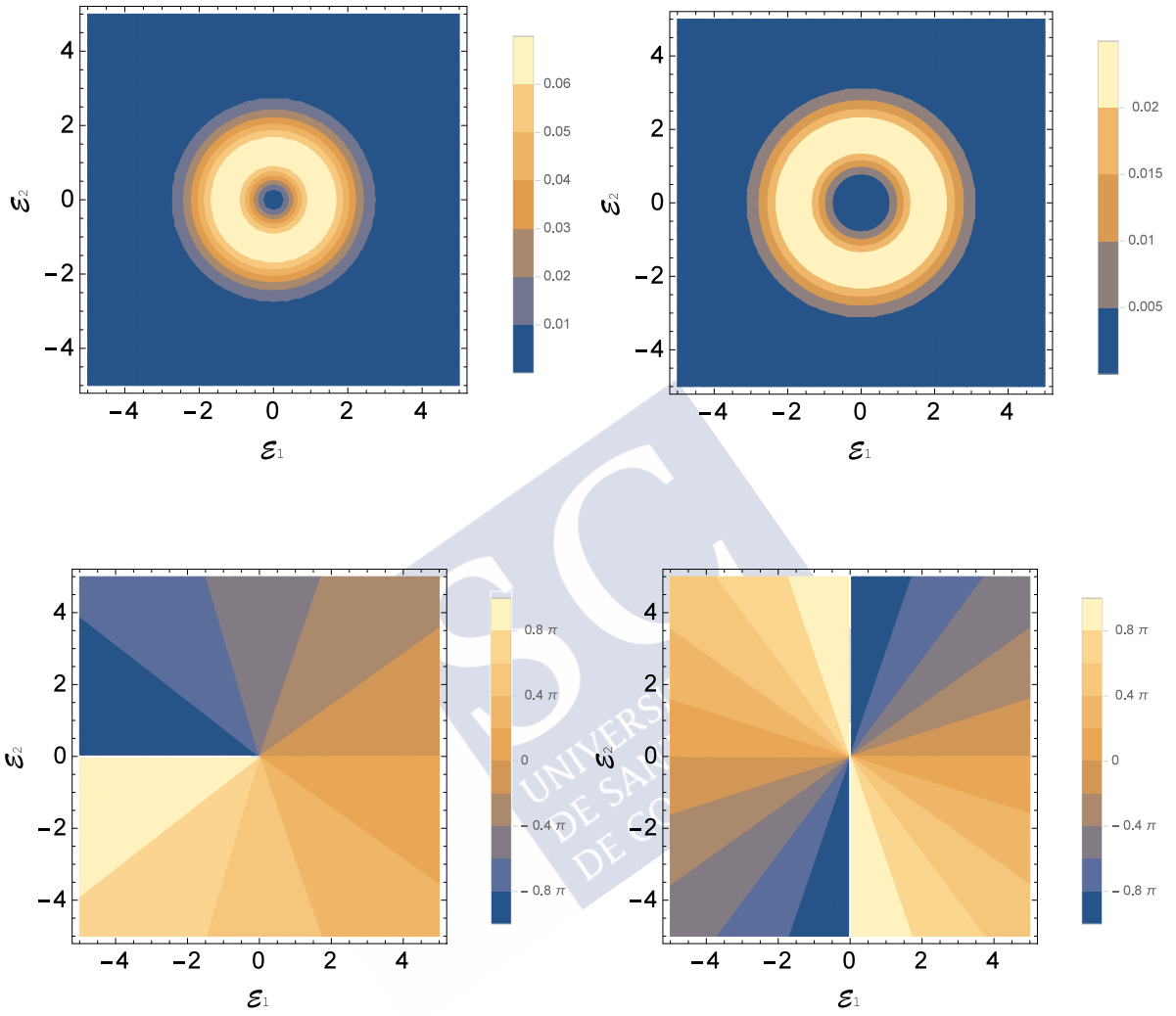


Figure P1.2: Plots of probability (upper) and phase (lower) densities of quantum vortices of order 1 (left) and 2 (right) with a squeezing factor $s = 0.25$.

$|n_{\pm}\rangle$ of order n and $\pm$ handedness, or $(n_{\pm}, 0_{\mp})$ [Agarwal et al., 1997]. This family of states shows a high entanglement, as well as non-gaussian and non-classical features as recently shown in [Barral and Liñares, 2016]. It should be noted that the probability of heralding a quantum vortex of order n scales with $(\sinh(s)\,\theta)^n$, so this scheme would be only practical in the production of low-order quantum vortices. On the other hand, the vorticity of these states is better visualized in the optical field-strength space where $\mathcal{E}_j$ is the eigenvalue of the optical field-strength operator $\hat{\mathcal{E}}_j = (\hat{a}_j + \hat{a}_j^{\dagger})/\sqrt{2}$, proportional to

the first quadrature of the quantum optical field, and analogously $\hat{\mathcal{P}}_j = -i(\hat{a}_j - \hat{a}_j^\dagger)/\sqrt{2}$ is related to the second quadrature [Schleich, 2001]. In this representation, the normalized wavefunction corresponding to the quantum state given by Equation (P1.13) is as follows

$$\Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2) = \langle \mathcal{E}_1\, \mathcal{E}_2 | \Psi_E \rangle = \frac{1}{\sqrt{\pi\, n!\; e^{2(1+n)s}}} (\mathcal{E}_1 \pm i\mathcal{E}_2)^n e^{-\frac{\mathcal{E}_1^2+\mathcal{E}_2^2}{2e^{2s}}}, \tag{P1.14}$$

where $|\mathcal{E}_j\rangle$ are eigenstates of the optical field-strength fulfilling $\hat{\mathcal{E}}_j|\mathcal{E}_j\rangle = \mathcal{E}_j|\mathcal{E}_j\rangle$. Figure P1.2 shows the probability $P = |\Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2)|^2$ and phase $\varphi = \arg\{\Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2)\}$ densities for a squeezing factor $s = 0.25$, vortex orders 1 (Figure P1.2, left) and 2 (Figure P1.2, right) and minus handedness. We can observe the circular symmetry of the vortex with a growing radius with the number of photons (Figure P1.2, upper) and the order of the vortex appearing in the phase as the number of complete cycles (Figure P1.2, lower). If we had detected photons in mode 4, instead of mode 3, the only difference would be a change in handedness. Remarkably, both the probability and phase densities of the quantum state can be reconstructed by means of a weak values scheme [Barral et al., 2015].

Likewise, the Wigner function associated to the quantum vortex $|n_\pm\rangle$ is easily worked out from the wavefunction Equation (P1.14) and the Wigner formula

$$W(\mathcal{E}_1, \mathcal{P}_1, \mathcal{E}_2, \mathcal{P}_2) = \frac{1}{(2\pi)^2} \iint_{-\infty}^{\infty} \Psi(\mathcal{E}_1 + R_1/2, \mathcal{E}_2 + R_2/2)\Psi^*(\mathcal{E}_1 - R_1/2, \mathcal{E}_2 - R_2/2) \\ e^{i(R_1\mathcal{P}_1 + R_2\mathcal{P}_2)} dR_1 dR_2, \tag{P1.15}$$

obtaining [Pratap Singh et al., 2006]

$$W_{n\pm}(\mathcal{E}_1, \mathcal{P}_1, \mathcal{E}_2, \mathcal{P}_2) = \frac{(-1)^n}{\pi^2} e^{-e^{-2s}\,(\mathcal{E}_1^2+\mathcal{E}_2^2) - e^{2s}\,(\mathcal{P}_1^2+\mathcal{P}_2^2)} \\ \mathcal{L}_n(e^{-2s}\,(\mathcal{E}_1^2 + \mathcal{E}_2^2) + e^{2s}\,(\mathcal{P}_1^2 + \mathcal{P}_2^2) \pm 2(\mathcal{E}_1\mathcal{P}_2 - \mathcal{E}_2\mathcal{P}_1)), \tag{P1.16}$$

where $\mathcal{L}_n(\mathrm{x})$ is the Laguerre polynomial or order n and argument x. Figure P1.3 shows the Wigner distributions related to the quantum vortices with vorticity order $n_+ = 1$ and 2, for a squeezing factor $s = 0.7$. In order to sketch the four-dimensional Wigner function given by Equation (P1.16) in two dimensions we have set $\mathcal{E}_1 = \mathcal{P}_1 = 0$. It is remarkable the presence of negative values around the origin of the phase space for the order 1 vortex, and far from the origin for the order 2 vortex, which is a sign of the non-clasicality of these quantum states.

Additionally, it should be noted that the simultaneous detection of photons in the leaky modes does not lead to a vortex state. In that case the following expression is obtained

$$(\hat{a}_1 - i\hat{a}_2)^m (\hat{a}_1 + i\hat{a}_2)^n \hat{S}_1(s)\hat{S}_2(s)|0_1\, 0_2\rangle \neq C\, \hat{S}_1(s)\hat{S}_2(s)(\hat{a}_1^\dagger - i\hat{a}_2^\dagger)^m (\hat{a}_1^\dagger + i\hat{a}_2^\dagger)^n |0_1\, 0_2\rangle, \tag{P1.17}$$

with C a constant factor. That is, the heralded quantum state after simultaneous measurement of n photons by D_3 and m photons by D_4 is not the vortex state of order (n_+, m_-) given in the right term of Equation (P1.17).

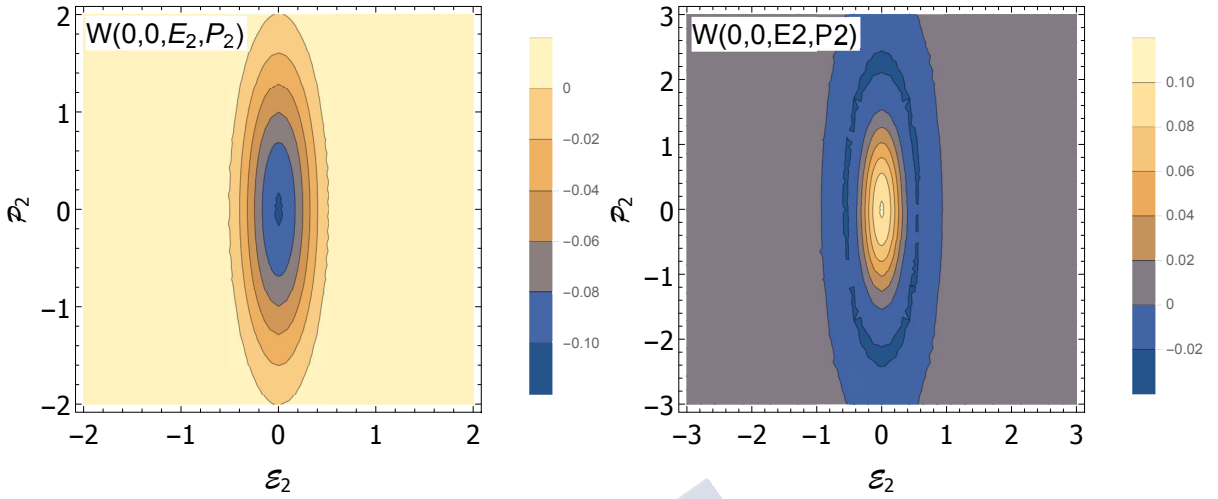


Figure P1.3: Plots of the Wigner distribution on the phase space for quantum vortices of order 1 (left) and 2 (right) with a squeezing factor $s = 0.7$.

P1.3 Realistic scenario

This section is devoted to the study of the generation of quantum vortices in a realistic approach, that is, when propagation losses, non-unity efficiency of the heralding detectors and modal purity of the heralded quantum state are taken into account. There are two main approaches in this direction: the density matrix and the Wigner function [Neergaard-Nielsen, 2008]. Since the quantum states involved are gaussian till the de-gaussification produced by the photon absorption, the gaussian formalism related to the Wigner function will be less cumbersome and more transparent than that corresponding to the density matrix. This approach has been extensively used along the last decade in the study of the generation of quantum states under different experimental imperfections [Ourjoumtsev et al., 2007a, Ourjoumtsev et al., 2007b, Ourjoumtsev et al., 2009].

Therefore, we start calculating the Wigner function related to Equation ($P1.5$), given by [Furusawa, 2015]

$$W_A(\mathcal{E}_1, \mathcal{P}_1, \mathcal{E}_2, \mathcal{P}_2) = \frac{1}{\pi^2} e^{-e^{-2s}(\mathcal{E}_1^2+\mathcal{E}_2^2)-e^{2s}(\mathcal{P}_1^2+\mathcal{P}_2^2)}. \tag{P1.18}$$

These modes are mixed on the first $3\,dB$ DC (C1) turning out in the following expression

$$W_B(\mathcal{E}_1, \mathcal{P}_1, \mathcal{E}_2, \mathcal{P}_2) = W_A(\frac{\mathcal{E}_1+\mathcal{P}_2}{\sqrt{2}}, \frac{\mathcal{P}_1-\mathcal{E}_2}{\sqrt{2}}, \frac{\mathcal{E}_2+\mathcal{P}_1}{\sqrt{2}}, \frac{\mathcal{P}_2-\mathcal{E}_1}{\sqrt{2}}), \tag{P1.19}$$

corresponding to the EPR state Eq. (P1.7). The quantum state finds the two weakly coupled DCs (A_1 and A_2). The modes 1 and 2 are mixed with vacuum modes 3 and 4, respectively. The Wigner function of the vacuum is given by $W_v(\mathcal{E}, \mathcal{P}) = \pi^{-1} e^{-(\mathcal{E}^2+\mathcal{P}^2)}$.

The output state can be then written as

$$\begin{aligned} &W_C(\mathcal{E}_1,\mathcal{P}_1,\mathcal{E}_2,\mathcal{P}_2,\mathcal{E}_3,\mathcal{P}_3,\mathcal{E}_4,\mathcal{P}_4) = \\ &W_B(t_1\,\mathcal{E}_1 + r_1\,\mathcal{P}_3, t_1\,\mathcal{P}_1 - r_1\,\mathcal{E}_3, t_2\,\mathcal{E}_2 + r_2\,\mathcal{P}_4, t_2\,\mathcal{P}_2 - r_2\,\mathcal{E}_4) \\ &W_3(t_1\,\mathcal{E}_3 + r_1\,\mathcal{P}_1, t_1\,\mathcal{P}_3 - r_1\,\mathcal{E}_1)\,W_4(t_2\,\mathcal{E}_4 + r_2\,\mathcal{P}_2, t_2\,\mathcal{P}_4 - r_2\,\mathcal{E}_2). \end{aligned} \tag{P1.20}$$

Now, we analyze the detection of photons in the ancillary modes 3 and 4. We will choose as detectors a pair of APDs, since they are more commonly used. These can not distinguish the number of photons. They only give information about if some photons were absorbed or not, in such a way that they project the state into a statistical mixture. This kind of detection, so-called on/off, can be modelled by the following operator

$$\hat{\Pi}_a^{on} = \sum_{n\geq 1} |n\rangle_a\langle n| = \hat{I}_a - \hat{\Pi}_a^{off} = \hat{I}_a - |0\rangle_a\langle 0|, \tag{P1.21}$$

where $\hat{I}$ stands for the identity operator and a for the ancillary mode measured. Note the contrast with the PNRD operator given by Equation (P1.10) which measures a fixed number of photons. The quantum state obtained after this measurement is given by

$$\hat{\rho}_s^{on} = \frac{Tr_a[\hat{\Pi}_a^{on}\hat{\rho}]}{Pr_{on}} \tag{P1.22}$$

with $Pr_{on} = Tr_{a,s}[\hat{\Pi}_a^{on}\hat{\rho}]$ the heralding probability and where s stands for the signal mode, Tr is the trace operator and $\hat{\rho}$ the matrix density of the quantum state before measurement. In the Wigner representation, this operation is given by [Leonhardt, 1997]

$$W^{on}(\mathcal{E}_s,\mathcal{P}_s) = \frac{2\pi \iint W_\rho\, W_{\Pi^{on}}\, d\mathcal{E}_a d\mathcal{P}_a}{(2\pi)^2 \iiiint W_\rho\, W_{\Pi^{on}}\, d\mathcal{E}_a\, d\mathcal{P}_a\, d\mathcal{E}_s\, d\mathcal{P}_s}, \tag{P1.23}$$

where W_ρ is the Wigner function of the input quantum state and $W_{\Pi^{on}} = (1/2\pi) - W_{\Pi^{off}} = (1/2 - e^{-(\mathcal{E}_a^2+\mathcal{P}_a^2)})/\pi$ the one related to the on/off operator Eq. (P1.21). This expression is easily generalized to a higher number of modes as in our case. Moreover, the detector is characterized by a total efficiency ν for the photons to be detected, given by its quantum efficiency and the losses in the ancillary channel. This non-unity efficiency can be included in the analysis by inserting a fictitious beamsplitter before the detector, mixing the state with a vacuum and tracing it out [Leonhardt, 1997] (Figure P1.4). The Wigner function when these losses are taken into account is given by

$$\begin{aligned} &W_{C'}(\mathcal{E}_1,\mathcal{P}_1,\mathcal{E}_2,\mathcal{P}_2,\mathcal{E}_3,\mathcal{P}_3,\mathcal{E}_4,\mathcal{P}_4) = \\ &\iiiint W_C(\sqrt{\nu_3}\,\mathcal{E}_3 + \sqrt{1-\nu_3^2}\,\mathcal{E}_5,\ \sqrt{\nu_3}\,\mathcal{P}_3 + \sqrt{1-\nu_3^2}\,\mathcal{P}_5,\ \sqrt{\nu_4}\,\mathcal{E}_4 + \sqrt{1-\nu_4^2}\,\mathcal{E}_6,\ \sqrt{\nu_4}\,\mathcal{P}_4 + \sqrt{1-\nu_4^2}\,\mathcal{E}_6) \\ &W_5(\sqrt{\nu_3}\mathcal{E}_5 - \sqrt{1-\nu_3^2}\mathcal{E}_3, \sqrt{\nu_3}\,\mathcal{P}_5 - \sqrt{1-\nu_3^2}\,\mathcal{P}_3)\,W_6(\sqrt{\nu_4}\,\mathcal{E}_6 - \sqrt{1-\nu_4^2}\,\mathcal{E}_4, \sqrt{\nu_4}\,\mathcal{P}_6 - \sqrt{1-\nu_4^2}\,\mathcal{E}_4) \\ &d\mathcal{E}_5\,d\mathcal{P}_5\,d\mathcal{E}_6\,d\mathcal{P}_6, \end{aligned} \tag{P1.24}$$

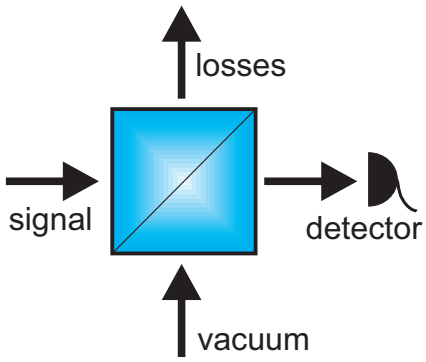


Figure P1.4: Fictitious beam splitter as a model of imperfect detection. The signal is both attenuated (non-unit efficiency) and contaminated by vacuum fluctuations entering the second input.

where 5 and 6 are the auxiliary modes which are mixed in the beamsplitter and ν_3 and ν_4 are the total efficiencies of the APDs D_3 and D_4. Then, a click event in the mode 3 and no-click in mode 4 produces the following Wigner function

$$W_D(\mathcal{E}_1,\mathcal{P}_1,\mathcal{E}_2,\mathcal{P}_2) = \frac{(2\pi)^2 \iiiint W_{C'}\, W_{\Pi_3^{on}}\, W_{\Pi_4^{off}}\, d\mathcal{E}_3\, d\mathcal{P}_3\, d\mathcal{E}_4\, d\mathcal{P}_4}{Pr_{on,off}}, \tag{P1.25}$$

where $Pr_{on,off} = (2\pi)^4 \int W_{C'}\, W_{\Pi_3^{on}}\, W_{\Pi_4^{off}}\, d\boldsymbol{E}\, d\boldsymbol{P}$ is the heralding probability, with $d\boldsymbol{E} \equiv d\mathcal{E}_1 \ldots d\mathcal{E}_4$ and $d\boldsymbol{P} \equiv d\mathcal{P}_1 \ldots d\mathcal{P}_4$. This expression is obtained after applying Equation (P1.24) on a generalization of Equation (P1.23) to this case. Additionally, the situation of a click in the detector D_4 and no-click in D_3 could be also studied by only exchanging the subindices 3 and 4 in Equation (P1.25).

Likewise, another question should be borne in mind in our analysis: the dark counts. In this case a click will be recorded without any impinging photon due to thermal noise in the diode. Therefore, the detector does not difference between a genuine photon and a dark count. Since a dark count click gives no information about the conditional state, it mixes the desired quantum state with the unconditional one. The fraction of genuine photons is called modal purity ζ, and its effect is included in the Wigner representation via the following expression [Wenger et al., 2004]

$$W_{D'} = \zeta\, W_D + (1-\zeta)\, W_B, \tag{P1.26}$$

where W_B is the Wigner function of the unconditonal state. Moreover, the modal purity can incorporate others sources of false clicks like mode crosstalk and after-pulsing

The quantum vortex state of light is obtained after crossing the second $3\,dB$ DC (C_2) which performs the inverse operation of C_1. Following Equation (P1.19), the next Wigner function is obtained

$$W_E(\mathcal{E}_1,\mathcal{P}_1,\mathcal{E}_2,\mathcal{P}_2) = W_{D'}\left(\frac{\mathcal{E}_1-\mathcal{P}_2}{\sqrt{2}}, \frac{\mathcal{P}_1+\mathcal{E}_2}{\sqrt{2}}, \frac{\mathcal{E}_2-\mathcal{P}_1}{\sqrt{2}}, \frac{\mathcal{P}_2+\mathcal{E}_1}{\sqrt{2}}\right). \tag{P1.27}$$

Finally, propagation losses in the modes 1 and 2 and the output coupling to fibers have to be taken into account. By using a fictitious beamsplitter like in Equation (P1.24), the Wigner function of the output quantum vortex state is then

$$W_{E'}(\mathcal{E}_1,\mathcal{P}_1,\mathcal{E}_2,\mathcal{P}_2) = \iiiint W_E(\sqrt{\eta_1}\,\mathcal{E}_1+\sqrt{1-\eta_1^2}\,\mathcal{E}_7,\,\sqrt{\eta_1}\,\mathcal{P}_1+\sqrt{1-\eta_1^2}\,\mathcal{P}_7,\,\sqrt{\eta_2}\,\mathcal{E}_2+\sqrt{1-\eta_2^2}\,\mathcal{E}_8,\,\sqrt{\eta_2}\,\mathcal{P}_2+\sqrt{1-\eta_2^2}\,\mathcal{E}_8)$$
$$W_7(\sqrt{\eta_1}\,\mathcal{E}_7-\sqrt{1-\eta_1^2}\,\mathcal{E}_1,\sqrt{\eta_1}\,\mathcal{P}_7-\sqrt{1-\eta_1^2}\,\mathcal{P}_1)\,W_8(\sqrt{\eta_2}\,\mathcal{E}_8-\sqrt{1-\eta_2^2}\,\mathcal{E}_2,\sqrt{\eta_2}\,\mathcal{P}_8-\sqrt{1-\eta_2^2}\,\mathcal{E}_2)$$
$$d\mathcal{E}_7\,d\mathcal{P}_7\,d\mathcal{E}_8\,d\mathcal{P}_8. \tag{P1.28}$$

where η_1 and η_2 stand for the propagation losses in the modes 1 and 2, respectively, and 7 and 8 are vacuum auxiliary modes.

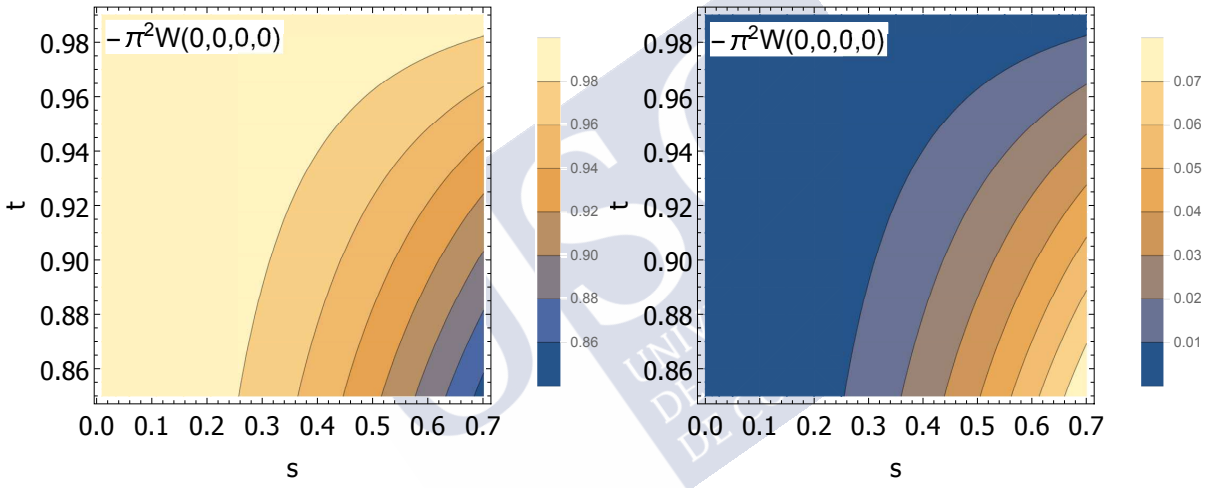


Figure P1.5: Plots of $-\pi^2\,W_{E'}(0,0,0,0)$ and heralding probability $Pr_{on,off}$ for different values of squeezing s, weakly couplers transmission t. Left: $-\pi^2\,W_{E'}(0,0,0,0)$ vs t-s with $\eta=1$, $\nu=1$ and $\zeta=1$. Right: $Pr_{on,off}$ vs t-s with $\eta=1$, $\nu=1$ and $\zeta=1$.

The realistic approach above introduced measures the consequences on the quality of the quantum states produced by the use of non-ideal detectors and losses. The Wigner function related to non-classical quantum states show negative values along the phase space. Particularly, single-photon subtracted quantum states show a large negativity in the center of the phase space, which is considered a strong signature of non-classicality. Due to this feature, an extensively used figure of merit in the generation of photon-subtracted quantum states is the value of the Wigner function at the origin, $W(0,0,0,0)$ [Suzuki et al., 2006]. In the case of ideal quantum vortices, a value $W(0,0,0,0)=-1/\pi^2$ is obtained for a vortex order $n=1$, as shown in Figure P1.3. However, experimental imperfections and mixing due to the absorption of higher number of photons will reduce this value. Figures P1.5 and P1.7 show values of the normalized Wigner function related

to the ideal value $-1/\pi^2$ for different device parameters and imperfections. Likewise, the dependence of the heralding probability $Pr_{on,off}$ on some parameters (Figure P1.5 right) is also shown to complement the analysis of the system. In order to simplify, we have set identical values for the transmittivity of $C1$ and $C2$, $t_1 = t_2 \equiv t$, the total efficiencies of detectors D_3 and D_4, $\nu_3 = \nu_4 \equiv \nu$, and propagation and output coupling losses $\eta_1 = \eta_2 \equiv \eta$. The transmittivity and input squeezing dependence of $-\pi^2 W_{E'}(0,0,0,0)$ and $Pr_{on,off}$ are sketched in Figure P1.5 left and right, respectively, where no losses are considered. They show the inverse relationship between non-classicality and heralding probability. For a fixed transmittivity of the directional couplers $C1$ and $C2$, a higher value of squeezing increases the rate of production of vortex states at the cost, however, of the subtraction of higher number of photons which are available in the state, decreasing accordingly the value of $-\pi^2 W_{E'}(0,0,0,0)$ due to the statistical mixture produced. This admixture is shown in Figure P1.6, where we have compared the Wigner function $W_{E'}$ for a squeezing factor as high as $s = 0.7$ and a transmittivity $t = 0.85$ with a superposition of the Wigner functions associated to the first two ideal quantum vortices (Figure P1.3) given by Equation (P1.16): $0.91\, W_{1+} + 0.07\, W_{2+}$, where the coefficients are the calculated fidelities $\mathcal{F}$ between the quantum state $\hat{\rho}_{E'}$ and the ideal vortices, given by [Leonhardt, 1997]

$$\mathcal{F}(|n_{\pm}\rangle,\, \hat{\rho}_{E'}) = (2\pi)^2 \iiiint W_{\rho}\, W_{n_{\pm}}\, d\mathcal{E}_1\, d\mathcal{P}_1\, d\mathcal{E}_2\, d\mathcal{P}_2. \tag{P1.29}$$

Figure P1.6 shows a good agreement between both Wigner functions in the area surrounding the origin of the phase space. However, higher order vortex terms should be added in order to get a better fit in the areas far from it.

Likewise, Figure P1.7 left shows the effect of the total efficiency of the heralding detectors and imperfections in channels 1 and 2 on the non-classicality. A dramatic dependence with the losses in the main channels is shown whereas the efficiency in the ancillary detectors is barely noticed, lowering however the heralding rate as it decreases. In Figure P1.7 right, the joint effect of the modal purity and the main losses is depicted. The mixing of the conditioned and unconditioned states weighted by the modal purity shows a severe impact on the quality of the generated state, sometimes even losing the non-classicality. Therefore, we can conclude that the main causes of degradation of the output quantum state are the losses due to propagation and coupling in the principal modes and the modal purity of the quantum state, mainly related to dark counts, and they are the key points to be improved for the optimal operation of this photonic device.

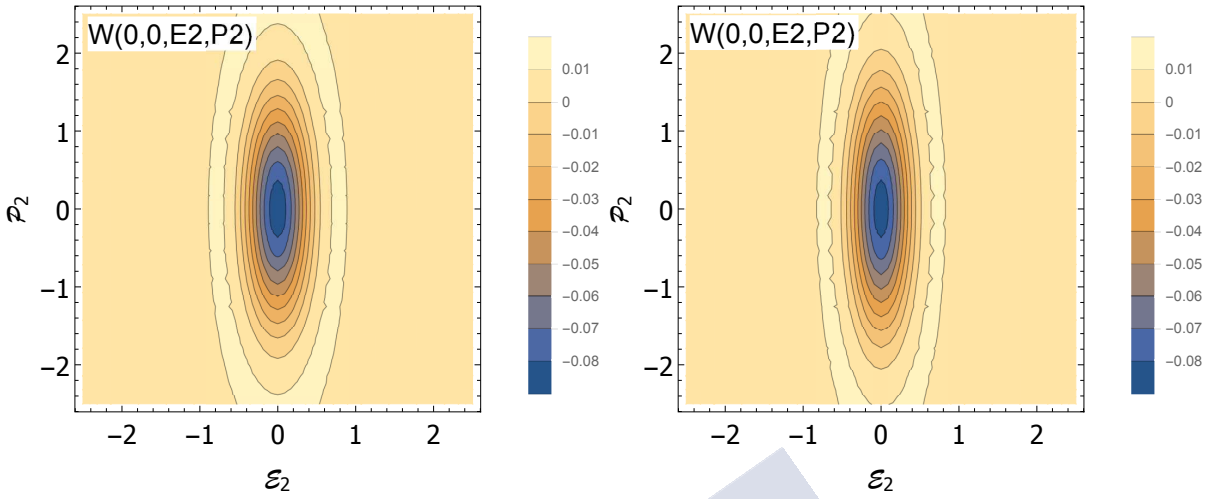


Figure P1.6: Comparison of the Wigner functions related to quantum vortices obtained by APD heralding (left) and a superposition of ideal Wigner functions for the first two vortex orders (right). Left: plot of the Wigner distribution on the phase space $W_{E'}$ for a quantum vortex with squeezing factor $s = 0.7$, weakly couplers transmission $t = 0.85$ and ideal transmission and heralding ($\eta = 1$, $\nu = 1$, $\zeta = 1$). Right: superposition of Wigner functions for ideal quantum vortices of orders $n = 1$ and 2: $0.91\,W_{1+} + 0.07\,W_{2+}$.

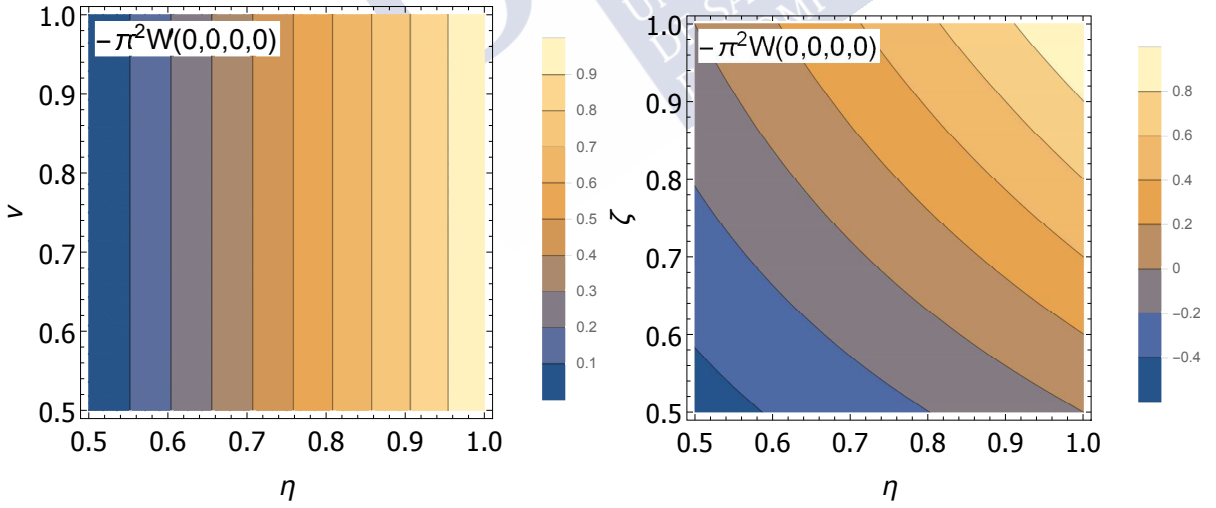


Figure P1.7: Plots of $-\pi^2\,W_{E'}(0,0,0,0)$ for different values of propagation and coupling losses in the main channels η, total efficiency of ancillary detectors ν and modal purity ζ. Left: $-\pi^2\,W_{E'}(0,0,0,0)$ vs ν-η with $s = 0.2$, $t = 0.99$ and $\zeta = 1$. Right: $-\pi^2\,W_{E'}(0,0,0,0)$ vs ζ-η with $s = 0.2$, $t = 0.99$ and $\nu = 1$.

P1.4 Order and handness detection

The quantum vortices above presented show an hybrid nature: they are CV quantum states which carry DV quantum information. This can be shown by applying the abstract angular momentum operator $\hat{L}_z$ on Equation (P1.14) as follows [Agarwal et al., 1997]

$$\hat{L}_z \Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2) = -i(\hat{\mathcal{E}}_1 \partial_{\mathcal{E}_2} - \hat{\mathcal{E}}_2 \partial_{\mathcal{E}_1}) \Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2) = \pm n \, \Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2). \tag{P1.30}$$

Therefore, the quantum vortices $|\Psi_E\rangle$ are eigenstates of the abstract angular momentum with eigenvalues (or vorticity) $\pm n$, and they carry an orbital angular momentum of $\pm n\hbar$. This feature can be used in the implementation of specific protocols in QIP. However, a measurement scheme is necessary in order to do so. To this end, the following simple detector of the order and handedness of the quantum vortex states is proposed: a 3 dB DC with two photon number-resolving detectors (PNRDs) [Hadfield, 2009] connected at its outputs or integrated on chip (Figure P1.8) . The operation of this device is easily shown by applying the 3 dB DC operator on Equation (P1.30) [Korolkova et al., 2002]

$$\hat{U}_{12}(\pi/2)\, \hat{L}_z \Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2) = \hat{U}_{12}(\pi/2)\, \hat{L}_z\, \hat{U}_{12}^\dagger(\pi/2) \hat{U}_{12}(\pi/2) \Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2) = \pm n\, \hat{U}_{12}(\pi/2)\, \Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2). \tag{P1.31}$$

This is an eigenvalue equation where $\hat{U}_{12}(\pi/2)\, \Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2)$ are eigenstates of the operator $\hat{L}'_z \equiv \hat{U}_{12}(\pi/2)\, \hat{L}_z\, \hat{U}_{12}^\dagger(\pi/2)$ with eigenvalues $\pm n$, where the prime denotes the output modes related to the DC. Working out the value of the transformed abstract angular momentum operator we have $\hat{L}'_z = \hat{n}'_1 - \hat{n}'_2$, with $\hat{n}'_j = \hat{a}'^\dagger_j \hat{a}'_j$ the photon number operator related to each mode j at the output. Hence, Equation (P1.31) is rewritten as follows

$$(\hat{n}'_1 - \hat{n}'_2)\, [\hat{U}_{12}(\pi/2)\, \Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2)] = \pm n\, [\hat{U}_{12}(\pi/2)\, \Psi_{n_\pm}(\mathcal{E}_1, \mathcal{E}_2)\,]. \tag{P1.32}$$

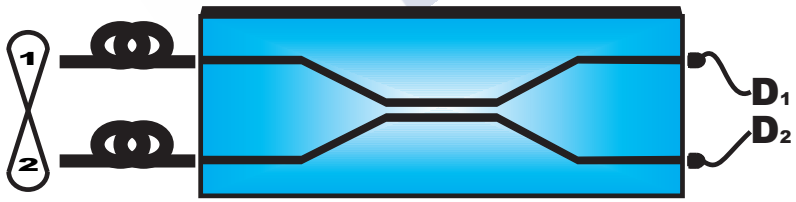


Figure P1.8: Integrated detection system. The device is made up of a 3 dB DC and two PNRDs. The difference of the number of photons recorded at each output D_1 and D_2 gives information about the order and handedness of the input quantum vortex state.

The interpretation of this Equation is clear: measuring the difference of the number of photons at each output $1'$ and $2'$, we can obtain the order and abstract handedness of the quantum vortex associated to the modes 1 and 2. This measurement device enables therefore the use of quantum vortices as a carrier of quantum information with possibilities in QIP.

However, as shown in section P1.2, the quality in the detection of the number of photons will be degraded by the propagation losses as well as by the non-unity efficiency

and the dark counts of the detector [Hadfield, 2009]. An input quantum state $\hat{\rho}$ given by a Wigner function $W_\rho(\mathcal{E}_1, \mathcal{P}_1, \mathcal{E}_2, \mathcal{P}_2)$ is transformed after crossing the 3 dB DC as given by Equation (P1.19). If the dark counts are not considered, the propagation losses, coupling efficiency and non-unity efficiency of the detectors can be introduced in our model as in the above section by means of Equation (P1.28), taking μ_1 and μ_2 as the total detection efficiencies at each output of the detection system. On the other hand, when the photodetectors show dark counts, the vacua in the auxiliary modes entering the free input ports of the fictitious beam splitters should be replaced by either thermal states $\hat{\rho}_{th}$ or phase-averaged coherent states $\hat{\rho}_{pa}$, depending on the origin of the noise, either thermal or Poissonian, which are admixed with the input signal state in the same way as in Equation (P1.28) [Ferraro et al., 2005]. The Wigner distributions related to these two kinds of noise are given by

$$W_{th} = \frac{1}{\pi\,\sigma} e^{-\frac{(\mathcal{E}^2+\mathcal{P}^2)}{\sigma}}, \qquad W_{pa} = \frac{1}{\pi}\,\mathcal{I}_0(\,2|\alpha|\sqrt{\mathcal{E}^2+\mathcal{P}^2}\,)\,e^{-(\mathcal{E}^2+\mathcal{P}^2+|\alpha|^2)}, \tag{P1.33}$$

where $\sigma = \mathrm{cotanh}(\hbar\omega/2\kappa T)$, with k the Boltzmann's constant, T the temperature and $\mathcal{I}_0(x)$ the $0th$ order modified Bessel function of the first kind with argument x. The mean number of dark counts in the selected detection window is given by $\bar{n}_{th} = 1/(e^{2\,\mathrm{arctanh}(1/\sigma)} - 1)$ in the case of thermal noise or by $\bar{n}_{pa} = |\alpha|^2$ if the noise is Poissonian. When the mean number of dark counts is zero, the vacuum state is recovered. It should be outlined that a different treatment of the dark counts problem has been carried out in section P1.3. The reason is that in that case we were not interested in the quantum state of the auxiliary channel, but in the heralded quantum state propagating in the signal waveguides, thus the introduction of the modal purity. Figure P1.9 shows the fidelity $\mathcal{F}(|1_+\rangle, \hat{\rho}_O)$ of the measured state $\hat{\rho}_O$ for an input quantum vortex $|1_+\rangle$ with squeezing factor $s = 0.7$, where the effect of dark counts and total efficiencies of the detectors ($\mu_1 = \mu_2 \equiv \mu$) is shown for thermal (left Figure P1.9) and Poissonian (right Figure P1.9) noise. These fidelities have been worked out applying the Wigner function W_O associated to the output quantum state $\hat{\rho}_O$ on Equation (P1.29). Likewise, W_O has been obtained applying Equations ($P1.19$), ($P1.28$) and ($P1.33$) on W_ρ in the way pointed out in the previous paragraph. It is shown that, in both cases, the detection efficiency produces a stronger impact on the fidelity than the dark counts in the regime depicted. For instance, four-photon waveguide PNRDs based on superconducting niobium-nitride (NbN) nanowires present efficiencies of $\approx 24\%$, a dark count rate of ≈ 5 Hz and a timing resolution of ≈ 20 ns [Mattioli et al., 2015]. Then, in this detection window we would have $\approx 10^{-7}$ dark counts, which is a negligible value. However, the fidelity of the state for this detection efficiency would be highly degraded, with values of $\approx 15\%$. On the other hand, a tungsten transition edge sensor (TES) PNRD with an efficiency close to the 90% and negligible dark counts has been recently shown on an integrated chip [Calkins et al., 2013]. However, TES devices show a poor temporal resolution, being three orders of magnitude slower than the superconducting NbN nanowires. In this case we would obtain fidelities of about the 75%.

Finally, since the PNRDs placed at the outputs of the integrated detection system will measure the number of photons of the state, it would be interesting to calculate

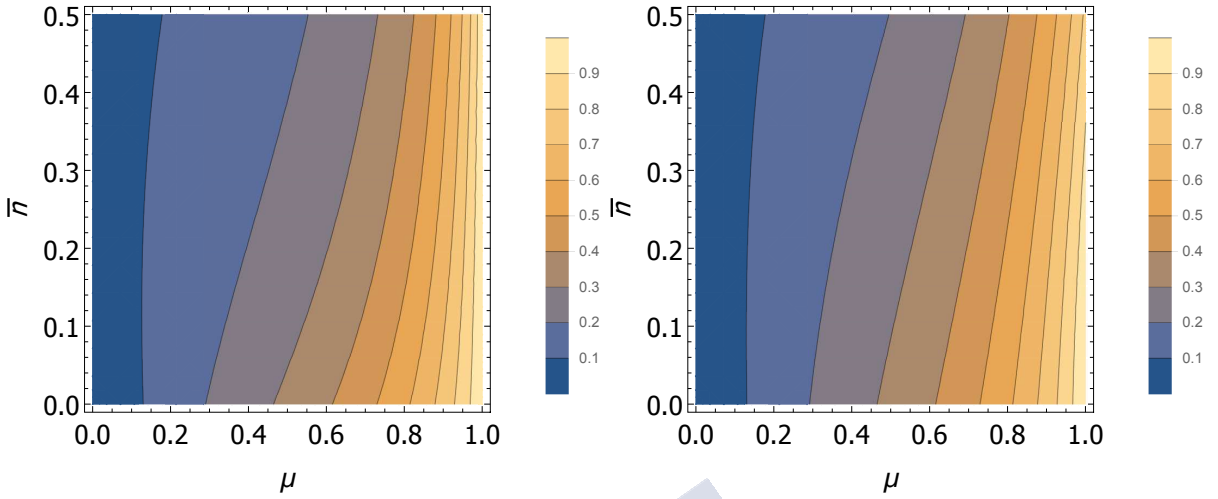


Figure P1.9: Plots of the fidelity $\mathcal{F}$ between the detected state and a quantum vortex $|1_+\rangle$ for a realistic detection system with dark counts of thermal (left) and Poissonian (right) origin. Left: $\mathcal{F}$ vs $\bar{n}_{th}$-μ with s=0.7. Right: $\mathcal{F}$ vs $\bar{n}_{pa}$-μ with s=0.7.

the joint probability distribution of the number of photons n_1' and n_2' measured at each detector under the experimental imperfections previously mentioned. This probability is equivalent to the fidelity between the measured state and the Fock states in each mode $\mathcal{F}(|n_1'\, n_2'\rangle,\, \hat{\rho}_O)$, and it is calculated by means of

$$Pr_{n_1',n_2'} = (2\pi)^2 \iiiint W_O\, W_{n_1'}\, W_{n_2'}\, d\mathcal{E}_1\, d\mathcal{P}_1\, d\mathcal{E}_2\, d\mathcal{P}_2, \tag{P1.34}$$

where $W_{n_j'} = ((-1)^{n'}/\pi)\mathcal{L}_{n'}(2(\mathcal{E}_j^2 + \mathcal{P}_j^2))\, e^{-(\mathcal{E}_j^2+\mathcal{P}_j^2)}$ is the Wigner function corresponding to a Fock state $|n_j'\rangle$. In Figure P1.10 the joint probability distribution of the number of photons $Pr_{n_1',n_2'}$ is depicted for an input vortex state $|1_+\rangle$ with squeezing factor $s = 0.5$ for the ideal (Figure $P1.10$ left) and realistic cases (Figure $P1.10$ center and right). In the ideal case (Figue $P1.10$ left), the difference of one photon between the output modes is hold along the distribution, obtaining an order 1 and + abstract handedness by means of Equation (P1.32). In the case of the use of TES PNRDs with the detection system, where $\mu = 0.88$ and $\bar{n}_{th} \to 0$, it is shown (Figure $P1.10$ center) a contribution from the vacuum which decreases the overall probability of detection, as well as a number of spurious counts which degrade slightly the measurement of the vorticity. On the other hand, Figure $P1.10$ right shows the outcome when superconducting NbN nanowires PNRDs are chosen, with parameters $\mu = 0.24$ and $\bar{n}_{th} = 10^{-7}$. There it is shown that the contribution of the vacuum is so high that more than a half of the input states would be lost without detection and the number of spurious counts would be $\approx 40\%$ of those really related to the input quantum vortex, heavily degrading the ability of the detection system to measure the abstract angular momentum of the quantum state. Therefore, highly efficient PNRDs are necessary in order to have order and handedness detection devices with high-fidelity.

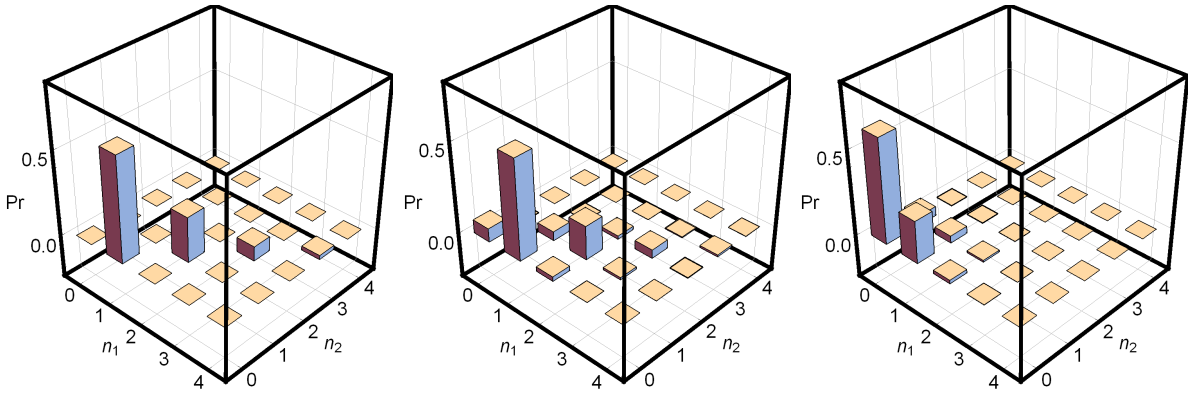


Figure P1.10: Plots of the joint probability distribution of the detected number of photons $Pr_{n_1',n_2'}$ for an input quantum vortex $|1_+\rangle$ with $s = 0.5$. Left: ideal case. Center: realistic case with $\mu = 0.88$ and $\bar{n}_{th} \to 0$. Right: realistic case with $\mu = 0.24$ and $\bar{n}_{th} = 10^{-7}$.

P1.5 Conclusions

A quantum photonic circuit with the ability to produce continuous variable quantum vortex states has been proposed. The device is composed by two stages. The first one produces two single-mode squeezed states by means of PPLN waveguides. The second is a Mach-Zehnder interferometer where photons are subtracted through weakly coupled directional couplers and sent to ancillary waveguides. The detection of a number of photons in these ancillary modes heralds the production of a quantum vortex. We have studied the generation of this family of states in an ideal scenario and have shown their features in the optical field-strength space and phase space. Moreover, we have studied a realistic scenario, where losses, non-unity detection and modal purity have been taken into account through the Wigner function. We have chosen a figure of merit and analyzed different cases. Finally, we have introduced a vortex detection system, which enables the measurement of order and handedness of quantum vortices, and studied the consequences of its inefficient operation. This study opens the possibility of conceiving new QIP protocols by using quantum vortex states.

P2 Engineering continuous and discrete variable quantum vortex states by non-local photon subtraction in a reconfigurable photonic chip

Journal of the Optical Society of America B
VOL. 33 NO. 11 PAGE 2225-2235
ISSN: 0740-3224 (print), 1520-8540 (online)
doi: https://doi.org/10.1364/JOSAB.33.002225

PUBLISHED 1 November 2016

by DAVID BARRAL[1], JESÚS LIÑARES[1] & DANIEL BALADO[1]

[1] Universidade de Santiago de Compostela

Abstract: *We study the production of entangled two- and N-mode quantum states of light in optical waveguides. To this end we propose a quantum photonic circuit which produces a reconfigurable superposition of photon subtraction on two single-mode squeezed states. Under post-selection, continuous variable or discrete variable entangled states with possibilities in quantum information processing are obtained. Likewise, nesting leads to higher dimension entanglement with a similar design, enabling the generation of non-gaussian continuous variable cluster states. Additionally, we show the operation of the device through the generation of quantum vortex states of light and propose an integrated device which measures their order and handedness. Finally, we study the non-gaussianity, non-classicality and entanglement of the quantum states generated with this scheme by means of the optical field-strength distribution, Wigner function and logarithmic negativity.*

P2.1 Introduction

Continuous-variable encoded quantum information processing (CV-QIP) has emerged in recent years as a solid alternative to its discrete-variable counterpart (DV-QIP). Continuous-variable entanglement is the key element for a great number of quantum information protocols [Braunstein and Van Loock, 2005]. These algorithms have been mostly carried out with gaussian entangled states, but demonstrations of the inability of these states to perform entanglement distillation protocols under certain circumstances have been shown [Eisert et al., 2002, Fiurášek, 2002, Giedke and Cirac, 2002]. This has led to the study of non-gaussian states overcoming these drawbacks by means of non-gaussian operations [Takahashi et al., 2010], a prominent example of photon-level quantum light engineering (QLE), which has attracted great attention over the last years [Kim, 2008]. QLE has interesting applications both in QIP as well as in fundamental quantum optics. Manipulating light at the photon level by means of subtraction and addition provides a simple way to construct these non-gaussian states, like the creation of quantum states from classical states by adding a single photon [Agarwal and Tara, 1991, Zavatta et al., 2004] or the generation of Schrödinger-cat-like states through conditional absorption of photons on a squeezed vacuum [Dakna et al., 1997, Neergaard-Nielsen et al., 2006, Ourjoumtsev et al., 2007b], as well as testing the foundations of quantum mechanics, like the bosonic commutation relation by means of the coherent superposition of photon addition followed by photon subtraction (and vice versa) [Kim et al., 2008, Zavatta et al., 2009] or carrying out loophole-free Bell tests [Nha and Carmichael, 2004, García-Patrón et al., 2004]. What is more, the application of this kind of states has been recently shown in CV quantum teleportation, showing the transfer of the non-gaussianity of the state [Lee et al., 2011].

Likewise, in recent times the use of the orbital angular momentum (OAM) spatial degree of freedom of optical vortex fields as a quantum information resource has yielded ground-breaking demonstrations in QIP [Molina-Terriza et al., 2007]. In this regard, there is a class of two-mode non-gaussian states with interesting related features: the quantum vortex states [Agarwal et al., 1997]. These are entangled squeezed eigenstates of the z component of the abstract angular momentum operator $\hat{L}_z$, in analogy with the quantum eigenstates of the spatial OAM operator, which show interesting non-classical properties. Other families of states have been named quantum vortices because of its similarity with spatial-mode optical vortices: SU(2)-transformed Fock states [Agarwal and Banerji, 2006], generalized quantum vortices [Bandyopadhyay and Singh, 2011, Bandyopadhyay et al., 2011, Agarwal, 2011, Banerji et al., 2014], Bessel-Gauss quantum vortex states [Zhu et al., 2012a, Zhu et al., 2012b] or Hermite polynomial quantum vortices [Li et al., 2015]. These are strongly entangled states [Agarwal and Banerji, 2006, Agarwal, 2011], being therefore interesting for CV-QIP. In this direction, Li *et al.* have lately shown their performance in a teleportation protocol [Li et al., 2015]. Moreover, quantum vortices have recently received attention in the context of quantum polarization and Bohmian dynamics [Luis and Sanz, 2013, Luis and Sanz, 2015].

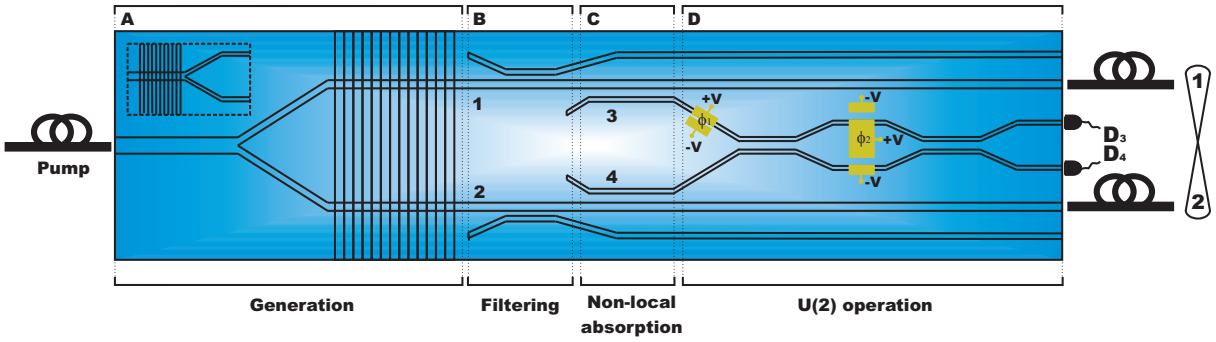


Figure P2.1: Sketch of the photonic circuit proposed for engineering CV entangled quantum states. The first stage is devoted to the generation of the quantum state (A) and pump suppression (B). The production of two single-mode squeezed states is carried out by means of a periodically poled zone. In the inset an alternative design of the generation stage is shown (dashed-line square). In the second stage a pair of directional couplers weakly coupled carry out non-local absorption of photons (C). Finally, in the third stage an U(2) operation on these photons is performed by means of a reconfigurable Mach-Zehnder interferometer (D). Measurement of these photons leads to the entanglement of the input factorable squeezed states.

On the other hand, integrated photonics has led to multiple new approaches on QIP with high success [Tanzilli et al., 2012]. These are based on the processing of quantum states of light in photonic circuits, either DV or CV-encoded [O'brien et al., 2009], and their measurement by single-photon detectors or homodyne detection schemes, respectively [Silberhorn, 2007]. The main features for which integrated optics circuits are crucial to QIP and quantum optics are the sub-wavelength stability and the great miniaturization they show with respect to bulk optics analogs, providing high-visibility quantum interference and scalability, indispensable as the level of complexity of the circuit increases; as well as the optical properties of the materials which make up the waveguides, enabling the generation of quantum states on chip by means of their enhanced non-linear features [Rogers et al., 2015, Dutt et al., 2015], the manipulation by means of their thermo-optic and electro-optic properties [Jin et al., 2014, Masada et al., 2015, Carolan et al., 2015]; and even the integration of detectors in the circuit [Sahin et al., 2014, Najafi et al., 2015]. This leads to high integration density, fidelity and fast control. Therefore, this technology has the potential to turn the real power of quantum mechanics into reality with practical, low cost, standardized, interconnectable and reconfigurable components [Tanzilli et al., 2012].

Bearing all the above in mind, the motivation of this article is to design a quantum circuit on-chip able to generate and manipulate CV entangled states of light by means of directional couplers, phase shifters and conditional measurement; and to show its performance with quantum vortex states. As we will show, entanglement is created by non-local photon absorption of two separable states by means of directional couplers with high transmittivity. This delocalized photon is locally manipulated by means of a reconfigurable interferometer which produces the desired state after photon counting. The

quantum states thus produced hybridize appealing features of both CV (squeezed light) and DV (single photons) [Andersen et al., 2015]. Likewise, the integrated nature of this circuit provides access to entanglement in higher-dimension Hilbert spaces via nesting, with application in measurement-based quantum computing [Andersen et al., 2015]. Furthermore, we demonstrate the versatility of this design as it can also be used to generate DV entangled states by only changing the power of the input pump in such a way that just one monolithic chip can be used in different QIP tasks. Finally, we introduce a possible application of this device by means of the generation of CV and DV quantum vortex states. To the best of our knowledge, this is the first proposal for the generation and manipulation of this family of states in photonic circuits, presenting also an integrated detection scheme able to detect the order and handedness of the quantum vortices. We study quantum features of these states like non-gaussianity, non-classicality and entanglement by means of their associated optical field-strength distribution, Wigner function and logarithmic negativity.

The article is organized as follows: Section II presents a scheme of generation of general CV and DV entangled quantum states in a reconfigurable chip, focusing afterwards on quantum vortices and studying their field-strength probability and phase distributions, as well a discussion about the merits of this proposal. Section III is devoted to study the non-classicality and entanglement through the Wigner distribution and logarithmic negativity of the generated states. Finally, the main results of this article are summarized in Section IV.

P2.2 CV & DV entanglement in a reconfigurable photonic chip

P2.2.1 Device operation

Our QLE-device is pictured in Figure P2.1. It is made up of three stages. The first one (Figure P2.1A) is devoted to the generation of two single-mode squeezed states. There are different approaches in integrated optics with the ability to produce these states [Tanzilli et al., 2012]. One of the more widespread is the use of periodically poled waveguides. Tailoring the non-linearity of the material, usually lithium niobate ($PPLN$) or potassium titanyl phosphate (PPKTP), enables quasi-phase matching of the propagation constants (QPM) improving the efficiency of conversion between the pump and the the desired quantum state [Tanzilli et al., 2001]. First order QPM is given by

$$\Delta\beta \equiv \beta(\omega_p) - \beta(\omega_s) - \beta(\omega_i) = \frac{2\pi}{\Lambda}, \tag{P2.1}$$

where $\Delta\beta$ represents the propagation constants mismatch between a pump photon (p) and its daughters photons, labelled signal (s) and idler (i), caused by dispersion; and Λ is an appropriate period of the inverted domains. This has been shown in the generation of both entangled twin photons [Suhara, 2009] and squeezed states [Yoshino et al., 2007] on chip. Likewise, generation of entanglement in different degrees of freedom, as mode

number, path, frequency or polarization, as well as hyperentanglement has been proposed in recent years through domain engineering on periodically poled waveguides [Saleh et al., 2009, Lugani et al., 2011].

Two different possibilities are sketched in Figure P2.1A. The main one shows a two-mode waveguide pumped with a single-mode coherent field followed by a symmetric Y splitter and two separated waveguides with a common periodic poled grating in the substrate, where the period is tailored such that type-I spontaneous parametric down-conversion (SPDC) is generated [Jin et al., 2014]. The generation of quantum light in waveguides can be mathematically represented by the Momentum operator $\hat{M}$ [Liñares et al., 2008, Barral et al., 2015]. In this case, the corresponding Momentum related to the interacting optical fields (interaction picture) for each waveguide $j = 1, 2$, is given by

$$\hat{M}_j = \frac{1}{2} \iiint \epsilon_0 \chi^{(2)}_{eff} (\sum_k \hat{E}_{j,k})^2 \, dxdydt, \tag{P2.2}$$

with $k = i, s, p$ and ϵ_0 is the vacuum permittivity, $\chi^{(2)}_{eff}$ the second order effective non-linearity in the poling area and the integral is performed over the transverse area of the waveguide and the period of the waves. Likewise, the quantum optical fields are given by

$$\hat{E}_{j,k} \propto \hat{a}_{j,k} \, e^{i\beta_j(\omega_k)z} \, e^{-i\omega_k t} \, \mathbf{e}_{j,k}(x, y) + h.c., \tag{P2.3}$$

with $\hat{a}_{j,k}$ and $\mathbf{e}_{j,k}(x, y)$ the absorption operators and the normalized transverse vector amplitudes related to each mode j, k, respectively. Then, pumping with a strong coherent field and taking into account the conservation of energy and the QPM, in such a way that the signal and idler waves are degenerated in frequency ($\omega_p/2 = \omega_s = \omega_i$), we obtain the following Momentum after applying the above fields into Equation ($P2.2$) and carrying out the integrals [Liñares et al., 2008]

$$\hat{M}^I_j(\Gamma) = -\frac{i\hbar}{2} (\Gamma \hat{a}^{\dagger 2}_j - \Gamma^* \hat{a}^2_j), \tag{P2.4}$$

with Γ a non-linear coupling constant which depends on the pump intensity, the effective non-linearity of the material $\chi^{(2)}_{eff}$, the mode mismatch and the QPM.

On the other hand, the inset in Figure P2.1A sketches a second possibility: a two-mode waveguide with a periodic poled grating satisfying simultaneously QPM for the two modes in a type-0 SPDC followed by a symmetric Y junction. In this case, a coherent pump excited in the odd spatial mode produces a two-mode squeezed vacuum excited in both the even and odd spatial modes of the waveguide which are set to be degenerated in frequency. The selection of the pump mode as odd is related to the overlap integral of the transverse profiles of the interacting modes, which would be zero if the pump mode is even [Saleh et al., 2009]. The excitation of the odd mode of this two-mode waveguide could be carried out by means of a binary phase plate transforming the spatial structure of the pump from a gaussian to a first-order Hermite-gaussian mode, before entering

the waveguide [Bai et al., 2012]. The Momentum operator related to this two-mode periodically poled waveguide is then given by

$$\hat{M}^{II} = -i\hbar(\Gamma'\hat{a}_o^\dagger\hat{a}_e^\dagger - \Gamma'^*\hat{a}_o\hat{a}_e), \tag{P2.5}$$

where o and e stand here for the first (even) and second (odd) excited guided modes. The light finds then the symmetric Y junction afterwards. This device performs the following transformation

$$\begin{pmatrix}\hat{a}_o\\ \hat{a}_e\end{pmatrix} \approx \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}\hat{a}_1\\ \hat{a}_2\end{pmatrix}, \tag{P2.6}$$

where we have used the approximation since part of the light is lost in the junction in the form of radiation modes. Applying Equation (P2.6) into Equation (P2.5), the next Momentum operator is obtained

$$\hat{M}^{II} \to \sum_{j=1,2}\hat{M}_j^I(\Gamma'). \tag{P2.7}$$

It should be outlined that this generation scheme is less efficient than the first one, since the spatial overlap between the the pump and the SPDC modes is not as good as in the first case, due to their different spatial parity. Likewise, in this case part of the entangled quantum states generated in the PPLN zone would be lost at the Y junction, lowering the flux of quantum light. Both schemes lead then to two degenerated single-mode squeezed vacuum states spatially separated, each one given by the following propagation operator

$$\hat{S}_j(\zeta) = e^{\frac{i}{\hbar}\hat{M}_j L_p} = e^{\frac{1}{2}(\zeta\hat{a}_j^{\dagger 2} - \zeta^*\hat{a}_j^2)}, \tag{P2.8}$$

where L_p is the length of the poling area and $\zeta \equiv re^{i\theta_s} = \Gamma L_p$ (or $\Gamma' L_p$) is the complex squeezing parameter generated in the poling area. We outline here that we have chosen above type-I and type-0 SPDC processes in order to have the same polarization in both the signal and idler guided modes.

Moreover, the pump can be filtered by means of properly designed wavelength dependent directional couplers [Kanter et al., 2002, Jin et al., 2014], as shown in Figure P2.1B. This operation is given in terms of operators by

$$\hat{B}_{j\,l}(\theta_j(\omega)) = e^{-i(\theta_j(\omega)/2)\hat{\sigma}_x}, \tag{P2.9}$$

where we have defined $\theta_j(\omega) \equiv 2\kappa(\omega)L_F$ and $\kappa(\omega)$ is the frequency-dependent coupling strength of the directional coupler of length L_F and $\hat{\sigma}_x = \hat{a}_j\hat{a}_l^\dagger + \hat{a}_j^\dagger\hat{a}_l$ is the corresponding Pauli operator. $\hat{B}_{j\,l}$ stands for a directional coupler with reflectivity $r_j = \sin(\theta_j(\omega)/2)$ and transmittivity $t_j = \cos(\theta_j(\omega)/2)$. In our case these devices are designed such that they fully reflect the pump ($\theta(\omega_p) = \pi$) towards the ancillary waveguides l and transmit the squeezed vacuum ($\theta(\omega_s) = 2\pi$) through the signal waveguides $j = 1, 2$. Therefore, we obtain after this stage the following factorable two single-mode squeezed vacuum state

$$|\Psi_B\rangle = \hat{S}_1(\zeta)\hat{S}_2(\zeta)|0_1\,0_2\rangle \equiv |0_{\zeta\,1}\,0_{\zeta\,2}\rangle, \tag{P2.10}$$

where $|0_\zeta\rangle$ accounts for the single-mode squeezed vacuum.

The second stage (Figure P2.1C) is comprised of two directional couplers with high transmittivity, where a small fraction of each mode is reflected and sent to the third stage. The mixing of modes 1 and 3 on one hand and 2 and 4 on the other, produces the following state

$$|\Psi_C\rangle = \hat{B}_{13}(\theta_1)\hat{B}_{24}(\theta_2)|0_{\zeta\,1}\,0_{\zeta\,2}\,0_3\,0_4\rangle, \tag{P2.11}$$

where $\theta_j \equiv \theta_j(\omega_s)$. As input modes 3 and 4 are in the vacuum, using the disentangling theorem for the SU(2) group [Kim, 2008], we can write

$$\begin{aligned}|\Psi_C\rangle = e^{-i\tan(\theta_1/2)\hat{a}_1\hat{a}_3^\dagger}\, t_1^{\hat{a}_1^\dagger\hat{a}_1}\, e^{-i\tan(\theta_2/2)\hat{a}_2\hat{a}_4^\dagger}\, t_2^{\hat{a}_2^\dagger\hat{a}_2} \\ |0_{\zeta\,1}\,0_{\zeta\,2}\,0_3\,0_4\rangle,\end{aligned} \tag{P2.12}$$

which under the conditions of high transmittivity $t_{1,2} \approx 1$ and moderate squeezing can be approximated by [Kim et al., 2008]

$$|\Psi_C\rangle = (1 - i\frac{r_1}{t_1}\hat{a}_1\hat{a}_3^\dagger)(1 - i\frac{r_2}{t_2}\hat{a}_2\hat{a}_4^\dagger)|0_{\zeta\,1}\,0_{\zeta\,2}\,0_3\,0_4\rangle, \tag{P2.13}$$

where single photons propagating through the lossy channels 3 and 4 appear with a certain probability.

The last stage is an integrated Mach-Zehnder interferometer (MZI) composed of two 3 dB directional couplers with an active phase shifter in between, preceded by another phase shifter, with the modes 3 and 4 as input states (Figure P2.1D). This device performs any U(2) operation on the input states adjusting the values of ϕ_1 and ϕ_2, being these the phases generated by the two phase shifters, respectively. The fidelity of this kind of devices has been thoroughly demonstrated along the last decade with both electro-optic and thermo-optic material supports [Martin et al., 2012, Bonneau et al., 2012, Shadbolt et al., 2012, Carolan et al., 2015]. If the material support selected is lithium niobate, considering the waveguides surrounded by electrodes, the phase shift is given by $\phi = n^3 r V \pi L_E/\lambda d$, with n the ordinary or extraordinary refractive index on the material for a given wavelength λ, depending on the input polarization, r the relevant component of the second order non-linear tensor, V the applied voltage, L_E the length of the electrodes and d the distance between them. In the case of the MZI, two reversed electrodes are used in order to lower the required voltage by a factor of two compared with an only phase shifter. A switching efficiency of $\approx 98\%$ and switching times of 4 ns have been reported with a MZI configuration [Bonneau et al., 2012]. Likewise, this operation could be carried out with an alternating $\Delta\beta$ directional coupler, which could improve the integration density and fidelity of the operation, as proposed in [Barral and Liñares, 2015]. Then, applying

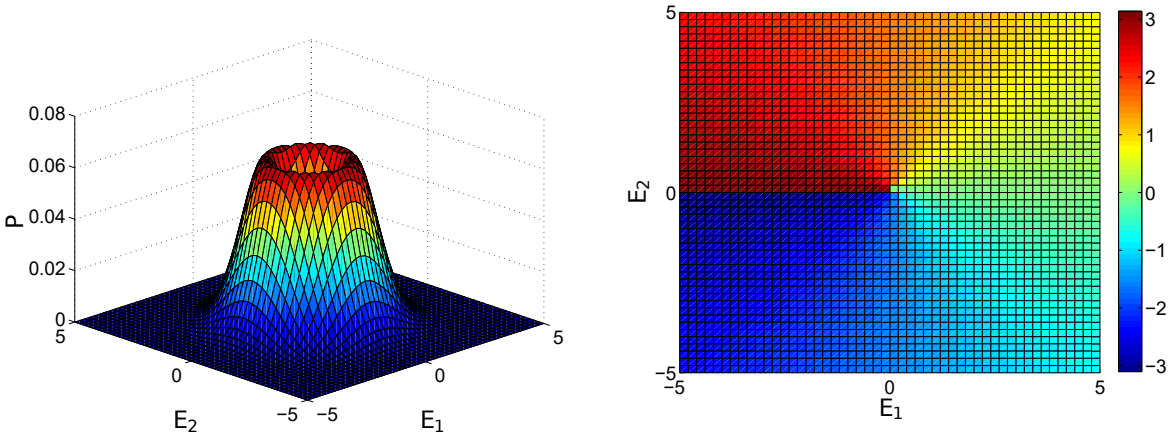


Figure P2.2: Plots of probability (upper figure) and phase (lower figure) densities of a CV circular quantum vortex with squeezing factor $r = 0.3$ and $\eta' = 1$.

this transformation on $|\Psi_C\rangle$ we have the following state [Campos et al., 1989]

$$\begin{aligned}|\Psi_D\rangle &= \hat{U}_{34}(\phi_1,\phi_2)|\Psi_C\rangle \\ &= \{1 - i\frac{r_1}{t_1}e^{i\phi_1/2}\hat{a}_1[\cos(\phi_2/2)\hat{a}_3^\dagger + \sin(\phi_2/2)\hat{a}_4^\dagger] \\ &- i\frac{r_2}{t_2}e^{-i\phi_1/2}\hat{a}_2[-\sin(\phi_2/2)\hat{a}_3^\dagger + \cos(\phi_2/2)\hat{a}_4^\dagger] + \mathcal{O}(r^2)\} \\ &\times |0_{\zeta\,1}\,0_{\zeta\,2}\,0_3\,0_4\rangle,\end{aligned} \tag{P2.14}$$

where $\hat{U}_{34}(\phi_1,\phi_2) = e^{i\phi_2\hat{\sigma}_y/2}\,e^{i\phi_1\hat{\sigma}_z/2}$ and $\hat{\sigma}_y$ and $\hat{\sigma}_z$ are the well known Pauli operators. The terms quadratic in the reflectivity are neglected since large transmittivity is considered.

P2.2.2 CV quantum vortex states

Next, we present a post-selection method to generate non-gaussian CV entangled states. It is easy to see that the detection of a photon in the modes 3 or 4 will herald the subtraction of a delocalized photon, generating the following entangled states

$$\begin{aligned}&\langle 1_3 0_4|\Psi_D\rangle \propto \\ &[\frac{r_1}{t_1}\cos(\phi_2/2)\hat{a}_1 - \frac{r_2}{t_2}\sin(\phi_2/2)e^{-i\phi_1}\hat{a}_2]|0_{\zeta\,1}\,0_{\zeta\,2}\rangle,\end{aligned} \tag{P2.15a}$$

$$\begin{aligned}&\langle 0_3 1_4|\Psi_D\rangle \propto \\ &[\frac{r_1}{t_1}\sin(\phi_2/2)e^{i\phi_1}\hat{a}_1 + \frac{r_2}{t_2}\cos(\phi_2/2)\hat{a}_2]|0_{\zeta\,1}\,0_{\zeta\,2}\rangle.\end{aligned} \tag{P2.15b}$$

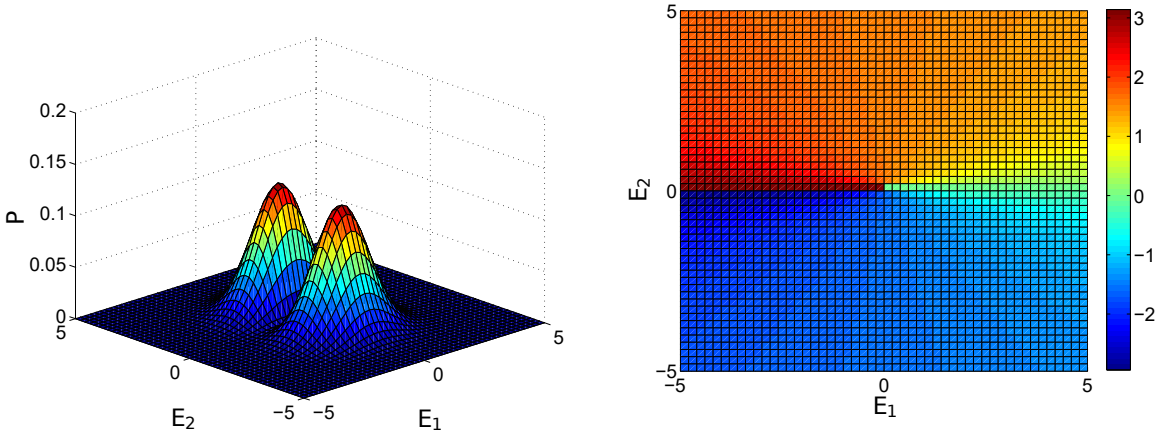


Figure P2.3: Plots of probability (upper figure) and phase (lower figure) densities of a CV elliptical quantum vortex with squeezing factor $r = 0.3$ and $\eta' = 5$.

These measurements can be carried out with single-photon avalanche photodiodes (SPADs) or superconducting single photon detectors (SSPDs), inter alia [Eisaman et al., 2011]. Moreover, taking into account the single-mode squeezing Bogoliubov transformation [Agarwal, 2012]

$$\hat{S}^{\dagger}(\zeta)\hat{a}\hat{S}(\zeta) = \hat{a}\cosh(r) + \hat{a}^{\dagger}\sinh(r)\, e^{i\theta_s}, \tag{P2.16}$$

we can write Equations (P2.15) as follows:

$$\langle 1_3 0_4|\Psi_D\rangle \propto |1_{\zeta 1} 0_{\zeta 2}\rangle - \eta\, \tan(\phi_2/2) e^{-i\phi_1}|0_{\zeta 1} 1_{\zeta 2}\rangle, \tag{P2.17a}$$

$$\langle 0_3 1_4|\Psi_D\rangle \propto |1_{\zeta 1} 0_{\zeta 2}\rangle + \eta\, \cot(\phi_2/2) e^{-i\phi_1}|0_{\zeta 1} 1_{\zeta 2}\rangle, \tag{P2.17b}$$

with $\eta = \frac{r_2 t_1}{r_1 t_2}$ and where $|1_{\zeta}\rangle = \hat{S}(\zeta)\hat{a}^{\dagger}|0\rangle$ accounts for a squeezed single photon. Both states are two-mode strongly entangled states, as we will see in the next section. Fixing the phase ϕ_1 to any value $(2n-1)\pi/2$ we obtain an elliptical vortex state, with a degree of ellipticity dependent on the values of ϕ_2 and η. Focusing on Equation (P2.17a), we can write the elliptical quantum vortex as

$$|\Psi\rangle = \frac{1}{\sqrt{1+\eta'^2}}(|1_{\zeta 1} 0_{\zeta 2}\rangle + (-1)^n i\, \eta' |0_{\zeta 1} 1_{\zeta 2}\rangle), \tag{P2.18}$$

where we have defined $\eta' = \eta\, \tan(\phi_2/2)$ as an ellipticity factor. It is important to outline that this approach enables the manipulation of the quantum state as well as correct fabrication errors or asymmetries between the couplers B_{13} and B_{24}, represented by values of $\eta \neq 1$. Likewise, adjusting the phase of the second phase shifter such that

$\phi_2 = 2\arctan(\eta^{-1})$ (or $\phi_2 = 2\arctan(\eta)$ in Eq. (P2.17b)) we obtain the vortex state of the quantized optical field or circular quantum vortex [Agarwal et al., 1997]

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|1_{\zeta 1}0_{\zeta 2}\rangle + (-1)^n i\,|0_{\zeta 1}1_{\zeta 2}\rangle). \tag{P2.19}$$

The vorticity field is better visualized in the optical field-strength space (sometimes referred as configuration-space-like space). In this representation $\mathcal{E}$ is the eigenvalue of the optical field-strength operator $\hat{\mathcal{E}} = (\hat{a}+\hat{a}^\dagger)/\sqrt{2}$, proportional to the first quadrature of the optical field, and analogously $\hat{\mathcal{P}} = -i(\hat{a}-\hat{a}^\dagger)/\sqrt{2}$ is related to the second quadrature [Schleich, 2001]. Then, the normalized wavefunction corresponding to the quantum state heralded when a click in mode 3 is measured is given by [Agarwal, 2012]

$$\Psi(\mathcal{E}_1,\mathcal{E}_2) = \sqrt{\frac{2}{\pi(1+\eta'^2)e^{4r}}}(\mathcal{E}_1 + (-1)^n\, i\eta'\,\mathcal{E}_2)\, e^{-\frac{\mathcal{E}_1^2+\mathcal{E}_2^2}{2e^{2r}}}, \tag{P2.20}$$

where we have chosen ζ real. Figures $P2.2$ and $P2.3$ show the probability $P = |\Psi(\mathcal{E}_1,\mathcal{E}_2)|^2$ and phase $\varphi = \arg\{\Psi(\mathcal{E}_1,\mathcal{E}_2)\}$ densities for a squeezing factor $r = 0.3$ and different values of η', namely a circular squeezed vortex for $\eta' = 1$ (Figure $P2.2$) and an elliptical squeezed vortex for $\eta' = 5$ (Figure $P2.3$). Comparing the probability densities it is easy to visualize the lack of symmetry as the value of η' moves away from 1. Likewise, comparing the phase densities we can see the appearance of a phase step as ellipticity increases.

It is important to outline here that the circular squeezed vortex is an eigenstate of the abstract angular momentum operator $\hat{L}_z = -i(\hat{\mathcal{E}}_1\partial_{\mathcal{E}_2} - \hat{\mathcal{E}}_2\partial_{\mathcal{E}_1})$ with eigenvalues ± 1, so the vortex state carries an orbital angular momentum of $\pm\hbar$. This fact could be interesting for implementing specific CV-QIP protocols. In this respect, this operator can be implemented by means of a 3 dB DC with two photon number-resolving detectors (PNRDs) connected at its outputs [Mattioli et al., 2015]. This is easily proved applying the operator which represents the DC, given by Equation (P2.9) with $\theta(\omega_s) = \pi/2$, on the abstract angular momentum operator above presented

$$\hat{L}'_z = \hat{B}_{12}(\pi/2)\,\hat{L}_z\,\hat{B}^\dagger_{12}(\pi/2) = \hat{n}'_1 - \hat{n}'_2, \tag{P2.21}$$

where $\hat{n}'_j = \hat{a'}^\dagger_j\hat{a}'_j$ is the photon number operator related to each mode j and the prime denotes the output modes related to the DC. Therefore, measuring the difference of number of photons at each output $1'$ and $2'$, we can obtain the order and abstract handedness of the quantum vortex associated to the modes 1 and 2. This supports the use of this kind of states in an hybrid QIP, where DV information is transported by a CV channel, and recovered by this measurement technique. Moreover, it should be remarked that the use of SPADs in the measurement of the ancillary photons results in the conditional state to be mixed, since photodiodes do not resolve the number of photons, but under the conditions above outlined, specifically high transmittivity of the directional couplers and moderate squeezing, the resultant state is close to the ideal one [Kim, 2008]. This fact is

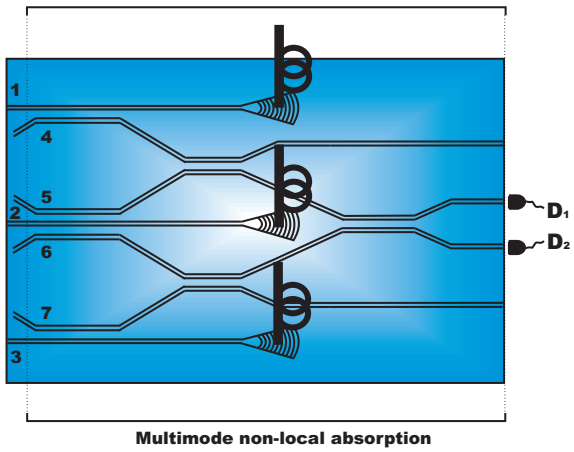


Figure P2.4: Sketch of the photonic circuit proposed for engineering three-mode CV entangled quantum states. A click in detectors D_1 or D_2 heralds the entangling of the three input states.

fully prevented if SSPDs are used. However, if necessary, a model of inefficient detection which could be readily adapted to this scheme to fit real data from an experiment has been introduced in [Ourjoumtsev et al., 2009].

Likewise, we would like to outline that higher Hilbert dimensions are accessible by this scheme via the nesting of periodically poled waveguides and 3 dB DCs. This is achieved by means of the multimode non-local absorption of one photon from a number of single-mode squeezed vacua excited in different waveguides. To illustrate, a three-mode CV entangled state could be produced by the generation of three squeezed vacua in the waveguides 1, 2 and 3 in a similar way as that shown above (Figure P2.1A), and the absorption of photons by means of four weak DCs, as shown in Figure P2.4. The quantum state after going through these couplers would be given by

$$|\Psi\rangle = (1 - i\frac{r_1}{t_1}\hat{a}_1\hat{a}_4^\dagger)(1 - i\frac{r_2}{\sqrt{2}t_2}\hat{a}_2(\hat{a}_5^\dagger + \hat{a}_6^\dagger))(1 - i\frac{r_3}{t_3}\hat{a}_3\hat{a}_7^\dagger) \\ |0_{\zeta 1}\, 0_{\zeta 2}\, 0_{\zeta 3}\, 0_4\, 0_5\, 0_6\, 0_7\rangle. \tag{P2.22}$$

The photons coupled to the lossy channels find then a series of 3 dB DCs which erase the information about the source from which the photon is absorbed. The measurement of one photon in detector D_1 would herald the entangling of the three single-mode squeezed states in the following way

$$\langle 1_{D1}|\Psi\rangle \propto \\ (\frac{r_1}{t_1}|1_{\zeta 1}\, 0_{\zeta 2}\, 0_{\zeta 3}\rangle + \frac{r_2}{t_2}e^{i\pi/4}|0_{\zeta 1}\, 1_{\zeta 2}\, 0_{\zeta 3}\rangle + \frac{r_3}{t_3}e^{i\pi/2}|0_{\zeta 1}\, 0_{\zeta 2}\, 1_{\zeta 3}\rangle). \tag{P2.23}$$

A similar outcome would be obtained detecting a photon with detector D_2. In this configuration, the entangled modes are collected into fibers by means of grating couplers. This scheme can be easily widened to a higher number of modes at the cost, however, of

lowering the probability of generation of the state, since some of the absorbed photons are lost. Additionally, an adapted scheme to temporal multiplexing with heralding could be used to get access to ultra-large number of entangled modes [Yokoyama et al., 2013].

It should be noted that the states thus produced are interesting in the context of continuous variable cluster states. Recently, it has been demonstrated that non-ideal gaussian cluster states would present limitations in long computations [Ohliger et al., 2010], introducing the necessity of a resource of non-gaussian states for measurement-based quantum computing [Andersen et al., 2015]. This device could act as a generator of path-encoded non-gaussian CV cluster states.

P2.2.3 DV quantum vortex states

Additionally, it is interesting to note that this device could be also used for a second purpose. If instead of being interested on CV we move to DV-QIP, this design shows the ability to produce entanglement as well. This is directly carried out by lowering the power of the input pump, in such a way that two-photon states are generated at the waveguides 1 and 2. Taking the lower terms of the the single-mode squeezing operator given by Equation (P2.8), we would have at each waveguide j the following quantum state [Agarwal, 2012]

$$|0_{\zeta\, j}\rangle \approx \frac{1}{\sqrt{\cosh(r)}}(|0_j\rangle + \frac{e^{i\theta_s}\tanh(r)}{\sqrt{2}}\,|2_j\rangle), \tag{P2.24}$$

having a two-photon state with a certain probability. We have neglected here higher-order photon-number states since they will be produced with a very low probability in this regime. Substituting these states in Equation (P2.14), and following the same steps above outlined for the generation of CV quantum vortex states, the heralded output quantum states after detection of a single photon in modes 3 or 4 would be given by

$$\langle 1_3 0_4|\Psi_D\rangle \propto |1_1 0_2\rangle - \eta\,\tan(\phi_2/2)e^{-i\phi_1}|0_1 1_2\rangle, \tag{P2.25a}$$

$$\langle 0_3 1_4|\Psi_D\rangle \propto |1_1 0_2\rangle + \eta\,\cot(\phi_2/2)e^{-i\phi_1}|0_1 1_2\rangle, \tag{P2.25b}$$

in such a way that adjusting the phases ϕ_1 and ϕ_2 we have any state on the Bloch sphere, or a qubit. Choosing odd multiples of $\pi/2$ for ϕ_1 we obtain again quantum states as these given by Equation (P2.18) for $r = 0$. These are non-squeezed elliptical vortex states. Likewise, setting the second phase shifter in the MZI in such a way that $\phi_2 = 2\arctan(\eta^{-1})$ (or $\phi_2 = 2\arctan(\eta)$), we will have a circular non-squeezed quantum vortex, eigenstate of $\hat{L}_z$ as well. The abstract angular momentum is in this case $\pm\hbar$ per photon. Figure $P2.5$ is devoted to show the probability densities corresponding to these non-squeezed vortex states for values of $\eta' = 1$ and 5 in order to compare with those shown in Figures $P2.2$ and $P2.3$. Note the higher localization of these states in the optical field-strength space reaching larger values of probability in comparison with their squeezed counterparts. The phase densities will be the same as those sketched in Figures $P2.2$ and $P2.3$.

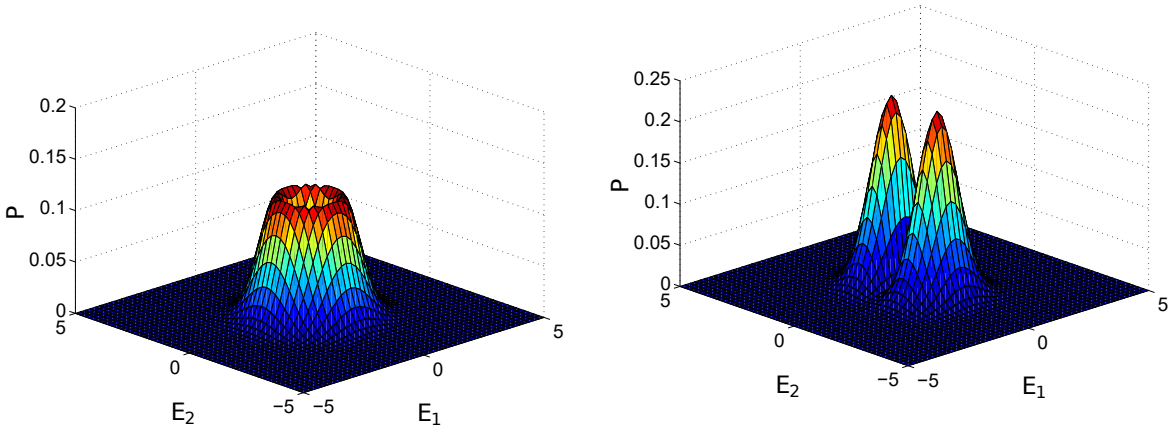


Figure P2.5: Plots of probability density of DV quantum vortex states with $\eta' = 1$ (circular, upper figure) and 5 (elliptical, lower figure).

P2.2.4 Discussion

Now, we address some of the merits that this scheme shows. Firstly, we would like to point out that a similar scheme has been proposed in bulk optics with polarization-encoded Schrödinger kittens [Ourjoumtsev et al., 2007a, Ourjoumtsev et al., 2009]. However, our integrated scheme presents noteworthy differences as well as new possibilities. Current technology has shown recently the ability to generate in few-centimeters-in-size chips bright squeezed light [Yoshino et al., 2007] as well as both high-fidelity manipulation [Carolan et al., 2015] and fast modulation [Bonneau et al., 2012] of quantum states of light. We can estimate the performance of our device with experimentally available parameters. Propagation losses around $\approx 0.3\ dB\ cm^{-1}$ have been reported in a quantum relay chip in the telecommunication C band [Martin et al., 2012]. Such advanced device showed geometrical losses of $\approx 1\ dB$ due to the sinusoidal bends related to the DCs. Likewise, a SPDC photon flux as high as 1.4×10^7 pairs $nm^{-1}\ mW^{-1}\ s^{-1}$ in a 1 cm-long PPLN waveguide operating in the telecom C and L bands has been recently reported [Jin et al., 2014]. With these parameters, considering a typical value of 1 dB in the output coupling losses using micro-lenses systems (guide-to-fibre), SSPDs in the lossy channels with typical detection efficiencies of $\approx 10\%$ and a transmittivity of 99% in the DCs related to the non-local absorption stage (Figure P2.1C), a flux of $\approx 1.25 \times 10^4\ nm^{-1}\ mW^{-1}\ s^{-1}$ entangled quantum states would be measured in a 5 cm-long chip after the PPLN zone. It is important to outline that this figure could be improved by the optimization of the propagation efficiency (losses as low as 0.1 $dB\ cm^{-1}$ have been reported) and with the use of high-efficiency detectors, like the future superconducting nanowire-based single photon detectors [Sahin et al., 2014].

Likewise, guided modes of light have also proven to be robust carriers of quantum information over long distances and in various degrees of freedom [Tanzilli et al., 2012]. Specifically, our approach is compact and polarization independent which, on the one hand, increases the stability and gets rid of insertion losses; and, on the other hand, allows long-distance transmission, since polarization maintaining fibers which show higher losses than standard fibers are not necessary in order to guide the output light. It also presents access to an universal set of states as well as error tolerance to the fabrication defects or asymmetries in the couplers responsible of the non-local absorption of photons, thanks to the reconfigurable circuit of stage 3, in addition to the capacity of dealing with higher-dimension quantum states in a reasonable size by means of nesting (scalability), issues difficult to manage with bulk optics circuits. Furthermore, our proposal shows the novel ability of generation of both CV and DV entangled quantum states in the same device by only changing the measurement configuration in a such a way that just a monolithic circuit can be applied on different QIP tasks. Another interesting feature of this scheme is an improvement of a factor of two in the probability of generation of the non-gaussian states in comparison with other proposals where only one lossy channel is used. However, it could be argued that with this configuration the probability of success in the generation of DV entangled states is low in comparison with other current methods [Jin et al., 2014]. This is the price to be paid in this hybrid configuration. This issue could be sorted out via the use of tunable electro-optic directional couplers [Martin et al., 2012, Barral and Liñares, 2015] in the second stage of the circuit (Figure P2.1C), with the aim of acting as a 3 dB directional couplers and sending, with a probability of 50% for each channel 1 and 2, one photon to the lossy channels 3 or 4, respectively.

Additionally, we would like to outline that this scheme could be also used in entangled coherent state QIP. The squeezed vacuum and squeezed single photon states are also known as even and odd Schrödinger kittens, respectively, due to the high fidelity they show with odd Schrödinger cats for low values of squeezing [Lund and Ralph, 2005, Neergaard-Nielsen et al., 2006]. They can be written as

$$|0_\zeta\rangle \propto |\alpha\rangle + |-\alpha\rangle, \qquad |1_\zeta\rangle \propto |\alpha\rangle - |-\alpha\rangle. \tag{P2.26}$$

Using this representation in, for instance, Equation (P2.17a), we obtain

$$\begin{aligned}\langle 1_3 0_4|\Psi_D\rangle \propto & C_-(|\alpha\rangle_1|\alpha\rangle_2 - |-\alpha\rangle_1|-\alpha\rangle_2) \\ & + C_+(|\alpha\rangle_1|-\alpha\rangle_2 - |-\alpha\rangle_1|\alpha\rangle_2),\end{aligned} \tag{P2.27}$$

with $C_\pm = 1 \pm \eta \tan(\phi_2/2) e^{-i\phi_1}$. It has been shown that two-mode entangled coherent states of this kind can perform quantum teleportation and rotations of coherent qubits [Jeong et al., 2001, Ourjoumtsev et al., 2009], opening the possibilities of this integrated device in coherent quantum communications and quantum computation through the tuning of the coefficients $C_\pm(\phi_1, \phi_2)$. In fact, applying the scheme proposed in Figure $P2.4$ in this representation, cluster-type entangled coherent states could be produced [Munhoz et al., 2008].

Finally, it is noted that the use of a directional coupler in the generation of a different family of quantum vortices has been dealt with in [Bandyopadhyay and Singh, 2011], but in that proposal neither the problem of generation of the non-gaussian states necessary to produce vorticity nor the reconfigurability necessary for manipulation and the measurement of these states were covered.

Now, in the next section we study the quantum features of the quantum states produced by this device.

P2.3 Non-classicality and entanglement

We start this section studying the negativity of the Wigner function to assess qualitatively the non-classicality and of the quantum states generated with this scheme. We would like to outline that these features are related with the non-gaussian nature of these states. As the relative phase does not affect the non-classicality and the entanglement of the quantum states presented above, we focus our attention on the quantum vortices without loss of generality. In order to simplify the calculation we start with the following ansatz

$$|L\rangle = \frac{1}{\sqrt{1+\eta'^2}}\{|10\rangle + i\eta'|01\rangle\}. \tag{P2.28}$$

This state is an elliptical DV quantum vortex, equivalent to an elliptical CV quantum vortex given by Equation (P2.18) if $\zeta = 0$ is chosen. The Wigner function of this state can be readily worked out by the usual methods obtaining [Furusawa, 2015]

$$\begin{aligned} W_{|L\rangle}(\alpha_1,\alpha_2) = \frac{4}{\pi^2\,(1+\eta'^2)} e^{-2(|\alpha_1|^2+|\alpha_2|^2)} \\ \{(4|\alpha_1|^2-1) + \eta'^2(4|\alpha_2|^2-1) - 8\eta'|\alpha_1||\alpha_2|\sin(\delta_1-\delta_2)\}, \end{aligned} \tag{P2.29}$$

where $\alpha_j \equiv |\alpha_j|e^{i\delta j} = (\mathcal{E}_j + i\mathcal{P}_j)$ with $j = 1, 2$. This is clearly a non-gaussian Wigner function. The regions of phase space with negative values of this function give a qualitative measure of the non-classicality of the state, since classical states are positive along the entire space. They are given by the following condition

$$|\alpha_1|^2+\eta'^2|\alpha_2|^2-2\eta'|\alpha_1||\alpha_2|\sin(\delta_1-\delta_2) < \frac{1+\eta'^2}{4}. \tag{P2.30}$$

So this points out the non-classicality of the DV quantum vortices given by Equations (P2.25) when $\phi_1 = \pm\pi/2$, since there are a great number of values of α_1, α_2 and ϕ_2 which fulfill the condition (P2.30) for a given η'. For instance, in the case of a DV circular quantum vortex, the following condition is obtained

$$|\alpha_1|^2+|\alpha_2|^2-2|\alpha_1||\alpha_2|\sin(\delta_1-\delta_2) < 1/2. \tag{P2.31}$$

Next, we pay attention on CV quantum vortices given by Equation (P2.18). With the help of the following relation between density matrices related by a squeezed transformation [Agarwal, 2012]

$$\hat{\tilde{\rho}} = \hat{S}(\zeta)\hat{\rho}\hat{S}^\dagger(\zeta) \rightarrow W_{\hat{\tilde{\rho}}}(\alpha) = W_{\hat{\rho}}(\tilde{\alpha}), \tag{P2.32}$$

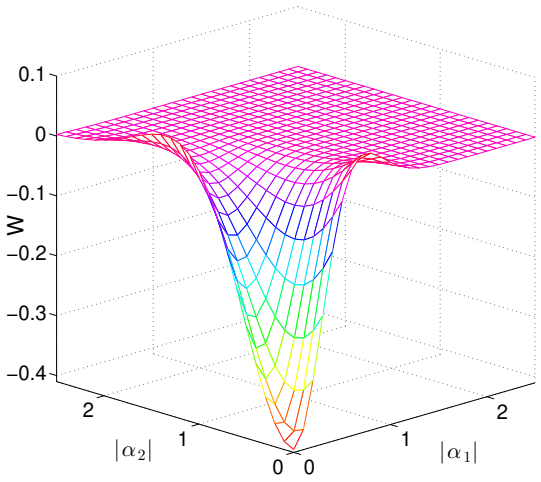


Figure P2.6: Plot of the Wigner function related to a CV circular quantum vortex with $r = 0.3$. We have set $\delta_1 = \pi/2$ and $\delta_2 = 0$ in order to represent it in two dimensions.

where $\tilde{\alpha} = \alpha \cosh(r) - \alpha^* e^{i\theta_s} \sinh(r)$, we can directly relate the Wigner function for the ansatz above calculated, Equation (P2.29), with the Wigner function of the family of quantum states given by Equations (P2.17) by only exchanging α_j by $\tilde{\alpha}_j$ in that equation. This of course keeps the non-gaussian shape of the Wigner function. Likewise, the negative regions are also obtained with the same substitution in Equation (P2.30). For instance, setting ζ real we have

$$|\alpha_1 e^r|^2 + \eta'^2 |\alpha_2 e^{-r}|^2 - 2\eta' |\alpha_1||\alpha_2| \sin(\delta_1 - \delta_2) < \frac{1 + \eta'^2}{4}. \tag{P2.33}$$

It is shown in Figure P2.6 a plot of the Wigner function corresponding to a circular CV vortex state ($\eta' = 1$) with a real squeezing factor with value $r = 0.3$ and where we have set $\delta_1 = \pi/2$ and $\delta_2 = 0$ in order to be able to sketch it in two dimensions [Seshadreesan et al., 2015]. It is easy to see that it takes on negative values along a large area of the phase space, as given by Equation (P2.33).

On the other hand, we are interested on a quantitative measure of entanglement. To this end we choose here the logarithmic negativity because of its appealing properties. Namely, that it is computable, additive and provides an upper bound on the efficiency of distillation, so it measures to which extent a quantum state is useful for a certain QIP protocol or how many resources are needed to produce it. This is defined by [Vidal and Werner, 2002]

$$E = \log_2(1 + 2\mathcal{N}), \tag{P2.34}$$

with $\mathcal{N}$ the modulus of the sum of all negative eigenvalues of the partial transpose of the density matrix associated to the state to be measured. Furthermore, for pure states

Equation (P2.34) can be written as

$$E = 2\,\log_2\left(\sum_\alpha c_\alpha\right), \tag{P2.35}$$

where c_α are the Schmidt coefficients of the pure state in a suitable orthonormal basis $e_\alpha^{(j)}$, with $j = 1, 2$ [Vidal and Werner, 2002]. For a given squeezing, the maximum CV entangled vortex states will be the circular ones given by Equation (P2.19). With the help of the circular basis

$$\hat{b}_1 = \frac{\hat{a}_1 - i\,e^{in\pi}\,\hat{a}_2}{\sqrt{2}}, \qquad \hat{b}_2 = \frac{\hat{a}_1 + i\,e^{in\pi}\,\hat{a}_2}{\sqrt{2}}, \tag{P2.36}$$

we can easily work out the Schmidt decomposition of the circular quantum vortex given in Equation (P2.19). In this basis the state can be written as

$$|\Psi\rangle = \hat{S}_{12}(\zeta)\,\hat{b}_1^\dagger\,|0_1\,0_2\rangle, \tag{P2.37}$$

where $\hat{S}_{12}(\zeta) = \exp\{\zeta\hat{b}_1^\dagger\hat{b}_2^\dagger - \zeta^*\hat{b}_1\hat{b}_2\}$ is the two-mode squeezing operator. Applying the decomposition of the two-mode squeezing operator for $\zeta = r$ (Appendix A), we can write the state in the circular Fock basis as

$$|\Psi\rangle = \sum_{n=0}^{\infty} c_n(r)|n+1, n\rangle, \tag{P2.38}$$

with $c_n(r) = \sqrt{n+1}\,\tanh^n(r)/\cosh^2(r)$ the corresponding Schmidt coefficients. Setting these values on Equation (P2.35), we have

$$E = 2\,\log_2\left(\cosh^{-2}(r)\,(1 + \sum_{n=1}^{\infty}\sqrt{n+1}\tanh^n(r)\,)\right). \tag{P2.39}$$

So entanglement quickly increases with squeezing and, in the limit of no squeezing ($r = 0$), the state would be fully untangled ($E = 0$), since it would be equivalent to not having quantum light within the chip at all. It is interesting to note that the same logarithmic negativity has been obtained studying the generalized vortex state produced by means of photon subtraction from a two-mode squeezed vacuum [Agarwal, 2011]. It should be outlined however, that these states present different quantum features. For instance, they are not eigenstates of $\hat{L}_z$, as could be readily shown by calculating the expected value of the abstract angular momentum.

Generalizing the above result to CV elliptical vortex states, E will decrease as the ellipticity η' tends to zero in the following way

$$\begin{aligned} &E = 2\,\log_2\left(\sum_n |c_n(r,\Phi)|\right) = \\ &2\,\log_2\left(\cosh^{-2}(r\sin(2\Phi)\,(1 + \sum_{n=1}^{\infty}\sqrt{n+1}|\tanh^n(r\sin(2\Phi))|)\right), \end{aligned} \tag{P2.40}$$

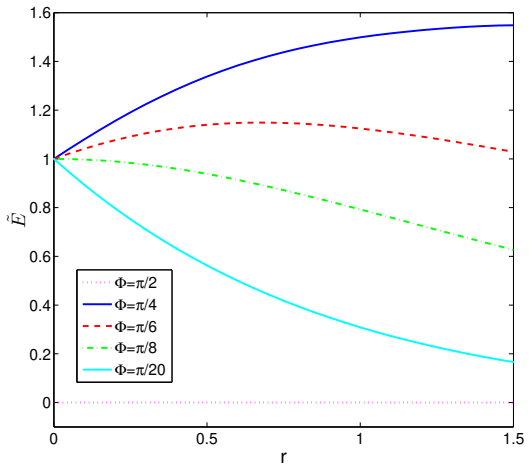


Figure P2.7: Ratio between the logarithmic negativity of CV vortex states and that corresponding to a two-mode squeezed vacuum over a range of values of the squeezing parameter r and different values of ellipticity given by Φ.

where we have defined $\Phi = \arctan(\eta')$ and $|c_n(r,\Phi)|$ are the Schmidt coefficients, which recover the circular vortex state for $\Phi = (2l+1)\pi/4$ ($|c_n(r,(2l+1)\pi/4)| \equiv c_n(r)$), with l any integer. A detailed calculation of this Equation is shown in Appendix A. On the other hand, unlike CV quantum vortices, DV vortex states keeps the value of logarithmic negativity equal to 1 for any Φ different of $\pi/2$ [Agarwal, 2012], since there are always an eigenbasis which diagonalizes the state (Equation (P2.42) with $\Phi = \phi_2/2$).

Therefore, the most interesting states in terms of entanglement presented here are the CV quantum vortices. In order to visualize the degree of entanglement these states reach, we use the ratio between the logarithmic negativity of the quantum vortices and that corresponding to a two-mode squeezed vacuum, $2\log_2(e^r)$, given by the following relation [Agarwal, 2011]

$$\tilde{E} = \left(\sum_n c_n(r,\Phi)\, e^{-r} \right)^2 . \tag{P2.41}$$

In Figure $P2.7$ this ratio is shown over a range of values of r and for various values of ellipticity Φ (or equally η'). It is noted that $\tilde{E} > 1$ for $\Phi = \pi/4$ (solid, blue), in such a way that the circular vortex state entanglement increases faster and higher with squeezing than that related to the two-mode squeezed vacuum. Even for values different but close to $\pi/4$ the state keeps a strong entanglement for moderate values of squeezing (dashed, red). As we get closer to values of Φ multiples of π, the state becomes linearized, or experiences a lost of symmetry (Figure P2.2 vs Figure P2.3), and the entanglement diminishes with r, such that $\tilde{E} \to 0$ (dot-dashed, green & solid, cyan). In the limit of $\Phi = \pi/2$ the state is fully untangled and $\tilde{E} = 0$ (dot, magenta). It is interesting to note that we observe an inverse relationship between generalized quantum polarization in the optical field-strength

space and entanglement [Liñares et al., 2011, Barral et al., 2013]. The lack of symmetry in this space increases the polarization degree and decreases the entanglement.

P2.4 Conclusions

In this article we have proposed a monolithic quantum photonic circuit for QLE via a reconfigurable superposition of photon subtraction on two single-mode squeezed states produced with periodically poled waveguides, directional couplers and phase shifters. This scheme allows the generation of both CV and DV strongly entangled quantum states of light in general, and quantum vortices in particular, on the same chip, modifying only the power of the input pump from which the quantum states are generated. We have demonstrated the ability of nesting that this design presents, increasing the number of dimensions of CV entanglement and thus showing a great potential in future integrated applications for QIP. Moreover, we have studied the application of this device to the production, manipulation and detection of photonic quantum vortex states, showing a measurement scheme of vorticity order and abstract handedness with possibilities in QIP. We have also studied relevant quantum properties like non-gaussianity, non-classicality and entanglement, via the optical field-strength probability distributions, Wigner function and logarithmic negativity. Specifically, we have shown this scheme produces large values of entanglement for moderate values of squeezing.

P2.5 Acknowledgements

Authors wish to acknowledge the partial financial support of this work by Ministerio de Economía y Competitividad, Central Government of Spain, Contract number FIS2013-46584-C2-1-R, and Fondo Europeo de Desenvolvemento Rexional 2007-2013 (FEDER).

P2.6 Appendix A

With the help of the following transformation

$$\begin{pmatrix}\hat{b}_1\\ \hat{b}_2\end{pmatrix} = \begin{pmatrix}\cos(\Phi) & -i\,e^{in\pi}\sin(\Phi)\\ \sin(\Phi) & i\,e^{in\pi}\cos(\Phi)\end{pmatrix}\begin{pmatrix}\hat{a}_1\\ \hat{a}_2\end{pmatrix}, \tag{P2.42}$$

where $\Phi = \arctan(\eta')$, we can readily rewrite Equation (P2.18) in the new basis as

$$|\Psi\rangle = \hat{S}_1(r\cos(2\Phi))\,\hat{S}_2(-r\cos(2\Phi))\,\hat{S}_{12}(r\sin(2\Phi))\,|1_1 0_2\rangle. \tag{P2.43}$$

The single-mode squeezing operators $\hat{S}_1$ and $\hat{S}_2$ in the previous Equation do not contribute to entanglement since they can be cancelled out by local unitary operations on each mode [Kim et al., 2002], so they can be neglected in this calculation onwards. Applying the decomposition theorem of the two-mode squeezing operator

$$\hat{S}_{12}(r) = e^{\tanh(r)\,\hat{b}_1^\dagger\hat{b}_2^\dagger}\,e^{-\ln\cosh(r)(\hat{b}_1^\dagger\hat{b}_1+\hat{b}_2^\dagger\hat{b}_2+1)}\,e^{-\tanh(r)\,\hat{b}_1\hat{b}_2}, \tag{P2.44}$$

we obtain the following state

$$|\Psi'\rangle = \sum_{n=0}^{\infty} c_n(r,\Phi)|n+1,n\rangle, \tag{P2.45}$$

with $c_n(r,\Phi) = \sqrt{n+1}\tanh^n(r\sin(2\Phi))/\cosh^2(r\sin(2\Phi))$ and where we have applied the local operations above discussed, that is $|\Psi'\rangle = \hat{S}_1(-r\cos(2\Phi))\,\hat{S}_2(r\cos(2\Phi))\,|\Psi\rangle$. Since these coefficients can show negative values, we calculate the negativity $\mathcal{N}$ of this state, given by $\mathcal{N} = |\sum_k \lambda_k|$, with λ_k the negative k eigenvalues of the partial transpose of the density operator $\hat{\rho}^{PT}$. From Equation (P2.45) the partial transpose is

$$\hat{\rho}^{PT} = \sum_{n,m=0}^{\infty} c_n(r,\Phi)c_m(r,\Phi)\,|n+1,m\rangle\langle m+1,n|. \tag{P2.46}$$

We can diagonalize the non-positive terms ($n \neq m$) of this matrix by means of the following eigenvectors

$$\begin{aligned}&(|n+1,m\rangle + |m+1,n\rangle)(\langle n+1,m| + \langle m+1,n|),\\ &(|n+1,m\rangle - |m+1,n\rangle)(\langle n+1,m| - \langle m+1,n|),\end{aligned} \tag{P2.47}$$

with eigenvalues $(\frac{c_n c_m}{2}, -\frac{c_n c_m}{2})$, respectively. Therefore the negativity is given by

$$\mathcal{N} = \frac{1}{2}|\sum_{n\neq m} c_n(r,\Phi)\,c_m(r,\Phi)|, \tag{P2.48}$$

and the logarithmic negativity (Equation (P2.34)) is

$$E = \log_2\left(1 + |\sum_{n\neq m} c_n(r,\Phi)\,c_m(r,\Phi)|\right). \tag{P2.49}$$

By taking into account that $\sum_n c_n^2(r,\Phi) = 1$, we finally obtain

$$E = 2\,\log_2\left(\sum_n |c_n(r,\Phi)|\right). \tag{P2.50}$$

A APPENDIX

A.1 Generation of quantum vortex squeezed states

In this section we are going to analyse how to generate vortex states by means of a single-mode squeezed state, as expressed in equation (2.3.113). As explained this state can be generated through either optical parametric oscillator, or using four-wave mixing.

A.1.1 Generating SAM squeezed vortex states

A.1.1.1 Single-photon squeezed state vortex

Let us suppose that we generate a single-photon squeezed state, obtained by absorption of one photon from the squeezed vacuum state (2.3.113) in just one polarization mode

$$|1_\xi\rangle = \hat{S}(\xi)\,|1\rangle = \frac{1}{\cosh r}\hat{a}^\dagger \hat{S}(\xi)\,|0\rangle = \frac{1}{(\cosh r)^{3/2}}\sum_{n=0}^{\infty}\left(-e^{i\phi}\tanh r\right)^n \frac{\sqrt{(2n+1)!}}{2^n n!}\,|2n+1\rangle. \tag{A.1}$$

This can be done by using a a low reflection BS and a photon detector. A detection of a single photon will generate our state (A.1)

Assuming that the single-photon squeezed state is horizontally polarized, in the OFS the state is given by, according to [Nieto, 1997],

$$\langle x_H, x_V|\,\hat{S}_H(\xi)\,|1_H 0_V\rangle = \sqrt{\frac{F_3}{2\pi^{1/2}F_1}}\frac{2x_H}{F_4}\exp\left(-\frac{F_2}{2}x_H^2\right)\frac{1}{\sqrt{\pi}}\exp\left(-\frac{1}{2}x_V^2\right), \tag{A.2}$$

where

$$F_1 = \cosh r + e^{i\phi}\sinh r, \tag{A.3}$$

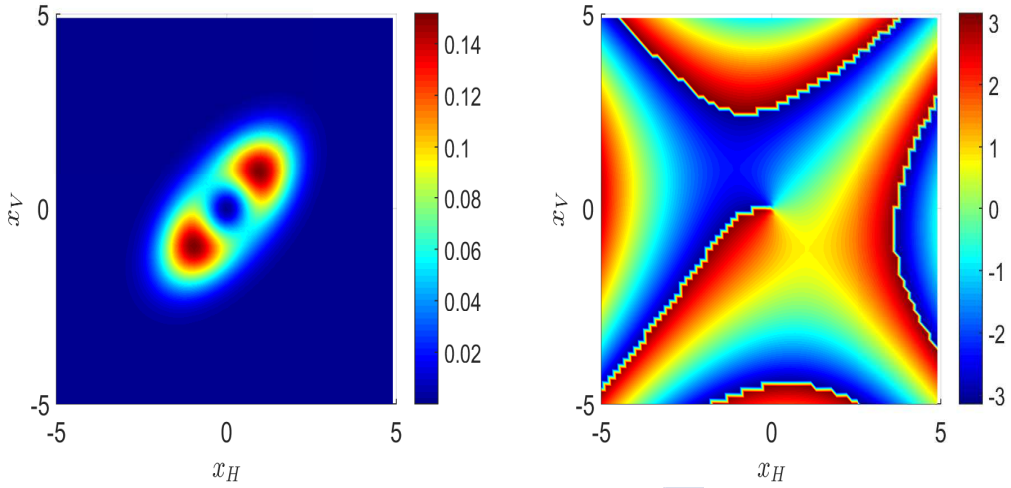
$$F_2 = \frac{1 - i\sin\phi\sinh r\left(\cosh r + e^{i\phi}\sinh r\right)}{\left(\cosh r + \cos\phi\sinh r\right)\left(\cosh r + e^{i\phi}\sinh r\right)} = \frac{\cosh r - e^{i\phi}\sinh r}{\cosh r + e^{i\phi}\sinh r}, \tag{A.4}$$

$$F_3 = \frac{\cosh r + e^{-i\phi}\sinh r}{\cosh r + e^{i\phi}\sinh r}, \tag{A.5}$$

$$F_4 = \sqrt{\left(\cosh r + e^{i\phi}\sinh r\right)\left(\cosh r + e^{-i\phi}\sinh r\right)}. \tag{A.6}$$

Now, if state (A.1) goes through a QWP oriented $\pi/4$ respect the polarization basis, we can obtain the final state by means of Feynman propagation [Hibbs and Feynman, 1965, Liñares et al., 2012]

$$\Psi_F(x,y) = \int\int K(x,y,x_0,y_0,z,0)\Psi(x_0,y_0)dx_0dy_0 \tag{A.7}$$



(a) Probability density (b) Phase density.

Figure A.1: Quantum vortex obtained from a single-photon squeezed state with $r = 0.5, \phi = 0$.

where we have applied the coordinates system to the axis of the QWP

$$\begin{pmatrix} x_H \\ x_V \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \tag{A.8}$$

and $K(x, y, x_0, y_0, z, 0)$ is Feynman's propagation constant

$$K(x, y, x_0, y_0, z, 0) = \frac{i}{2\pi} \frac{1}{\sqrt{\sin(\beta_x z)\sin(\beta_y z)}} \exp\left\{\frac{-i}{2}\left[\frac{x^2 + x_0^2}{\tan(\beta_x z)} - \frac{2x_0 x}{\sin(\beta_x z)}\right]\right\} \exp\left\{\frac{-i}{2}\left[\frac{y^2 + y_0^2}{\tan(\beta_y z)} - \frac{2y_0 y}{\sin(\beta_y z)}\right]\right\} \tag{A.9}$$

After the QWP, we obtain the state

$$\Psi_F(x_H, x_V) = \frac{i}{\sqrt{\pi \cosh^3 r}} (x_H - i x_V) \exp\left\{-\frac{1}{2}\left[(1 - i\eta) x_H^2 + (1 + i\eta) x_V^2 - 2\eta x_H x_V\right]\right\} \tag{A.10}$$

where $\eta = e^{i\phi} \tanh r$. We can observe this state in Figure A.1. In Figure A.1((a)) we see the state in the OFS where we can see how the squeezing affects the state by squeezing the density in one direction instead of being distributed around the singularity. The phase, shown in Figure A.1((b)), variates 2π around the singularity when we are close to it, but the squeezing also adds phase changes when we move far from it.

We can calculate the orbital angular momentum (OAM) of this squeezed state to study the effect of the QWP in the single-photon squeezed state. The OAM in the OFS is given by:

$$L_z = -i\hbar \left(x_H \partial_{x_V} - x_V \partial_{x_H} \right). \tag{A.11}$$

So the average value of the OAM of state (A.10) is given by

$$\langle L_z \rangle = \int\int \Psi^* L_z \Psi \, dx_H \, dx_V = -\hbar \left(1 + 3 \sinh^2 r \right). \tag{A.12}$$

We can see that there's a increasing of OAM as squeezing r of the original state does it.

A.1.1.2 Multi-photon squeezed state vortex

We can generalize our previous study for a number n of photons. So, we can consider a state on n photons polarized in one mode and squeezed as follows

$$\hat{S}_H \left| n_H \, 0_V \right\rangle = \sqrt{\frac{F_3^n}{2^n n! \, \pi F_1 F_\sigma}} H_n \left(\frac{x_{Ho}}{F_4} \right) \exp\left\{ -\frac{F_2}{2} x_{Ho}^2 \right\} \exp\left\{ -\frac{1}{2} x_{Vo}^2 \right\}. \tag{A.13}$$

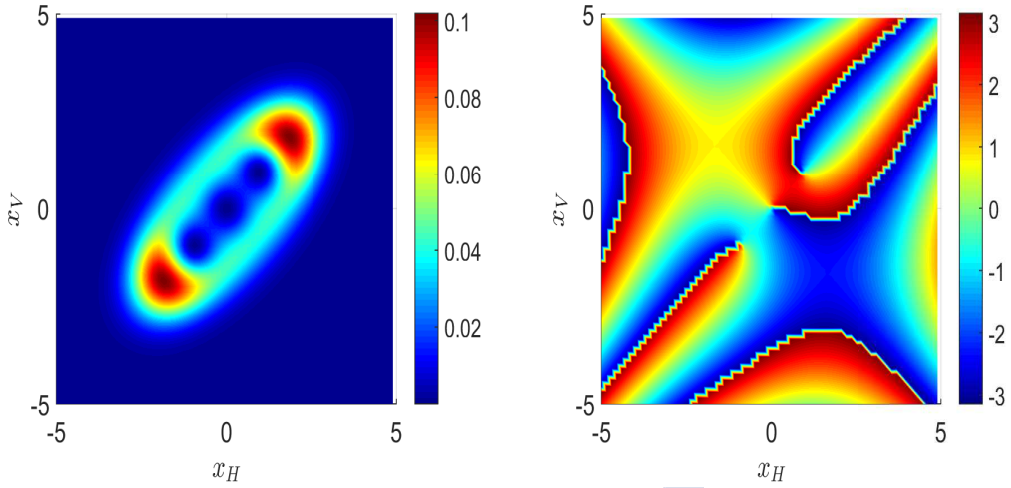
If we change the basis for the axis of the QWP (A.8), we have

$$\Psi(x_0, y_0) = \sqrt{\frac{F_3^n}{2^n n! \, \pi F_1}} H_n \left(\frac{x_0 - y_0}{\sqrt{2} F_4} \right) \exp\left\{ -\frac{1}{4} \left[(F_2 + \sigma) \left(x_0^2 + y_0^2 \right) + 2 \left(\sigma - F_2 \right) x_0 y_0 \right] \right\} \tag{A.14}$$

So, applying equation (A.7) to this state and going back to the original basis we have

$$\Psi_F(x_H, x_V) = \sqrt{\frac{(\tanh r \, e^{-i\phi})^n}{2^n n! \, \pi \cosh r}} e^{i\frac{\pi}{4}} H_n \left(\sqrt{\frac{e^{i\phi}}{\sinh 2r}} e^{i\frac{\pi}{4}} \left(x_H - i x_V \right) \right) \exp\left\{ -\frac{1}{2} \left[(1 - i\eta) x_H^2 + (1 + i\eta) x_V^2 - 2\eta x_H x_V \right] \right\} \tag{A.15}$$

The most interesting aspect from this state (A.15) is that it's a polynomial expression of $(x_H - i x_V)$. This means that when a polarized multi-photon squeezed state crosses a QWP we obtain a superposition of n vortex states. We can better see this in Figure A.2, where we represent state (A.15) in the OFS for the case $n = 3$. In Figure A.2(a) we can see how the state is squeezed along the main axis of the QWP and presents three minimums in the same direction. In Figure A.2(b) we can see how those three points correspond to singularities around which the phase changes 2π.



(a) Probability density. (b) Phase density.

Figure A.2: Quantum vortex obtained from a multi-photon squeezed state with $r = 0.5, \phi = 0$.

A.1.2 Generating quantum vortex squeezed states with OAM

Our previous studies about squeezed vortex states are also valid in spatial modes like HG and LG modes. In this case, the angular momentum of the vortex acquires information of the OAM of the states. When working with theses spatial modes cylindrical lens converters (CLCs) can be used the same way that HWPs and QWPs work with polarization modes.

Let us suppose that we have n photons in mode HG_{10}. If we compress these photons we would have state $\Psi(x_{10}, x_{01})$ given by (A.13). So, if we employ a CLC, in the way of a QWP for polarization, the final state will be given, as well, by expression (A.15). The only difference consists of the physical momentum carried in this case. State (A.15) is a vortex of polarization modes, so, as we see in (A.12) it carries spin momentum. In this case, as we have a vortex made of HG modes, this is a LG mode, our state carries orbital angular momentum. Specifically, we can see that $x_{10} - ix_{01}$ corresponds, according to LG mode decomposition [Agarwal and Banerji, 2006] to mode $LG_{l=-1,\,p=0}$.

The OAM operator is given by (2.3.110). In this case, the operator is simplified in function of HG operators as

$$\hat{L} = -i\hbar \left(\hat{a}_{10}^{\dagger} \hat{a}_{01} - \hat{a}_{01}^{\dagger} \hat{a}_{10} \right). \tag{A.16}$$

Same expression as (A.11), so the OAM of our state is going to be given by (A.12) and we can see that it grows with the squeezing.

Let's consider now that we have n photons in mode HG_{20} and we squeeze them. In

this case, we have state

$$\hat{S}_{20}\left|n_{20}\,0_{11}\,0_{02}\right\rangle = \sqrt{\frac{F_3^n}{2^n n!\,\pi^{3/2}F_1}}H_n\left(\frac{x_{10}}{F_4}\right)\exp\left\{-\frac{F_2}{2}x_{10}^2\right\}\exp\left\{-\frac{1}{2}x_{11}^2\right\}\exp\left\{-\frac{1}{2}x_{02}^2\right\}. \tag{A.17}$$

If we make this state cross a CLC, according to HG decomposition in diagonal HG modes [Beijersbergen et al., 1993, Agarwal and Banerji, 2006] we have to apply the change of basis

$$\begin{pmatrix} x_{20} \\ x_{11} \\ x_{02} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & \sqrt{2} & 1 \end{pmatrix}\begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \tag{A.18}$$

Then, we apply Feynman's propagation (A.7) knowing that the CLC introduces phase shifts $\beta_z - \beta_x = \pi$ and $\beta_z - \beta_y = \pi/2$. Returning to the original basis, we will obtain the following state

$$\Psi = \frac{1}{\sqrt{2^n n!\,\pi^{3/2}}}\sqrt{\frac{e^{-in\phi}\sinh^n r}{\cosh^{n+1} r}}H_n\left(\sqrt{\frac{e^{i\phi}}{\sinh r\cosh r}}\left(\frac{x_{20}}{2} - \frac{ix_{11}}{\sqrt{2}} - \frac{x_{02}}{2}\right)\right)\cdot$$
$$\exp\left\{-\frac{1}{2}\left[\left(1+\frac{\eta}{2}\right)(x_{20}^2 + x_{02}^2) + (1-\eta)x_{11}^2 + i\sqrt{2}\eta x_{11}(x_{02} - x_{20}) - \eta x_{20}x_{02}\right]\right\}. \tag{A.19}$$

We have again an Hermite polynomial, that is function of $\frac{x_{20}}{2} - \frac{ix_{11}}{\sqrt{2}} - \frac{x_{02}}{2}$, ignoring the constant. According to LG mode decomposition, this corresponds to mode $LG_{-2,0}$. So, we have again a superposition of vortices. However, these vortices are a bit different than before and we can consider them 3 dimensional vortices. Let's study the simple case.

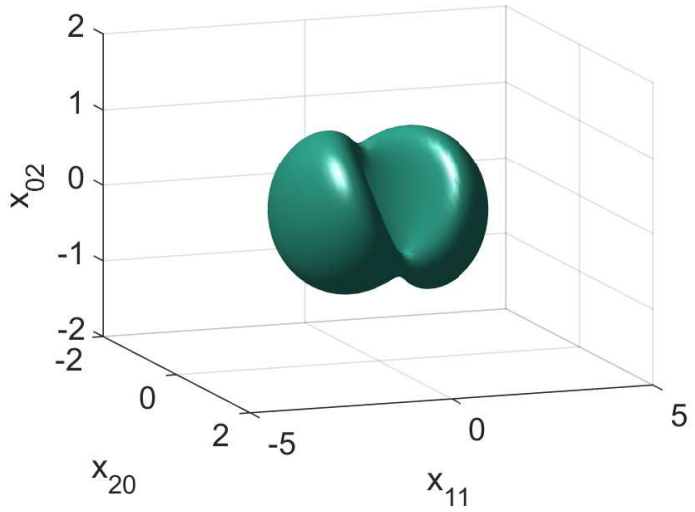
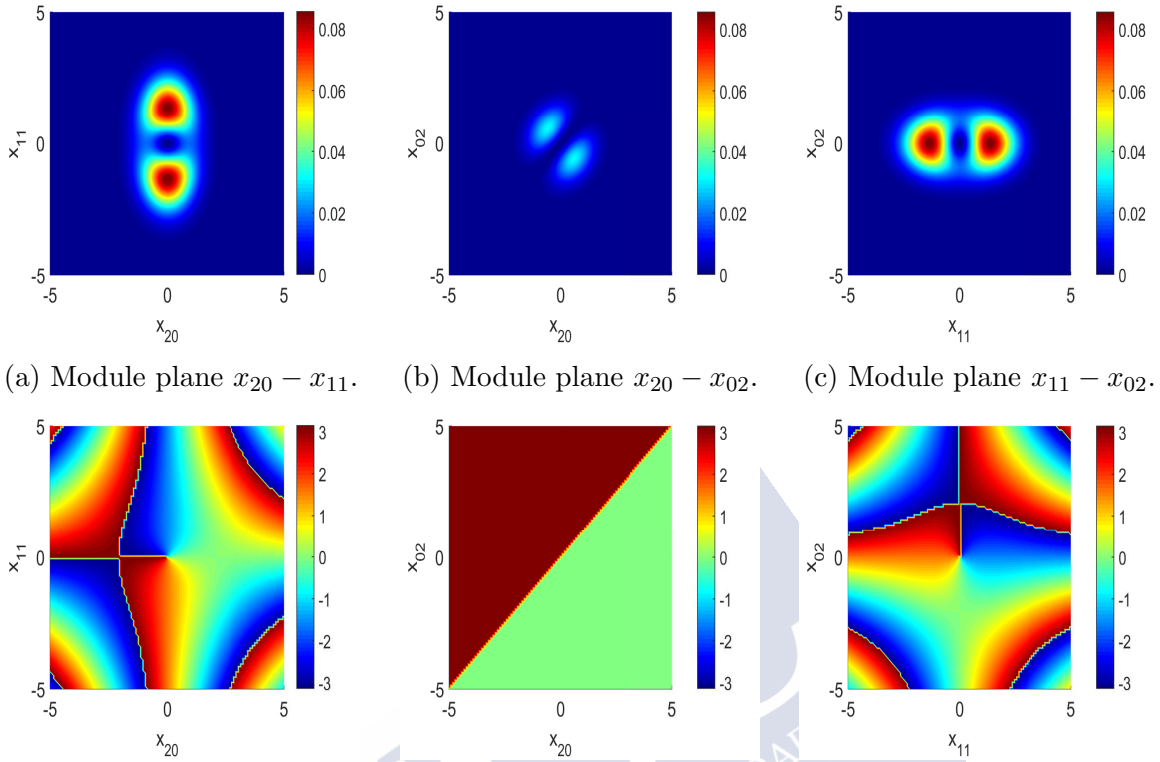


Figure A.3: Squeezed vortex state with three HG modes, with $r = 0.5$, $\phi = 0$.



(a) Module plane $x_{20} - x_{11}$. (b) Module plane $x_{20} - x_{02}$. (c) Module plane $x_{11} - x_{02}$.

(d) Phase plane $x_{20} - x_{11}$. (e) Phase plane $x_{20} - x_{02}$. (f) Phase plane $x_{11} - x_{02}$.

Figure A.4: Squeezed vortex state with three HG modes, with $r = 0.5$, $\phi = 0$. Slides

,

For the case $n = 1$, we have the following vortex state

$$\Psi = \frac{2}{\sqrt{2\pi^{3/2}\cosh^3 r}}\left(\frac{x_{20}}{2} - \frac{ix_{11}}{\sqrt{2}} - \frac{x_{02}}{2}\right)\cdot$$
$$\exp\left\{-\frac{1}{2}\left[\left(1+\frac{\eta}{2}\right)(x_{20}^2 + x_{02}^2) + (1-\eta)x_{11}^2 + i\sqrt{2}\eta x_{11}(x_{02} - x_{20}) - \eta x_{20}x_{02}\right]\right\}. \quad \text{(A.20)}$$

In Figure A.3 we represent an isosurface of the module in 3 dimensions to see its shape. We also represent in Figure A.4 the slices of the module for the 3 main planes, as well as their phases. Observing both figures, we can see how we have a singularity on axis given by $x_{02} = x_{20}$, $x_{11} = 0$ (Figs. A.4(b), A.4(e)), around which the phase rotates 2π (Figs. A.4(d), A.4(d)). We can also observe the effect of the squeezing in the vortex state in its module compression around the singularity (Figs. A.3, A.4(a), A.4(c)).

The OAM operator is now given by, in HG basis,

$$\begin{aligned}\hat{L} = &- i\sqrt{2}\hbar\left[\left(\hat{a}_{20}^\dagger - \hat{a}_{02}^\dagger\right)\hat{a}_{11} - \hat{a}_{11}^\dagger\left(\hat{a}_{20} - \hat{a}_{02}\right)\right] \\ &- i\sqrt{2}\hbar\left[\left(x_{20} - x_{02}\right)\partial_{x_{11}} - x_{11}\left(\partial_{x_{20}} - \partial_{x_{02}}\right)\right] \quad \text{(A.21)}\end{aligned}$$

So the average value of the OAM of state (A.20) is given by

$$\langle L \rangle = \int\int\int \Psi^* L \Psi \, dx_{20} \, dx_{11} \, dx_{02} = -\frac{\hbar}{4} \left(-1 + 3\cosh\left(2r\right)\right). \tag{A.22}$$

Just like with HG_{10} and HG_{01} modes, the momentum rises with the squeezing.

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

3

Autocompensating Quantum Cryptography in Few-Mode Fibers

High dimensional quantum key distribution (HD-QKD) has been shown to provide a higher level of security security against an eavesdropper attack than the regular and most used two dimensional QKD [Cerf et al., 2002]. However, it is still subjected to the influence of noise disturbance. The main objective of this chapter is to develop an autocompensating HD-QKD system. More specifically, we are going to design a system to implement the BB84 protocol in high dimension employing the different modes of a few-mode fiber (FMF) that corrects all the possible phase disturbances to which the system is naturally subjected to. FMFs are used because of the growing interest and applicability in communications. Moreover, we are going to study possible attacks that can affect our proposed system and analyse its security. A particular case of our system studied in our work [Balado Souto et al., 2019] also included in the chapter.

The chapter is structured as follows. First, section 3.1 is dedicated to explain the original BB84 protocol (subsection 3.1.1), as well as its possible perturbations and the first solutions proposed (subsection 3.1.2). Next, in section 3.2, we present the theoretical structure of an HD-QKD autocompensating system employing spatial modes of an elliptical core FMF (EC-FMF) by means of multi-loop propagation. We explain its main component (subsection 3.2.1), the autocompensating process (subsection 3.2.2) and the transmission rate limitations (subsection 3.2.3). Additionally, we propose particular systems for two and four dimensions (subsection 3.2.4 and 3.2.5), with the latter being detailed in our published work [Balado Souto et al., 2019] annexed as section P3 at the end of the chapter. Finally, a security study is done in section 3.3. In this section, we analyse the main attacks the main attacks that our system is vulnerable to, like the general photon-number splitting attack (subsection 3.3.3) and the quantum cloning attack (subsection 3.3.2), as well as the phase-remapping attack (subsection 3.3.3), which is the more specific one to our system.

3.1 Original BB84 protocol, perturbations and solutions

The purpose of any QKD protocol is to share a common secret key between a sender, usually referred to as Alice, and a receiver, known as Bob, in a secure way that guarantees that no eavesdropper, called Eve, is able to obtain it. Employing such key Alice can encrypt a message and send it to Bob, who can use his copy of the key to decrypt the message. As explained, even if some eavesdropper obtains the message, the security of the encryption is guaranteed whenever the size of the message and the secret key are the same. So, as long as Eve can not obtain the secret key, the communication between Alice and Bob will be secure.

Any communication working with QKD requires, then, of two different communication channels: a quantum channel, to perform QKD, and a classical one, to assist QKD and share messages. The quantum channel consists of a transmission channel where quantum carriers are transmitted from Alice to Bob. For practical reasons, these carriers are usually photons or certain states of light, while the channel itself may be an optical fiber or the open air. Alice encodes random bits in a certain quantum property of these carriers. These bits will be used to generate the secret key. The randomness generation of these bits prevents any possibility of Eve predicting the key.

Eve can eavesdrop the transmission through the quantum channel between Alice

[1]Figure designed using resources from Flaticon.com [Eucalypt,].

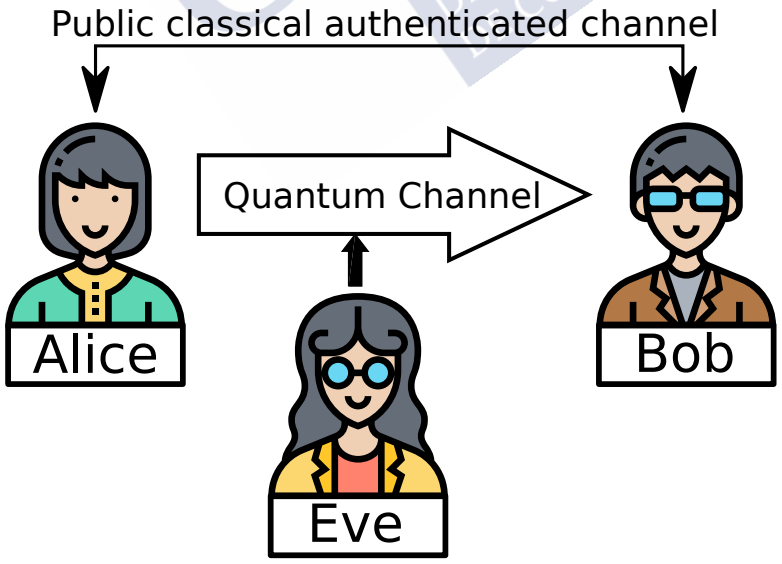


Figure 3.1.1: Quantum key distribution comprises a quantum channel and a public classical authenticated channel. Alice sends quantum states to Bob through a quantum channel, while Eve is suspected of eavesdropping on the line.[1]

and Bob and obtain potential secret key bits. However, her eavesdropping will cause transmission errors detectable by Alice and Bob. In this way, after the transmission, Alice and Bob can make use of a classical channel to share and compare a fraction of the exchanged key. Comparing their bits, they can detect transmission errors and they can know if the communication is compromised. If no eavesdropper is found, Alice and Bob can generate a secret key with the fraction of bits that they did not share. What is more, the secret-key distillation techniques allow Alice and Bob to correct such errors and generate a secret key anyway with the bits that are unknown to Eve. This means that any eavesdrop into the classic channel is pointless, as it does not give Eve any information about the key. Thus, the classical channel does not require to be confidential and can be a public channel, but it must be authenticated, that is, Alice must known that she really is talking to Bob and not Eve.

Apart from the eavesdropper influence, errors can appear due to perturbations and fluctuations on the quantum channel. This generates a problem that must be corrected cause it compromises the security of the system.

3.1.1 BB84 protocol

Bennett and Brassard proposed the first QKD protocol in 1984, thus, it is known as the BB84 protocol [Bennett and Brassard, 1984]. BB84 was the base for many of the following QKD protocols, so let us explain it in detail [Bennett et al., 1992b].

As previously said, the unit of information in the quantum information theory is the qubit. The qubit can be defined as

$$|q\rangle = c_0 |0\rangle + c_1 |1\rangle , \tag{3.1.1}$$

where $|c_0|^2+|c_0|^2= 1$, $c_i \in \mathbb{C}$, and $|0\rangle$ and $|1\rangle$ are the two orthogonal reference qubits that build the orthonormal basis of the qubit. In BB84, Alice must randomly encode classical bits $\{0, 1\}T$ in a set of four different qubits. More specifically, each bit can be randomly encoded in two different linearly dependent MUBs, with each value of the bit corresponding to each of the reference qubits of said basis. For dimension 2, there are actually 3 different possible MUBs. In this way, Alice can encode the bit 0 in the qubits $|0\rangle$, $|+\rangle$ or $|R\rangle$, and bit 1 in qubits $|1\rangle$, $|-\rangle$ or $|L\rangle$, as shown in Table 3.1.

Table 3.1: BB84 qubits.

Bit	Qubit		
	Base $\bigoplus$	Base $\bigotimes$	Base $\bigcirc$
0	$\|0\rangle$	$\|+\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|R\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$
1	$\|1\rangle$	$\|-\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|L\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$

Physically, these qubits can be implemented in different ways. To begin with, they can correspond to the polarization state of the photons used as carriers (*polarization encoding*), as originally proposed. In such manner, Alice can encode each bit in a photon by means of a polariser, generating four different polarization states, and send it to Bob. In particular, these states would be $|H\rangle = |0\rangle$, $|V\rangle = |1\rangle$, $|H'\rangle = |+\rangle$ and $|V'\rangle = |-\rangle$. Here, H and V refer to horizontal and vertical polarization, that creates the linear basis $\bigoplus$; while H' and V' denote the diagonal polarizations of a diagonal basis $\bigotimes$ rotated 45° respect to the linear one. Another possibility is *phase encoding*, which consists of using qubits $|0\rangle$ and $|1\rangle$ as a base state to generate the four coded qubits by means of a phase shift θ between them, as follows

$$|q\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}\,|1\rangle\right). \tag{3.1.2}$$

In this case, qubits $|0\rangle$ and $|1\rangle$ can correspond to two single-photon states in different temporal or spatial modes. By applying phases $\theta = \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ between both modes by means of a phase modulator, the four qubits of basis $\bigotimes$ and $\bigcirc$ are implemented, where the later corresponds to the circular base. Anyway, the protocol works the same with independence of the coding physical property and the different basis used.

Once the encoded photons arrive to Bob, he needs to decode them by measuring. Nonetheless, in quantum mechanics is impossible to completely measure a qubit, that is, coefficients c_i in equation (3.1.1) can not be accurately determined. Instead, measuring in quantum mechanics consists of making a projection on a pair of orthogonal qubits, resulting in the obtention of one of them. Accordingly, Bob needs to measure the qubits sent by Alice in one of the two basis used (for example, $\bigoplus$ or $\bigotimes$). If he chooses the same basis of the qubit, he is always going to distinguish the right bit. However, when the chosen basis is different, Bob would obtain bit i with a probability of $|c_i|^2$. For example, if Bob measures in base $\bigoplus$ and Alice is sending qubits $|0\rangle$ or $|1\rangle$, he obtains bits 0 and 1 respectively, but if Alice sends qubits $|+\rangle$ or $|-\rangle$, Bob can get any bit (0 or 1) with a probability of 50% for both states. All the possible cases are shown in Table 3.2.

In practice, if polarization encoding is used, Bob can perform this measure by means of a polarization beam splitter (PBS) and two detectors situated at each output of the splitter. The PBS splits two orthogonal polarizations determined by its main axis. If the polarized photon is aligned with the axis of the PBS, it goes out by one of the outputs and detected by the corresponding detector. If its polarization is not aligned, the output quantum state is a superposition of the photon in both directions and can be detected by any detector. Bob can change the base of measurement by rotating the PBS or introducing a rotator. For phase encoding, it is precise to use some interferometric system instead, that separates both states from a same basis in different outputs.

In the BB84 protocol, Bob has to randomly choose the measurement basis. Once the transmission is over, Alice tells Bob the basis she used to encode her bits and Bob discards all the bits obtained with the wrong basis. Theoretically, all the bits measured with the right basis must be the same as those sent by Alice, excluding possible errors of

Table 3.2: QKD using BB84 without an eavesdropper. The first two rows show all the possible states sent by Alice. The bottom rows show all the possible measurements of Bob according with his chosen measurement basis. Only the bits corresponding to the case where Bob chose the right basis are taken into account to form the key.

Alice	Original bit	0	0	0	0	1	1	1	1
	Coded state	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$
Bob	Measurement basis	$\bigoplus$	$\bigotimes$	$\bigoplus$	$\bigotimes$	$\bigoplus$	$\bigotimes$	$\bigoplus$	$\bigotimes$
	Measured state	$\|0\rangle$	$\|+\rangle, \|-\rangle$	$\|0\rangle, \|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle, \|-\rangle$	$\|0\rangle, \|1\rangle$	$\|-\rangle$
	Measured bit	0	0‖1	0‖1	0	1	0‖1	0‖1	1
	Key bits	0	-	-	0	1	-	-	1

due to noise in the transmission and in the devices employed, which mus be taken into account. Hence, Alice and Bob only make use of these bits to create the secret key, as shown in Table 3.2.

Now, what happens if Eve spies on the quantum channel? Naturally, Eve can intercept photons send by Alice and measure them. However, just like Bob, she has to measure in a random basis, as she is unaware of the basis of each qubit. The wave function collapse of quantum mechanics establishes that, whenever a measurement is done in a quantum state, this state is reduced to the corresponding eigenstate that gives that value. Consequently, when Alice intercepts and measures the photons, the original qubit is destroyed, and Eve only has knowledge of the state she has measured. That is, if Alice is sending qubit $|q\rangle$ and Eve measures in base $\bigoplus$, the qubit is going to become $|q\rangle \rightarrow |0\rangle$ or $|q\rangle \rightarrow |1\rangle$, depending on the measurement result. Moreover, the no-cloning theorem [Wootters and Zurek, 1982, Dieks, 1982] forbids the possibility of Eve cloning the original qubit to measure a copy and not disturb it.

Therefore, every time Eve intercepts and measures Alice's qubits, she has to send Bob new qubits that corresponds with her measurements. The probability of Eve choosing the right basis of measurement is 1/2. Hence, half of the time, Eve is sending the right qubit to Bob, while in the other half, she sends any of the qubits of the wrong basis. As said before, to generate the key Alice and Bob only consider the bits corresponding to the times they used the same basis. If Eve sent to Bob a qubit in the wrong basis, Bob would get an incorrect bit half of the times. In consequence, Eve' eavesdropping results in the introduction of errors between Alice's an Bob's bits with a probability of 1/4. Different situations reflecting this are shown in Table 3.3.

Let us suppose that Alice and Bob have exchanged n key bits. As previously explained, Alice and Bob make use of the public classical authenticated channel to share a fraction $n - k$ of their key bits. Then, they compare them to calculate the bit error rate in their communication channel $e_r = e/(n - k)$, where e is the number of errors in the

Table 3.3: QKD using BB84 with eavesdropper. Only the cases where Alice and Bob chooses the same basis ($\oplus$) is considered (the case for $\otimes$ is identical). Bob's wrong bits due to eavesdropping are shown in red. In case that all bits were checked, the error rate would be 0.4.

Alice	Key bit	0	0	0	0	0	1	1	1	1	1
	Coded state	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$
Eve	Measurement basis	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\otimes$
	Eavesdropped state	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$
	Eavesdropped bit	0	0	0	1	1	1	0	0	1	1
Bob	Measurement basis	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$
	Result	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
	Measured state	0	0	1	0	1	1	0	1	0	1

shared key. If they get an error rate of about 25% or more, that means the presence of an eavesdropper and so, the security of the communication is compromised. Alice and Bob can decide to abort the protocol preventing the creation of a key that may not be secret. If the error rate is far lower, the channel is secure and Alice and Bob generate a secret key employing the remaining k bits.

Even in the presence of an eavesdropper, it still may be possible to generate a secret key. Eve's intercepted key also has an error rate of 25%. Furthermore, she may just have eavesdropped a small fraction of the exchanged key. Therefore, Alice and Bob can make an estimation of the amount of information Eve knows and then, apply secret-key distillation techniques to correct the errors in their key. These techniques need to be applied, anyway, to correct errors due to noise or losses in the quantum channel, imperfect generation of quantum states or imperfect detectors.

To sum up, BB84 protocol is based on the following points

1. Alice encodes key bits into two pairs of orthogonal quantum states in a random way and sends them to Bob through the quantum channel.

2. Bob measures Alice's states choosing randomly the measurement basis.

3. Alice tells Bob the basis used on each of her bits through the classical channel and Bob discards all the bits where he used the wrong basis.

4. Alice and Bob share a fraction of the valid bits and calculate the bit error rate.

5. If the transmission is secure, Alice and Bob generate the secret key with the remaining bits.

The original BB84 essentially makes use of quantum states belonging to a two dimensional Hilbert space. Later, it was demonstrated that using high dimensional quantum states provides greater robustness to noise and a higher level of security in presence of an eavesdropper [Cerf et al., 2002]. To implement BB84 in higher dimensions, it is only required to generate different quantum states that correspond to, at least, two MUBs of said dimension. For example, for dimension N, at least $2N$ states belonging to two different MUBs are necessary, although N or even $N+1$ basis can be used. Phase encoding results very useful to take the BB84 to higher dimensions.

Growing the dimension means that more information is transmitted. In particular, information theory establish that a total of $\log_2(N)$ bits are transmitted by qudit for dimension N. For example, for dimension $N = 4$, the four qudits from a same basis correspond to states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. The security of the protocol is enhanced by the use of more states for each basis. If Eve uses an intercept and resend attack, as the one explained previously, and do not choose the right basis, the probability of her obtaining the sent qudit is decreased. Employing more basis also increases the security of the system, as it makes difficult for Eve to choose the right basis. But, it also has the drawback of lowering the transmission key rate, as the amount of time that Alice and Bob use the same basis is also reduced and it is the only case where the transmitted bits are valid. To sum up, implementing the BB84 in high dimension has several advantages. However, it is also subjected to the same possible noise transmission problems of the regular protocol. For this reason, to implement an autocompensating high dimension BB84 system constitutes one of the main objectives of this chapter.

3.1.2 Quantum States Perturbation in Optical Fibers

In quantum cryptography it is essential to avoid disturbance generated by the possible noise sources. Noise can arise in a lot of different ways. For example, fluctuations in the light source or other components of a state generator system can be sources of noise, as well as detector devices also have noise problems(dark counts...). This kind of problems must be minimized and taken into account in the coding scheme. During transmission, fluctuations of the medium through which the photons travel are a source of noise. QKD can be implemented either through free space or through optical fibers. In the former, noise is caused by atmospheric density fluctuations. These fluctuations change randomly in time and space, however, they are locally highly isotropic; so the phase fluctuations suffered by the different light states travelling through the air are random, but they affect isotropically the different modes of the state. For example, if we use phase polarization encoding, this is, code information in a phase difference between two orthogonal polarization modes, the contrast between the states will barely be affected and the fluctuations only will reduce the key generation rate.

Nonetheless, free space optical systems are not the main approach to employ QKD. Instead, optical fibers are used, as they allow to transmit light over long distances without general perturbations and are easily connected to other integrated devices. However, light

transmission through optical fibers experiment different problems that can perturb QKD. Most optical fibers experiment birefringence effects caused by variations in the structure of the fiber and due to mechanical tensions originated by bends, twists, etc. Other components in the optical system can also introduce birefringence.

3.1.2.1 Polarization perturbations and Plug and play systems

Birefringence will affect and randomly change the polarization state of the transmitted light. So, if polarization modes are used as a basis for coding information for QKD, these modes are going to experiment rotations and phase shifts between them and the quantum information transmitted by the light states is going to be perturbed.

In consequence, it becomes necessary to employ some sort of compensating system in order to correct fluctuations in polarization to use it as a basis for coding quantum information. For example, some kind of active feedback control that makes a constant measurement of the perturbations and compensates them accordingly can be successfully used [Ribordy et al., 2000]. However, another possible approach is to build an auto-compensation optical system for QKD, this is, a system that inherently and passively compensates the fluctuations originated in it. This kind of systems are also referred as *plug and play* systems. The first autocompensation systems proposed were independently developed by groups at the university of Geneva [Muller et al., 1997] and at IBM [Bethune and Risk, 2000]. Both approaches are based on Martinelli's idea to compensate birefringence effects on the polarization state of retracting beam [Martinelli, 1989]. Martinelli observed that, by means of a Faraday mirror, birefringence effects on a beam which retraces its path are eliminated and the light returns in the polarization state orthogonal to that in which it was originated. The cause of this is that a Faraday mirror does an exchange of orthogonal polarization states and, in consequence, even if both polarization modes suffer a difference between their accumulated phases over propagation, such difference is going to be corrected in the back trip. Based on this, Muller and Bethune proposed using a round-trip propagation through a Faraday reflection in order to correct

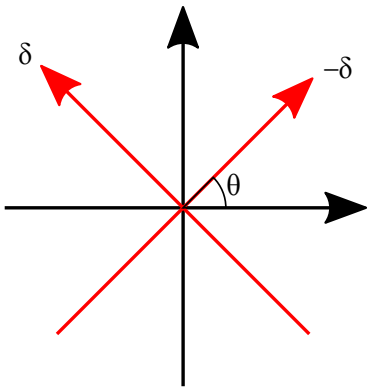


Figure 3.1.2: Birefringence diagram.

the birefringence effects along the optical fiber. If the quantum information is encoded in a phase difference between two orthogonal polarization modes, QKD will be unperturbed by birefringence in the fiber [Bethune and Risk, 2002, Bethune et al., 2002]. The first to implement a plug and play system experimentally were Zbinden et al. in 1997 [Zbinden et al., 1997]. Fives years later, Stucki et al. were able to implement another reaching distances of over 67 km [Stucki et al., 2002].

Let's explain this mathematically. Birefringence can be understood as a polarization rotation to the main birefringence axis and a phase shift between them, as shown in Figure 3.1.2. Mathematically, the transformation between operators will be given by

$$\begin{pmatrix} \hat{a}_H \\ \hat{a}_V \end{pmatrix} = R^{-1}(\theta) \cdot \Delta(\delta) \cdot R(\theta) \begin{pmatrix} \hat{a}_{H0} \\ \hat{a}_{V0} \end{pmatrix}$$

$$\begin{pmatrix} \hat{a}_H \\ \hat{a}_V \end{pmatrix} = \begin{pmatrix} e^{\frac{i\delta}{2}}\cos^2(\theta) + e^{-\frac{i\delta}{2}}\sin^2(\theta) & \left(e^{-\frac{i\delta}{2}} - e^{\frac{i\delta}{2}}\right)\cos(\theta)\sin(\theta) \\ \left(e^{-\frac{i\delta}{2}} - e^{\frac{i\delta}{2}}\right)\cos(\theta)\sin(\theta) & e^{-\frac{i\delta}{2}}\cos^2(\theta) + e^{\frac{i\delta}{2}}\sin^2(\theta) \end{pmatrix} \cdot \begin{pmatrix} \hat{a}_{H0} \\ \hat{a}_{V0} \end{pmatrix}, \tag{3.1.3}$$

where $R(\theta)$ is the rotation matrix and $\Delta(\delta)$ represents the difference in phase propagation through the different birefringence axis:

$$R(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}, \tag{3.1.4}$$

$$\Delta = \begin{pmatrix} e^{\frac{i\delta}{2}} & 0 \\ 0 & e^{-\frac{i\delta}{2}} \end{pmatrix}. \tag{3.1.5}$$

Expression (3.1.3) can represent the polarization fluctuations suffered during forward propagation. If we want to describe mathematically the backward propagation, then we have to follow the convention that it has to be described by reversing $z-$ and $x-$axes [Brinkmeyer, 1981, Yariv, 1987]. This axis reversal can be made by changing the rotation angle θ to $-\theta$ in the rotation matrix (3.1.4). As birefringence in the optical fiber is reciprocal, matrix (3.1.5) will not change. Taken all these into account, the forward and backward propagation matrices can be described as

$$T_F = \begin{pmatrix} e^{\frac{i\delta}{2}}\cos^2(\theta) + e^{-\frac{i\delta}{2}}\sin^2(\theta) & \left(e^{-\frac{i\delta}{2}} - e^{\frac{i\delta}{2}}\right)\cos(\theta)\sin(\theta) \\ \left(e^{-\frac{i\delta}{2}} - e^{\frac{i\delta}{2}}\right)\cos(\theta)\sin(\theta) & e^{-\frac{i\delta}{2}}\cos^2(\theta) + e^{\frac{i\delta}{2}}\sin^2(\theta) \end{pmatrix}, \tag{3.1.6}$$

$$T_B = \begin{pmatrix} e^{\frac{i\delta}{2}}\cos^2(\theta) + e^{-\frac{i\delta}{2}}\sin^2(\theta) & -\left(e^{-\frac{i\delta}{2}} - e^{\frac{i\delta}{2}}\right)\cos(\theta)\sin(\theta) \\ -\left(e^{-\frac{i\delta}{2}} - e^{\frac{i\delta}{2}}\right)\cos(\theta)\sin(\theta) & e^{-\frac{i\delta}{2}}\cos^2(\theta) + e^{\frac{i\delta}{2}}\sin^2(\theta) \end{pmatrix}. \tag{3.1.7}$$

Now a Faraday mirror (FM) is a combination of a Faraday rotator, configured to to implement a 45° polarization rotation, and a regular mirror. A Faraday rotator can be expressed as a rotation matrix (3.1.4). However, Faraday rotators are not reciprocal elements, so reversing propagation will also change the sign of the rotation angle $45° \rightarrow -45°$. Therefore, the operator transformation matrix of the FM is given by

$$FM = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}. \tag{3.1.8}$$

Consequently, if we have a round trip system with forward (3.1.6) and backward (3.1.7) propagation caused by an FM (3.1.8), the full transformation matrix T_R is going to be given by

$$T_R = T_B \cdot FM \cdot T_F = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}. \tag{3.1.9}$$

As observed, the final expression of T_R is an anti-diagonal matrix with a global phase. This means that quantum operator are transformed as

$$\hat{a}_H = -\hat{a}_{V0}, \tag{3.1.10}$$

$$\hat{a}_V = -\hat{a}_{H0}. \tag{3.1.11}$$

The final polarization state of light obtained is orthonormal to the original state and the phase difference 2δ introduced between the main axis along propagation has been compensated at the end of the round trip. Thus, two orthogonally polarized light pulses introduced in such a round trip system will not experiment any differential phase shift or attenuation between them. In consequence, by coding the quantum information in a phase shift between two orthogonally polarized pulses, QKD can be implemented free of any perturbations happening during propagation.

3.1.2.2 Fiber modes perturbation

Birefringence is not the only problem that light can suffer while travelling through an optical fiber. In case a multimode fiber is employed in communication, problems can arise within the different propagation modes in the fiber. First and foremost, crosstalk between the different modes can perturb the state resulting in the loss of information and affecting the key transmission rate. Moreover, different modes can have different propagation constants generating modal lags between modes while travelling through the fiber. Modal phase shifts can also occur along propagation.

These drawbacks become even more problematic in case that we wanted to make use of the different modes of the fiber in a QKD protocol. Employing various fiber modes could become a good strategy to implement high dimensional quantum key distribution (HD-QKD). However, modal crosstalk can perturb the transmitted quantum information

and modal lags and phase shifts can destroy our state and prevent us to work properly with them. It becomes necessary to search for a way to deal with such problems.

When working with polarization in QKD, it is frequent the use of polarization maintaining fibers in order to minimize problems that can arise during transmission, like birefringence, as explaining before. So, a natural approach to the problem is to develop a QKD autocompensating system that makes use of fibers with low crosstalk between modes.

Elliptical-core few-mode fibers (EC-FMF) can be employed for this end. It has been proved that EC-FMFs have very low modal crosstalk between both normally degenerate spatial modes LP_{11x} and LP_{11y} and polarization modes [Milione et al., 2016b, Milione et al., 2016a]. Spatial modes of a EC-FMF are so stable that they do not couple even under fiber twisting or bending. Moreover, it has been shown that EC-FMFs present low losses during propagation [Liu et al., 2018]. This very low crosstalk makes EC-FMF useful to implement spatial division multiplexing, as it allows to avoid the MIMO technique [Ip et al., 2015, Milione et al., 2017, Parmigiani et al., 2017].

Consequently, EC-FMFs offer a really robust high-dimensional modal space, which can be used to excite high-dimensional optical quantum states to implement QKD protocols in higher dimensions. In summary, spatial division multiplexing with EC-FMFs hold a great potential to implement HD-QKD.

However, an obvious problem arises. While modal crosstalk is minimized in EC-FMF, modal lags are magnified. Trivially, the modes of EC-FMF have different propagation constants, as a consequence of birefringence arising from core asymmetry (ellipticity). Small accumulative changes due to local changes also generate modal lags between modes. As explained previously, relative phase shifts and lags between modes constitutes a major problem for HD-QKD using spatial modes, and no special design of an optical fiber is going to minimize this problem. It becomes necessary to implement some kind of compensating system in order to solve this drawback for being able to implement HD-QKD.

In the next section, we are going to develop an autocompensating system to implement QKD in high dimension generating qudits through phase encoding using the spatial modes of an EC-FMF. The autocompensating technique will be based on making light travel several times the path between Alice and Bob (rounds) and choosing suitable modal inversions, as inspired for the polarization autocompensation method explained before. Moreover, in the annexed [Balado Souto et al., 2019], we propose an specific autocompensation system for four dimensions, where we generate ququarts states by combining the fundamental spatial modes of an EC-FMF with polarization modes. For ququarts, two rounds and two appropriate modal inversions are needed, to allow each mode to acquire the deterministic and random phases of the other three modes, as will be shown. We will use optical systems based on modal converters and Mach-Zehnder interferometers, which are usual components in spatial multiplexing [Liñares et al., 2017a].

3.2 Quantum Cryptography Autocompensation by Multiloop Propagation

3.2.1 Effective Faraday Mirror

To implement an autocompensating system similar to the one explained in subsection 3.1.2.1 employing spatial HG modes, it is necessary to develop a system that works in a similar way to a Faraday mirror with polarization modes, that is, an "Effective Faraday Mirror" (EFM). A Faraday mirror has two main characteristics that need to be replicated. The first one is that it sends backwards the incident light, while the second one, is the fact that it exchanges two orthonormal polarization states. To achieve the second one, one possibility is using a CLC. We have shown in equation (2.2.91) that, for HG modes of order $N = n + m$ a π-converter whose main axis are rotated 45° respect the modes basis, the operator transformation matrix is given by

$$\begin{pmatrix} \hat{a}_{HG_{N,0}} \\ \vdots \\ \hat{a}_{HG_{N-i,i}} \\ \vdots \\ \hat{a}_{HG_{0,N}} \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 1 \\ & \iddots & \\ \vdots & 1 & \vdots \\ & \iddots & \\ 1 & \cdots & 0 \end{pmatrix} \cdot \begin{pmatrix} \hat{a_0}_{HG_{N,0}} \\ \vdots \\ \hat{a_0}_{HG_{N-i,i}} \\ \vdots \\ \hat{a_0}_{HG_{0,N}} \end{pmatrix}. \tag{3.2.12}$$

So, a π-converter of cylindrical lenses implements a modal exchange with orthonormal HG modes, just like the Faraday rotator does with polarization. However, CLCs are reciprocal elements, which means that, for light travelling backwards, they will undo every change that they implement to light travelling forward. As a consequence, instead of using a mirror to send the light backwards, it becomes necessary to employ a closed optical system. For instance, an optical circulator must be used along with a system of mirrors. The optical circulator constitutes simultaneously, the entrance and exit of our EFM closed optical circuit. The mirrors redirect the light coming from one of the ports of the circulator into another one. Finally, the π-CLC is situated on the circuit in order to implement a modal inversion.

Nonetheless, while the CLC modal inversion (3.2.12) allows to implement fluctuation autocompensation for spatial modes for dimension 2 just like with polarization, it presents an important limitation when designing an autocompensating system for higher dimension. The π-converter always exchanges the pairs of complementary modes $\mathrm{HG}_{n,m} \leftrightarrow \mathrm{HG}_{m,n}$, which enables phase autocompensation between them but not between modes of different pairs. Thus, a way to implement such compensation or a different autocompensating strategy with a different modal transformation are needed.

One possibility consists of implementing a cyclical transformation to realize compensation in a cyclical way. In this way, any spatial mode is transformed into the "following" mode of the modal basis like $\mathrm{HG}_{n,m} \rightarrow \mathrm{HG}_{n+1,m-1}$, with the last mode of the basis turn-

ing into the first (inversion) $\mathrm{HG}_{N,0} \rightarrow \mathrm{HG}_{0,N}$. Such cyclical transformation is known as a Pauli $\hat{X}$-gate. This gate operation has been widely implemented for OAM (LG) modes in four [Schlederer et al., 2016, Babazadeh et al., 2017] and more dimensions [Gao et al., 2019, Brandt et al., 2020] and it can be expressed for dimension D as

$$\hat{X}_{LG}^{(k)} |l\rangle = |(l+k) \mod (D)\rangle \,, \tag{3.2.13}$$

which represents a cyclic operation where each LG mode its transformed to its k-th nearest-neighbour, modulo the number of modes D. Let us consider the $N+1$ possible $\mathrm{LG}_{n,m}$ modes of order $N = n+m$ to implement a modal basis of dimension $D = N+1$. In this case $k = 2$, as it is trivially seen in $l = n - m = N - 2m$, and the matrix transformation $X_{LG}^{(2)}$ can be expressed as

$$\begin{pmatrix} \hat{a}_{LG_{N,0}} \\ \vdots \\ \hat{a}_{LG_{N-i,i}} \\ \vdots \\ \hat{a}_{LG_{0,N}} \end{pmatrix} = \begin{pmatrix} 0 & 1 & \cdots & \cdots & 0 \\ & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ & 0 & \cdots & \cdots & 1 \\ 1 & & \cdots & & 0 \end{pmatrix} \cdot \begin{pmatrix} \hat{a_0}_{LG_{N,0}} \\ \vdots \\ \hat{a_0}_{LG_{N-i,i}} \\ \vdots \\ \hat{a_0}_{lG_{0,N}} \end{pmatrix}, \tag{3.2.14}$$

The matrix expression is valid for any generic $X_{LG}^{(k)}$. If $k = 1$, we can use all possible $\mathrm{LG}_{n,m}$ modes of any order N to generate a modal basis of dimension D.

Now, what we want is to implement a $\hat{X}^{(2)}$-gate for HG modes. To achieve this, we can simply utilize $\pi/2$-converters rotated 45° respect the HG basis to turn HG modes into LG modes, and turn them back again once $\hat{X}^{(2)}$-gate operation for LG modes has been implemented. However, as two $\pi/2$-CLCs equal one π-CLC, which inverts the modes, another π-CLC is needed in order to correct the inversions that destroy the cyclical transformation. In this way, taking into account the CLCs transformations for $\pi/2$ (2.2.89) and π (2.2.91), the $\hat{X}^{(2)}$-gate operation for HG modes is given, in matrix form, by

$$X_{HG}^{(2)} = C_{\pi,\frac{\pi}{4}} \cdot C_{\frac{\pi}{2},\frac{\pi}{4}} \cdot X_{LG}^{(2)} \cdot C_{\frac{\pi}{2},\frac{\pi}{4}} = \mathbb{U} \cdot \mathbb{U} \cdot X_{LG}^{(2)} \cdot \mathbb{I} = X_{LG}^{(2)}. \tag{3.2.15}$$

Therefore, with the addition of these three CLCs we implement an $\hat{X}^2$-gate for HG modes from the one for LG modes.

It is important to note that, if a half-wave plate (HWP) is introduced into the circuit, and its main axis are rotated 45° respect to incident orthonormal polarization states, the EFM will work in the same way as a FM for polarization states. The HWP transformation was given by equation (2.2.40), equivalent to the FM transformation (3.1.8)

$$H_{\pi/4} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{3.2.16}$$

Therefore, it is possible to use both spatial and polarization modes with this autocompensating system, duplicating, then, the dimension used to $D = 2(N+1)$, .

$$\mathrm{EFM} \equiv E = H_{\pi/4} \otimes X_{HG}^{(2)}. \tag{3.2.17}$$

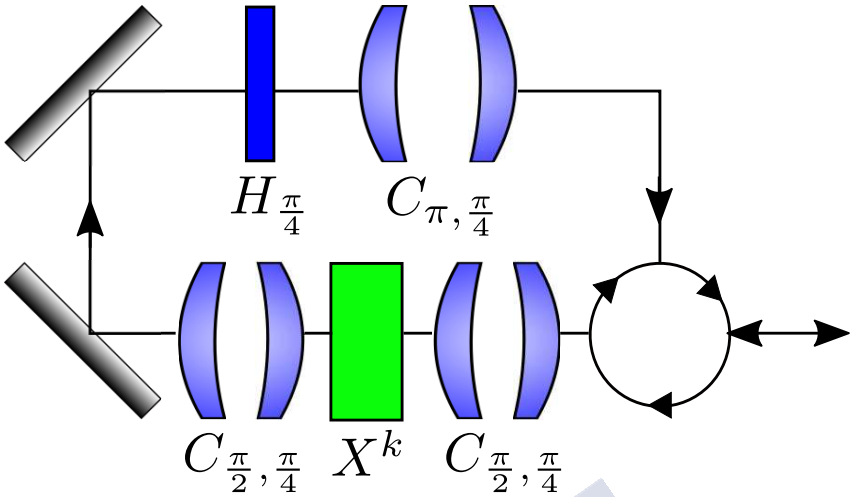


Figure 3.2.3: Effective Faraday Mirror system.

3.2.2 Autocompensating QKD in EC-FMF fibers in high dimension

Combining M spatial propagation modes of a fiber with polarization, a $2M$ quantum states basis can be created to implement a high-dimensional BB84 QKD protocol. In this way, it is important to note that the modes of an EC-FMF can be described by HG modes. Therefore, we can create a quantum state where a single photon can be excited in any of the $2M$ possible modes GS, where $G = \{\mathrm{HG}_{N-k,k}\}_{k=0}^{N}$ represents the spatial mode and $S = H, V$ is the polarization mode, which can be horizontally (H) or vertically (V) polarized along the fiber. Next, by adding phase shifts between the different modes, we can code quantum information. Formally, the qudit we want to generate is the following

$$|\psi\rangle = \sum_{GS} \frac{e^{i\theta_{GS}}}{\sqrt{D}} |GS\rangle =$$

$$= \frac{e^{i\theta_{\mathrm{HG}_{N,0;H}}}}{\sqrt{D}} |1_{\mathrm{HG}_{N,0;H}}\rangle + \frac{e^{i\theta_{\mathrm{HG}_{N,0;V}}}}{\sqrt{D}} |1_{\mathrm{HG}_{N,0;V}}\rangle + \cdots + \frac{e^{i\theta_{\mathrm{HG}_{0,N;H}}}}{\sqrt{D}} |1_{\mathrm{HG}_{0,N;H}}\rangle + \frac{e^{i\theta_{\mathrm{HG}_{0,N;V}}}}{\sqrt{D}} |1_{\mathrm{HG}_{0,N;V}}\rangle \tag{3.2.18}$$

where θ_{GS} represents the phases of the single photon quantum states where the information will be encoded and $D = 2M = 2(N+1)$ is the dimension.

The main requirement that allows to implement BB84 protocol is to work with mutually unbiased bases (MUBs), as defined in the previous chapter in subsection 2.4.1. In consequence, phases θ_{GS} must be chosen to fulfil condition (2.4.145). In subsubsection 2.4.1, we showed MUBs for a general case $D = 2^m$.

3.2.2.1 Multi-loop system

While employing a combination of polarization modes with spatial modes to implement HD-QKD a new problem arises. Let's suppose that the EC-FMF introduce phase shifts ϕ_{GS} to the different GS modes as expressed by matrix

$$T = \text{diag}\left\{e^{i\phi_{GS}}\right\}_{GS} = \text{diag}\left(e^{i\phi_{\text{HG}_{N,0},H}}, e^{i\phi_{\text{HG}_{N,0},V}}, \cdots, e^{i\phi_{\text{HG}_{0,N},H}}, e^{i\phi_{\text{HG}_{0,N},V}}\right). \quad (3.2.19)$$

Phase shifts ϕ_{GS} suffered by modes GS are not guaranteed to be a combination of the phase shifts suffered independently by the polarization and spatial mode. This is,

$$\phi_{GS} \neq \phi_G + \phi_S. \quad (3.2.20)$$

This means that the previous matrix T can not be reduced as

$$T \neq \text{diag}\left(e^{i\phi_{\text{HG}_{N,0}}}, \cdots, e^{i\phi_{\text{HG}_{0,N}}}\right) \otimes \text{diag}\left(e^{i\phi_H}, e^{i\phi_V}\right). \quad (3.2.21)$$

As a consequence, polarization and spatial phases are not compensated in an independent way. If this was the case, polarization would be compensated in just a loop. However, that is not the case for spatial modes

Not taking account of polarization, by looking at the spatial term of our EFM transformation (3.2.17), we can see that, after a round trip employing the EFM between the back and for trips, there is no phase compensation. This happens due to the fact that the EFM turns a spatial mode into its immediate superior following the cyclical transformation, and thus, the phase shifts acquired by the propagating and the counter-propagating spatial mode are summed. In order to realize a fully phase compensation, a single loop is not enough. Instead, the autocompensating system must consist of at least $N + 1$ loops, making necessary a controller in the system to generate loops.

However, as spatial and polarization phase fluctuations are not independent, all the phases in equation (3.2.19) are not going to be fully compensated like this. An additional transformation is required in the controller to fully compensate phases during the loops.

To that end, a *round trip controller* (RTC) is needed in order to send the states from Bob to Alice as many times as required with a polarization inversion. This can be achieved by using a FM, although a device is needed to control if the states are sent back or to Alice or go to Bob's detectors. A standard Mach-Zehnder interferometer with an electro-optic phase modulator can be used, by introducing phases $\delta = 0, \pi$ in one of its arms (as will be shown in Figure P3.3(a)) to control the path of the light. The phase modulator should be synchronized with the return time of photons in order to introduce a phase π when the light states arrive for the first time. As a consequence, light leaves the interferometer on a different path from the one it originally came from, where the FM is found. The Faraday mirror returns the states to Alice for a second time, permuting the polarization modes in order to swap their phases (second inversion). The corresponding permutation of absorption operators can be written in matrix form as follows

$$\text{RTC} \equiv R = FM \otimes \mathbb{I}^{(N+1)}, \quad (3.2.22)$$

where FM is given by (3.1.8) and $\mathbb{I}^{(N+1)}$ is the identity matrix of order $N+1$. The π phases introduced by the FM can be easily be compensated at the end of the system.

However, when the state returns to Bob after the second round trip, the modulator of the RTC will be switch off and will not introduce any phase. Thus, the state will straightforwardly go to the detection system , as the autocompensation of the states will have been achieved.

3.2.2.2 Generating the qudits

The implementation of a round-trip system implies that the final receptor of the encrypted state, Bob, must be the one to produce the original state where Alice is going to code her wished information. Accordingly, Bob can employ a *quantum state generator device* (QSG) consisting of a single photon source emitting a polarized photon and a mode converter (like a phase plate [Balado Souto et al., 2016]) in order to generate a HG mode of order N [Liñares et al., 2017a]. We have seen in subsection 2.2.3.2 that HG modes of order N can be decomposed in a series of HG modes rotated -45° as shown in equation (2.2.61). Therefore, by generating a single-photon state diagonally polarized and excited in a diagonal mode HG of order N, this is, state $|G'S'\rangle$, we have a superposition of modes $|GS\rangle$. However, to correctly generate Bob's initial state $|\psi_0\rangle$, it is necessary to equate the $b(N+1-j, j-1, k)$ coefficients. Thus, Bob's single-photon primary quantum state $|\psi_0\rangle$ is given by

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{D}} \sum_{G,S} |GS\rangle = \\ &= \frac{1}{\sqrt{D}} \left(|1_{\mathrm{HG}_{N,0},H}\rangle + |1_{\mathrm{HG}_{N,0},V}\rangle + \cdots + |1_{\mathrm{HG}_{0,N},H}\rangle + |1_{\mathrm{HG}_{0,N},V}\rangle \right). \end{aligned} \tag{3.2.23}$$

This state is going to be sent to Alice, who will introduce the corresponding relative phases θ_{GS} in it to obtain all the possible qudits states given by equation (3.2.18). Afterwards, Alice must employ an EFM so the encrypted states are sent back to Bob with the right permutations to implement the autocompensation system.

In order to introduce the phase shifts to encode information, different approaches can be used. For example, Alice could make use of general CLCs and wave-plates to introduce phase shifts between the different base states of equation (3.2.23). However, while wave-plates can be reconfigurable, CLCs are not; and so, some complex configurable interferometric circuit with CLCs and phase-plates should be designed. As this requires a complex system, other simple approaches can be used.

A better approach consists of encrypt information in delayed states. In this case, the D base states that make up the state given by equation (3.2.23) can be delayed in Bob's subsystem, arriving at different times to Alice's subsystem. By using a relative phase shifter device (RPS), Alice can introduce different phases θ_{GS} in each of the delayed states generating the state of equation (3.2.18). To achieve this, a time *multiplexer/demultiplexer*

(M/DM) is needed to separate the different modes in time introducing delays τ between each of them. Mathematically, the transformation matrix of this device can be written as

$$D = \text{diag}\left(1, e^{i\omega\tau}, \cdots, e^{i(D-2)\omega\tau}, e^{i(D-1)\omega\tau}\right). \tag{3.2.24}$$

Just like with the propagation phases (3.2.19), the delays are going to be corrected during the autocompensation process. This is the approach considered by us in our device proposed in [Balado Souto et al., 2019] (shown in Figure P3.2). Finally, it is worthwhile to comment that optical delays can also be achieved in a alternative way by taking into account the different propagation constants of the optical modes (intermodal dispersion). Thus, for an enough long optical fiber different delays would be obtained, which would also be cancelled by the autocompensating method.

3.2.2.3 Autocompensating process in dimension D

In Figure 3.2.4 we present the basic sketch of the encryption system required to implement QKD in D dimensions. Alice subsystem consists of the EFM (3.2.17) explained in subsection 3.2.1 in which we can add the *relative phase shifter device* (RPS), which will introduce phases θ_{GS}. Bob's subsystem is composed by the primary quantum state generator device, the multiplexer/demultiplexer, the multi-round trip controller electro-optical device and the detection system (DS), where quantum states are measured once a multi-round trip is made.

As explained previously, Bob's QSG generates the primary quantum state $|\phi_0\rangle$ given by Eq (3.2.23), which goes through an optical circulator and is sent to the M/DM, as the RTC device is switch off in this first loop. As it has been told in the previous section, the M/DM delays the base states ($\hat{D}$), according to equation (3.2.24). Taking into account the different phases shifts ϕ_{GS} introduced by the fiber during propagation ($\hat{T}$), as shown

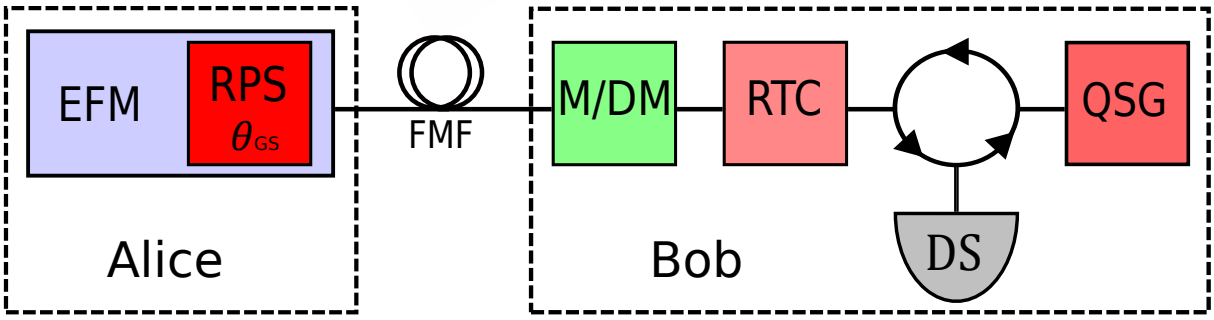


Figure 3.2.4: Sketch of the modal phase autocompensating encryption system. Bob's subsystem is formed by the quantum state generator (QSG), an optical circulator (OC), the round trip controller (RTC), the multiplexer/demultiplexer (M/DM) and the detection system (DS). Alice's subsystem consists of the effective Faraday mirror (EFM) with a relative phase shifter device (RPS) in it.

in matrix (3.2.19), for photons of frequency ω arriving to the Alice subsystem, we obtain the following state

$$|\psi_{A_1}\rangle = \hat{T} \cdot \hat{D} \cdot |\psi_0\rangle \,. \tag{3.2.25}$$

Once the delayed states reach Alice subsystem, the EFM ($\hat{E}$) transforms the quantum state by means of modal inversion according to equation (3.2.17). Next, the state returns to Bob, but the fiber introduces again the phases ϕ_{GS} in the respective modes and the M/DM also introduces new delays. Consequently, delays are compensated when the state crosses the M/DM a second time. However, propagation phases are only compensated in pairs. Thus, the RTC ($\hat{R}$) is switched on in order to implement another round-trip, according to equation 3.2.22, sending the following state back to Alice

$$|\psi_{B_1}\rangle = \hat{R} \cdot \hat{D} \cdot \hat{T} \cdot \hat{E} \cdot \hat{T} \cdot \hat{D} \cdot |\psi_0\rangle \,. \tag{3.2.26}$$

This process is repeated a total of $D/2$ times for dimension D. In the last trip, Alice can introduce phases θ_{GS} into the four delayed base states $|GS\rangle$, as each of them arrives at different times, by means of the RPS ($\hat{P}$). It is important to stress that the order in which the base states arrive to Alice for the last time is not the same in which they got out from Bob the first time, as a consequence of the EFM modal exchange in the different loops and the polarization permutation introduced by the FM between them. Alice must take this into account in order to introduce the phases in the right order to generate the wished state (3.2.18). Thus, the final state that Alice sends to Bob is given by

$$|\psi_{A_{N+1}}\rangle = \hat{P} \cdot \hat{E} \cdot \hat{T} \cdot \hat{D} \cdot \left(\hat{R} \cdot \hat{D} \cdot \hat{T} \cdot \hat{E} \cdot \hat{T} \cdot \hat{D}\right)^N \cdot |\psi_0\rangle \,, \tag{3.2.27}$$

where $P = \text{diag}\left\{e^{i\theta_{GS}}\right\}$ is the operator of the RPS.

Finally, when state (3.2.27) returns to Bob for the last time, the RTC will switch off and the state will straightforwardly go to the detection system through the circulator.

$$|\psi_{B_{N+1}}\rangle = \hat{D} \cdot \hat{T} \cdot \hat{P} \cdot \hat{E} \cdot \hat{T} \cdot \hat{D} \cdot \left(\hat{R} \cdot \hat{D} \cdot \hat{T} \cdot \hat{E} \cdot \hat{T} \cdot \hat{D}\right)^N \cdot |\psi_0\rangle \,. \tag{3.2.28}$$

Therefore, the final state that is measured by Bob can be calculated to be given by

$$|\psi\rangle = e^{i\left(\frac{D(D-1)}{2}\omega\tau + \sum_{GS}\phi_{GS}\right)} \sum_{GS} \frac{e^{i\theta_{GS}}}{\sqrt{D}} |GS\rangle. \tag{3.2.29}$$

We can see that, excluding a global phase, the desired qudit is obtained, so the multi-loop and appropriate modal conversion have allowed to correctly compensate all phase fluctuations and lags in the optical fiber communication system.

3.2.3 Transmission rate limitations

An important feature needs to be taken into account in the proposed system shown in Figure 3.2.4. As the system consists in several loops, it is necessary the states travelling in one loop do not overlap with those in another loop, as Alice's RPS and Bob's RTC must operate differently on them. Therefore, a temporal processing strategy must be used. We are going to see that the optimal strategy depends of the limiting operational time of our system. By limiting time, we understand the bigger one between the minimum operational times of Bob's RTC (t_B) and the period of the QSG (T).

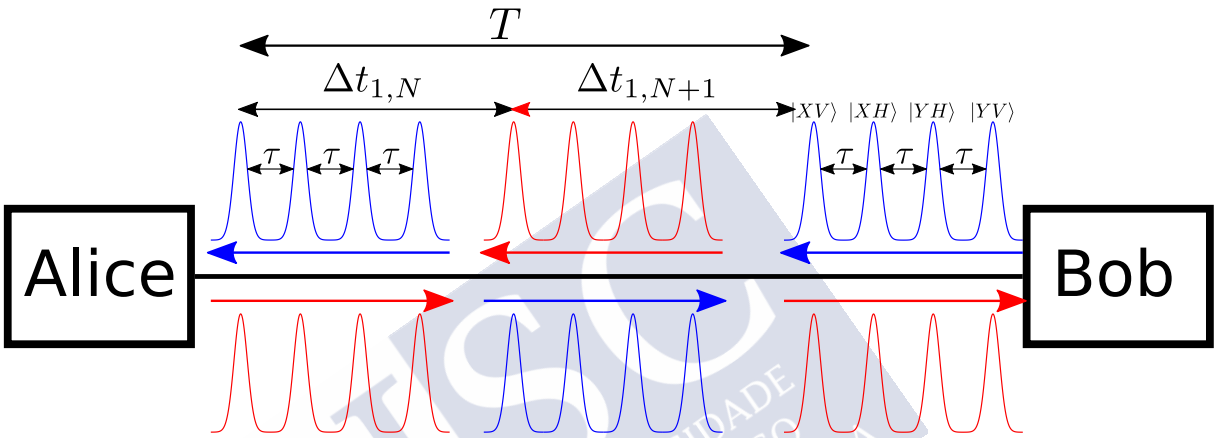


Figure 3.2.5: Transmission strategy of intercalated states for D=4. Blue signals refers to states in the first loop, while red signals are states in the second loop.

Let's consider $t_L = \frac{c_f}{L}$ the time that light takes to go from Alice to Bob through an optical fiber with length L, being c_f the speed of light in the fiber. Trivially, the time it takes a light state to complete a loop is, taking into account the total delay introduced by the M/DM,

$$t = 2t_L + (D-1)\tau, \tag{3.2.30}$$

while the maximum number of photons in the fiber in just one loop will be given by

$$N_p = \left\lfloor \frac{2t_L + (D-1)\tau}{T} \right\rfloor. \tag{3.2.31}$$

A first possibility, consists of intercalate states in different loops (Figure 3.2.5). When the first photon (photon 1) arrives to Bob for the first time and it is sent back to Alice, the time differences between this state and the last one (N_p), as well as the next one (N_p+1), sent by Bob are given by the following expressions:

$$\Delta t_{1,N_p} = 2t_L + (D-1)\tau - (N_p - 1)\,T, \tag{3.2.32a}$$

$$\Delta t_{1,N_p+1} = N_p T - 2t_L - (D-1)\tau. \tag{3.2.32b}$$

As a consequence, the time difference between states sent for the first time and those sent for the second time will be given by

$$\Delta t = \min\left(\Delta t_{1,N_p}, \Delta t_{1,N_p+1}\right), \tag{3.2.33}$$

where $0 \leq \Delta t \leq 2T/D$. However, because of the delay between the different base states during transmissionthe condition $\Delta t > (D-1)\tau$ must be fulfilled. This will prevent delayed states in the second loop to overlap with those in the first loop. This value Δt marks the maximum operation time that Bob's electro-optical modulator in the RTC must fulfil in order to be correctly switched on and off for states travelling in different lops

$$t_B \leq \Delta t. \tag{3.2.34}$$

Obviously, Δt is going to be optimal when states in the different loops are temporally equispaced travel in the middle of those in the first one, this is,

$$\Delta t = \frac{2T}{D}. \tag{3.2.35}$$

Regarding Alice's RPS, its operation time is limited by

$$t_A = \min\left(\tau, \Delta t - (D-1)\tau\right), \tag{3.2.36}$$

where τ is the difference between delayed states and $\Delta t-(D-1)\tau$ is the difference between the group of delayed states in consecutive loops. In order to ensure that the operation time is τ, it is needed that $\Delta t \geq D\tau$. So, we have to select our delay to be

$$\tau \geq \frac{2T}{D^2}. \tag{3.2.37}$$

This strategy has a transmission rate given by

$$Rt = \frac{N_p}{t_L + (D-1)\tau} = \frac{1}{t_L + (D-1)\tau}\left\lfloor \frac{2t_L + (D-1)\tau}{T} \right\rfloor \approx \frac{1}{T}, \tag{3.2.38}$$

this is, the rate depends on the frequency of the state generation. We also have seen that the operational times of Alice and Bob's modulators must fulfil

$$t_A \approx \tau < T, \tag{3.2.39a}$$

$$t_B \approx \frac{2T}{D} < T. \tag{3.2.39b}$$

Because of the delay of the states, condition (3.2.39a) must be fulfilled in any kind of transmission method. However, condition (3.2.39b) is not necessary in other methods. for example, another possible strategy for information processing is to send series of N_p states during a time $2t_L$ and stop during the same amount of time. This way, t_B can be

as big as $2t_L$, although it still needs a fast response time. This method is easier to apply, but the transmission rate is trivially reduced by a factor $D/2$ if the period T is the same

$$Rt = \frac{2N_p}{D \cdot (2t_L + (D-1)\tau)} \approx \frac{2}{DT}. \tag{3.2.40}$$

Another possibility is to implement a combination of both strategies (Figure 3.2.6). This is, intercalating n_g groups of n_p photons each one travelling in different loops. If t_g is the duration time of a group, the number of photons in it is going to be given by

$$n_p = \left\lfloor \frac{t_g}{T} \right\rfloor, \tag{3.2.41}$$

while the number of groups travelling in the same loop is

$$n_g = \frac{2}{D} \left\lfloor \frac{t_L}{t_g} \right\rfloor. \tag{3.2.42}$$

Trivially, in this case t_B is limited by t_g. The transmission rate is going to be given again by

$$Rt = \frac{n_p \cdot n_g}{2t_L + (D-1)\tau} \approx \frac{2}{DT}. \tag{3.2.43}$$

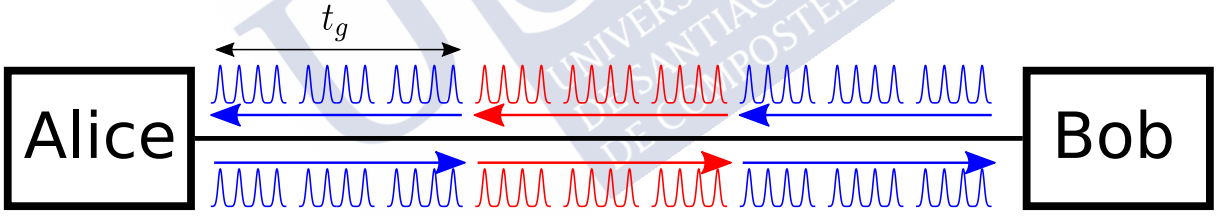


Figure 3.2.6: Transmission strategy of intercalated groups of states for D=4. Blue signals refers to states in the first loop, while red signals are states in the second loop.

3.2.4 Autocompensation in two dimensions

Let us consider the most basic case with $D = 2$, that is, using the fundamental HG modes to implement the original quantum encryption protocol BB84, instead of using polarization. We proposed such a system in [Balado et al., 2017] In particular, the basic modes of an EC-FMF, $\mathrm{LP}_{11\alpha}$, with $\alpha = c, s$ ($\cos\varphi$ and $\sin\varphi$ azimuthal dependence, respectively), correspond to HG modes HG_{10} (X) and HG_{01} (Y), where X and Y directions are parallel to the main axis of the elliptical core of the fiber. Utilizing these modes as base modes, we can build the following single-photon qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|1_X\rangle + e^{i\theta} |1_Y\rangle \right), \tag{3.2.44}$$

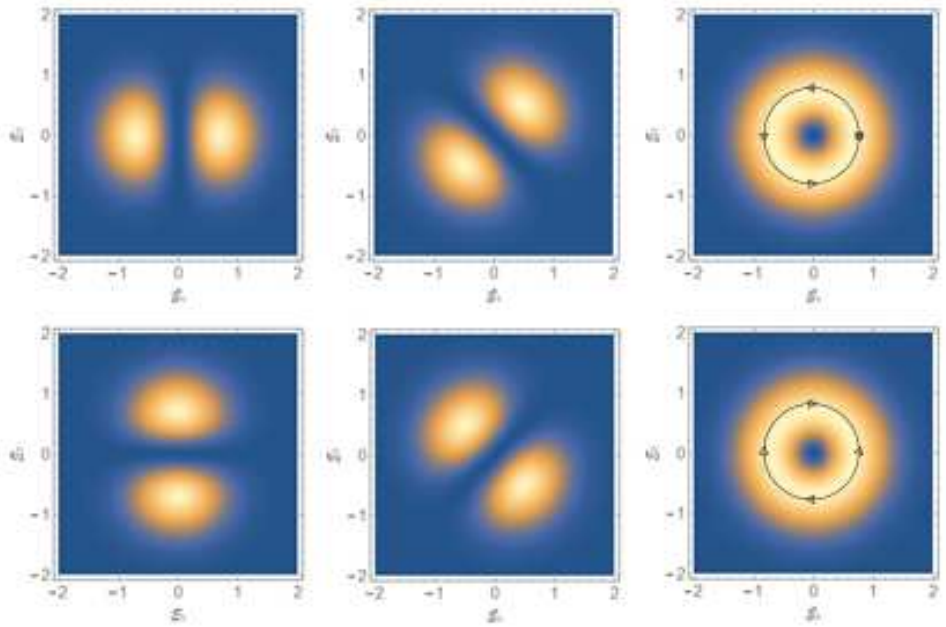


Figure 3.2.7: (Top to bottom) X, Y, X', Y', L, D modes.

where $\theta = 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ is the phase between modes where the quantum information is encoded. When $\theta = 0, \pi$, we have the basis formed by the symmetric (X') and antisymmetric (Y') linear combination of X and Y modes ($\bigoplus$), that is, diagonal basis ($\bigotimes$). While when $\theta = \frac{\pi}{2}, \frac{3\pi}{2}$, the basis will be formed by the vortex modes, that is, the Laguerre-Gaussian modes LG_{10} (D) and LG_{01} (L), that is, circular basis ($\bigodot$). The six modes of the linear, diagonal and circular basis are shown in Figure 3.2.7.

3.2.4.1 Generator

As explained in 3.2.2.2, two different approaches can be employed. Developing a system to introduce phases between the base modes or delaying them and introducing a phase in one. Let us considerate the former possibility first. For instance, two CLCs $C_{\pi/2}$ and C_{π} can be used to introduce the four possible θ phases. Alternatively, a Dove prism can be used in the place of the C_{π}, as it behaves the same way.

In Figure 3.2.8 we show an example device that makes use of polarization as an auxiliary tool in order to control the phase introduced between the spatial modes. This phase modulator (PM) can be divided into main parts of identical configuration. First, we can generate state $|1_{X'}\rangle = \frac{1}{\sqrt{2}}(|1_X\rangle + |1_Y\rangle)$ by means of a phase plate [Balado Souto et al., 2016] and polarized it using a polarizer. Next, an electro-optic device, such as a Pockels cell, is required in order to rotate the polarization mode of the states that passes through. Thus, by making use of a PBS, the state goes through different paths according to the polarization rotation introduced by us. In one of them, optical components, $C_{\pi/2,0}$ for PM_1 and $C_{\pi,0}$ for PM_2, are placed with axis oriented in the linear basis *bigoplus*. In

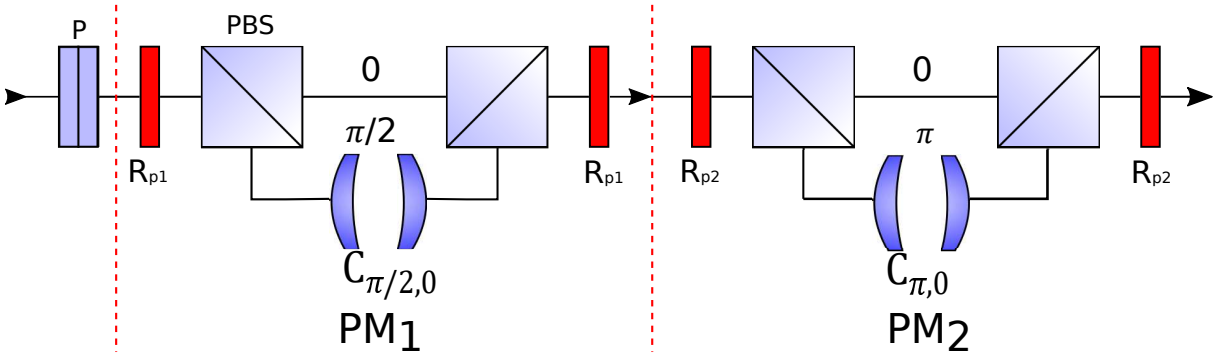


Figure 3.2.8: Generator device of modes X', L, Y', D.

this way, by controlling the path for which the state circulates, a phase θ_i is introduced between the modes X and Y, $\theta_1 = 0, \pi/2$ for PM_1 and $\theta_2 = 0, \pi$ for PM_2. Finally, another PBS is used to merge both paths which pass through a second Pockels cell synchronized with the first one, recovering the original polarization mode. In summary, the full PM implements the following transformation

$$PM = |1_X\rangle\langle 1_X| + e^{i(\theta_1+\theta_2)}|1_Y\rangle\langle 1_Y| \tag{3.2.45}$$

However, to correctly implement auto compensation it is better to send modes $|1_X\rangle$ and $|1_Y\rangle$ delayed and introduce a global phase θ to the latter. Therefore, PM can consist of a reconfigurable phase plate. To introduce the delay between both modes an MZIC_π can be used. It works as PBS for modes X and Y, so the output of the latter can be connected with the free input of the interferometer with a delay fiber, to delay both modes.

3.2.4.2 Detector

Once Bob corrects the delay between states $|1_X\rangle$ and $|1_Y\rangle$, recuperating state (3.2.44), he needs to randomly measure in diagonal ($\otimes$) and circular ($\odot$) basis, as it is required to implement the BB84 protocol. The sketch of our proposed receiving device is shown in Figure 3.2.9. It consists of two Mach-Zehnder interferometers with CLCs (MZIC), connected to the two outputs of a BS, and whose outputs end in photon detectors. Incident photons into the BS will get out by any of the outputs with equal probability.

Each one of the MZICs is designed to measure in each of the two basis. Both of them have phase shifting components in one of their arms in order to introduce a phase π between the respective modes of the measurement basis. In the case of the $\text{MZIC}_\otimes$, a $C_{\pi,\pi/2}$, whose main axis are aligned in the diagonal basis, is placed in one of its arms to phase shift modes X' and Y'. In the case of the $\text{MZIC}_\odot$, two C_π rotated 45° between them are required to obtain a phase shift π between modes L and D. However, these prisms also introduce a phase shift of $\pi/2$ between both arms, so a retarder is necessary in the other arm to compensate.

Mathematically, the transformation of an incident state into the MZIC of the same basis will be given by

$$\hat{M}_Z = -\left|1_{A,v}\right\rangle \left\langle 1_{A,h}\right| + \left|1_{B,h}\right\rangle \left\langle 1_{B,h}\right|, \tag{3.2.46}$$

where $A = X'/L$ and $B = Y'/D$ represent the mode of the incident state and h and v refers to the two outputs of the interferometer. In consequence, the two quantum states of the corresponding base will get out of the MZIC by different outputs, while the ones from the other base can exit by any output with equal probability.

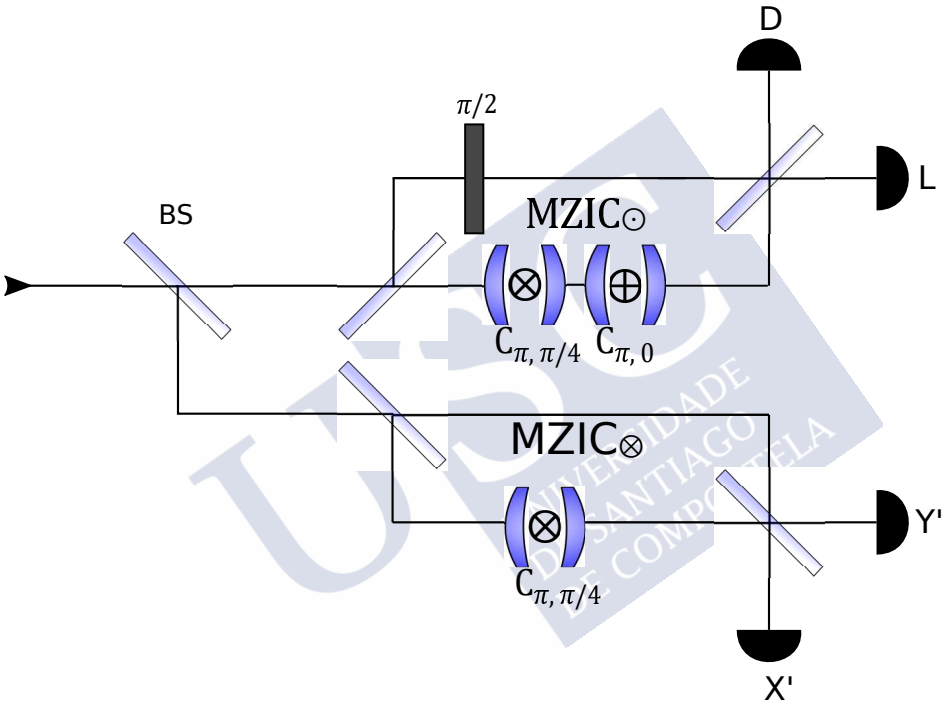


Figure 3.2.9: Detector device of modes X', L, Y', D.

3.2.4.3 Autocompensating system

The proposed plug and play autocompensation system is shown in Figure 3.2.10. First, Bob produces a single-photon state in mode X', as it is equivalent $|1_{X'}\rangle = \frac{1}{\sqrt{2}}(|1_X\rangle + |1_Y\rangle)$. Next, this state goes through an MZIC, with axes aligned in basis $\bigotimes$, which separates states $|1_X\rangle$ and $|1_Y\rangle$, with the former going through a delay fiber.

Both states enter in an optical circulator and are transmitted by the fiber. The phase shifts experimented within the fiber are given by equation (3.1.5) for dimension 2. Nonetheless, if we employ a polarization maintaining EC-FMF, we can consider fluctuations caused by modal crosstalk. So the general fluctuations induced by the fiber are given by a general SU(2) transformation

$$T_{BA}^{(2)} = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}, \quad T_{AB}^{(2)} = \begin{pmatrix} a & -b \\ b^* & a^* \end{pmatrix}, \tag{3.2.47}$$

where T_{BA} and T_{AB} represent the fluctuations of the trip from Bob to Alice and vice versa, being differentiated for a sign change $b \to -b = b^*$.

Then, Alice employs a simple EFM, containing only a CLC $C_{\pi,\pi/4}$ (3.2.12) as explained in subsection 3.2.1, to exchange X and Y modes and uses a PM to introduce a phase θ into the delayed mode as (3.2.45). When the states return to Bob through the fiber, all the fluctuations and phases are compensated. Mathematically, the transformations throughout transmission process for each of the base states is given by

$$\hat{T}_{AB}^{(2)} \cdot \hat{PM} \cdot \hat{C}_{\pi,\frac{\pi}{4}} \cdot \hat{T}_{BA}^{(2)} |1_{Y/X}\rangle = e^{i\theta_{X/Y}} |1_{Y/X}\rangle \tag{3.2.48}$$

Finally, the delay is corrected by means of the same MZIC and state (3.2.44) is obtained, This state travels through a circulator and is measured in the detector device (3.2.46)

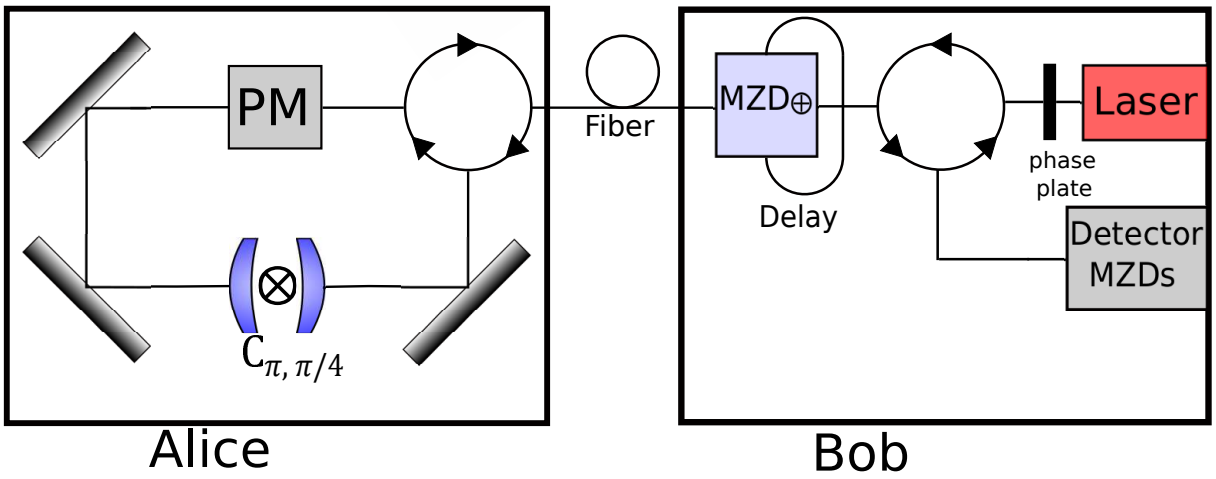


Figure 3.2.10: Plug and play autocompensating system for dimension 2.

3.2.5 Autocompensation in four dimensions

As it has been previously explained, we can combine the spatial modes X and Y with polarization H and V in order to implement a four dimensional BB84 protocol. An autocompensating system to implement this was proposed in our work *Phase autocompensating high-dimensional quantum cryptography in elliptical-core few-mode fibers* published on *Journal of Modern Optics* **66** (9) in 2019. This work [Balado Souto et al., 2019] is added as section P3, where it is explained in detail. The autocompensating system follows the same scheme and process explained in subsection 3.2.2, particularized for the case $D = 4$. Specifically, we present how the autocompensating protocol would work, the devices required for its implementation and a security analysis of the same.

The structure of our work is as follows. First, subsection P3.1 is an introduction where our problem and work is contextualized. Next, in subsection P3.2, the single-photon quantum states excited in the polarized spatial modes of an EC-FMF needed to implement the BB84 protocol in four dimensions are introduced. In particular, from equation (3.2.18) we have the following ququart

$$\begin{aligned} |\psi\rangle = \sum_{GS} \frac{e^{i\theta_{GS}}}{2} |GS\rangle = \\ = \frac{e^{i\theta_{XH}}}{2} |XH\rangle + \frac{e^{i\theta_{XV}}}{2} |XV\rangle + \frac{e^{i\theta_{YH}}}{2} |YH\rangle + \frac{e^{i\theta_{YV}}}{2} |YV\rangle , \end{aligned} \tag{3.2.49}$$

where θ_{GS}, with $G = X, Y$ and $S = H, V$, are the coding phases of the single-photon quantum states, chosen to implement the MUB basis in four dimension (2.4.147).

Afterwards, subsection P3.3 is dedicated to explain the phase autocompensation system for four dimensions, shown in Figure P3.2. More concretely, subsubsection P3.3.1 briefly explains the mode converters and MZIs already explained in chapter 2 (subsubsections 2.2.3.3 and 2.2.3.5). Next, in subsubsection P3.3.2 the different devices needed to generate a double loop system are explained in detail. These devices consist of the optical fiber delay device (OFD) (shown in Figure P3.3(b)), which is our M/DM device for four dimensions, the round trip controller (RTC) (Figure P3.3(a)), to implement a double loop, and the modal inversion device (MID), which consists in a π-converter and a HWP as already explained in 3.2.1. Then, the autocompensating process is mathematically explained in subsubsection P3.3.3.

Subsection P3.4 presents in detail the detection devices, shown in figures P3.4(a) and P3.4(b), required to measure state (3.2.49) in the four different MUB basis and makes a particular study of the transmission rate limitations explained in subsection 3.2.3.

Finally, a cryptographic security analysis of our system under side channel attacks is made in subsection P3.5. This security study is further explained in next section 3.3. Last, conclusions are presented in subsection P3.6.

3.3 Cryptographic Security Study under Side Channel Attacks

A new autocompensating system to implement BB84 protocol in high dimension has been proposed. However, the system may be subjected to classical attacks and flaws suffered by other QKD systems. In this section we are going to explain about different attacks that can be used against our system and we are going to realize a short study about the security of the cryptographic system previously described.

3.3.1 Photon number splitting attack and decoy states protocol

One of the main drawbacks of any QKD protocol involving single-photon states is the fact that there are no ideal single-photon sources. For example, most of the times, highly attenuated lasers are employed as sources. Unfortunately, this kind of sources sometimes produce signals that contain more than one photons. For example, be it a weak coherent source, as explained in subsection 2.1.2 that generates the coherent state (2.1.15). We saw that phase randomization generates a mixture of Fock states $|n\rangle$ (2.1.18) with probability P_n given by the Poissonian distribution (2.1.19) These multi-photon signals are a flaw that can be exploited in new kinds of eavesdropping attacks like the *photon number splitting* (PNS) attack.

The basic idea of the PNS attack was proposed by Huttner in 1995 [Huttner et al., 1995] and developed in other works [Yuen, 1996,Lütkenhaus, 2000,Lütkenhaus and Jahma, 2002]. The PNS attack is based on the assumption that an eavesdropper, Eve, can be able to measure the number of photons contained by each signal emitted by Alice and manipulate them in order to gain information. To do this, first, Eve selectively suppresses all the single-photon signals in the transmission channel. Second, Eve splits multi-photon signals to acquire a copy of the signal, sending the other to Bob. As a consequence, Eve acquires an identical copy of the state send to Bob by Alice because the photons in each signal have been coded identically by Alice. As the basis employed by Bob and Alice to code and measure the states are going be publicly transmitted by a classical channel, Eve can measure her signals, as long as she has preserved them, in the proper basis, getting full information about the key. Thus, the unconditional security of QKD has been completely compromised.

Let's suppose that a QKD system has a yield of Y, which means that only a fraction Y of the sent states arrive to Bob, and that $P_{n>1} = \sum_{n=2}^{\infty} P_n$ is the probability of generate a multi-photon state. Then, it is trivial that if $Y < P_{n>1}$, the system is not secure. However, when

$$Y > P_{n>1}, \tag{3.3.50}$$

selective suppression of single-photon states is going to reduce the detected Y, while abnormally increasing the yield of multi-photon states, open a possibility of detecting Eve's eavesdropping. This is the origin of the *decoy state* method, originally proposed by

Hwang in 2003 [Hwang, 2003] and actively developed since then [Ma et al., 2005, Curty et al., 2010, Tamaki et al., 2016].

The decoy-state method consists of Alice generating two kind of photon pulses by changing the intensity of the source. This way, she generates signal states ($\mu = s$), to implement the BB84 protocol, and decoy states ($\mu = d$), to detect the PNS attack. If $d > s$, decoy states are going to be mostly multi-photon pulses. Since Eve cannot distinguish between decoy and signal states, when employing the PNS attack she is going to increase the yield of the decoy pulses respect to the yield of the signal pulses. Therefore, Alice and Bob can detect the PNS attack by checking the yields of both kinds of pulses.

Let us describe the protocol in more detail. Be Y_s and Y_d the yields of signal and decoy states, respectively, be Y_s^m and Y_d^m the yields of the multi-photon states of both pulses.

$$Y_s = \sum_n P_n(s) y_n, \quad Y_s^m = \sum_{n=2}^{\infty} P_n(s) y_n, \tag{3.3.51a}$$

$$Y_d = \sum_n P_n(d) y_n, \quad Y_d^m = \sum_{n=2}^{\infty} P_n(d) y_n, \tag{3.3.51b}$$

where y_n is the yield of state $|n\rangle$ and P_n, its generation probability (2.1.19). Alice encode information in the signal pulses to perform the BB84 protocol, while replaces a portion of them by decoy states. After the pulses are received by Bob, Alice tells him which states are decoys. Thus, they can estimate the yields of the signal (Y_s) and decoy pulses (Y_d). If Y_d is much bigger than Y_s, they abort the whole protocol, as it is clear that Eve is eavesdropping. Otherwise, they continue the protocol by estimating yield of multi-photon signal pulses (Y_s^m) with the yield Y_d and checking that is lower than Y_s.

This estimation goes as follows. The normalized yields of multi-photon signal states is given by

$$\tilde{Y}_s^m = \frac{\sum_{n=2}^{\infty} P_n(s) y_n}{\sum_{n=2}^{\infty} P_n(s)}. \tag{3.3.52}$$

Introducing the multi-photon yield of the decoy states (3.3.51b) in expression (3.3.52) we have

$$\tilde{Y}_s^m = \frac{\sum_{n=2}^{\infty} P_n(s) y_n}{\sum_{n=2}^{\infty} P_n(d) y_n} \frac{Y_d^m}{\sum_{n=2}^{\infty} P_n(s)}, \tag{3.3.53}$$

As the larger the number of photons of a given pulse is, the more probable it is to be a decoy pulse, Eve's optimal strategy is to block pulses with more than 2 photons. So, it can be proven by statistics that the first fraction in equation (3.3.53) is going to be bounded by $\frac{P_2(s)}{P_2(d)}$. As trivially $Y_d^m < Y_d$, expression (3.3.53) turns into

$$\tilde{Y}_s^m \leq \frac{P_2(s)}{P_2(d)} \frac{Y_d}{\sum_{n=2}^{\infty} P_n(s)}, \tag{3.3.54}$$

As explained, in order for the protocol to be secure, condition of security (3.3.50) must be fulfilled. Which means that the total number of pulses that are detected must

be greater than that of attacked ones. Condition (3.3.50) can be written as

$$Y_s > \max\left\{\tilde{Y}_s^m\left[\sum_{n=2}^{\infty} P_n(s)\right]\right\} \tag{3.3.55}$$

Introducing expression (3.3.54) into (3.3.55), the condition security of the decoy method becomes

$$Y_s > \frac{P_2(s)}{P_2(d)} Y_d. \tag{3.3.56}$$

After calculating the yields of both pulses, as long as condition (3.3.50) is fulfilled, Alice and Bob know that the channel is safe. Assuming that the source has a perfect Poissonian distribution (2.1.19), equation (3.3.50) can be written as

$$\frac{P_2(s)}{P_2(d)}\frac{d}{s} = e^{i(d-s)}\frac{d}{s} < 1. \tag{3.3.57}$$

3.3.2 Quantum cloning

It is well known that quantum cryptography is based on the fact that measuring a quantum state inevitably perturbs such state altering its information. This way, any eavesdropper that wants to get information by attacking directly the transmitted coded state will perturb it, because it is impossible for them to generate a perfect copy of it, as indicated by the no-cloning theorem.

Csiszár and Körner [Csiszár and Korner, 1978] obtained in 1978 a minimum bound for the secret key rate R under an incoherent attack. This is, any attack where Eve attacks individually and in the same way each of the states sent by Alice. Therefore, the fraction of secret bits that Alice and Bob can extract under a regular one-way QKD protocol is

$$R \geq \max(I_{AB} - I_{AE}, I_{AB} - I_{BE}), \tag{3.3.58}$$

where I_{AB}, I_{AE} and I_{EB} represent the mutual information shared between Alice and Bob, Alice and Eve, and Bob and Eve, respectively. The mutual information is defined as

$$I(X;Y) = H(X) + H(Y) - H(X,Y) = H(X) - H(X|Y), \tag{3.3.59}$$

where H is the Shannon entropy, being $H(X,Y)$ the joint entropy and $H(X|Y)$ the conditional entropy.

$$H(X) = -\sum_i p(x_i)\log_2 p(x_i)$$

$$H(X,Y) = -\sum_{x,y} p(x,y)\log_2 p(x,y), \qquad H(X|Y) = -\sum_y p(y)\sum_{x,y} p(x|y)\log_2 p(x|y) \tag{3.3.60}$$

Defining the quantum bit error rate (QBER) E_R as the fraction of wrong bits obtained by Bob respect to the ones sent by Alice, it is immediate that the mutual information between Alice and Bob can be written as

$$I(A;B) = 1 - H(E_R) = 1 - H(F), \tag{3.3.61}$$

where $F = 1 - E_R$ is the fidelity, the fraction of correct bits received by Bob. Thus Eve's optimal attack will be the one that maximizes $I(A;E)$ and $I(B;E)$ for a particular E_R.

3.3.2.1 No-cloning theorem

Let us suppose that we have an arbitrary quantum state $|\Psi\rangle$. For different reasons, one may want to generate a copy of this state by making it interact with a previously prepared in a blank reference state $|Ref\rangle$ as follows

$$|\Psi\rangle \otimes |Ref\rangle \xrightarrow{?} |\Psi\rangle \otimes |\Psi\rangle \tag{3.3.62}$$

For Eve, this will allows her to obtain a perfect copy of a qubit sent by Alice to Bob without perturbing the original, gaining full information without making her presence detectable. However, this procedure is impossible. This is stated by the no-cloning theorem, which was demonstrated by Wootters and Zurek [Wootters and Zurek, 1982] and by Dieks [Dieks, 1982] in 1982. This theorem can be enunciated as follows:

"No quantum operation exists that can duplicate perfectly an arbitrary quantum state."

$$|\Psi\rangle \otimes |Ref\rangle \otimes \ldots \otimes |Ref\rangle \not\rightarrow |\Psi\rangle \otimes |\Psi\rangle \otimes \ldots \otimes |\Psi\rangle \tag{3.3.63}$$

This can be proved with a *reductio ad absurdum* [Wootters and Zurek, 1982]. Let us suppose that we realize a quantum cloning by means of an unitary transformation with help of an auxiliary system (machine). Then, we have

$$\hat{U} \cdot |\Psi\rangle \otimes |Ref\rangle \otimes |\mathcal{M}\rangle = |\Psi\rangle \otimes |\Psi\rangle \otimes |\mathcal{M}(\ominus)\rangle \tag{3.3.64}$$

If, for example, we have two orthogonal states representing information bits $\Psi = 0, 1$, we can write

$$\hat{U} \cdot |0\rangle |Ref\rangle |\mathcal{M}\rangle = |0\rangle |0\rangle |\mathcal{M}\rangle (0), \tag{3.3.65a}$$

$$\hat{U} \cdot |1\rangle |Ref\rangle |\mathcal{M}\rangle = |1\rangle |1\rangle |\mathcal{M}(1)\rangle . \tag{3.3.65b}$$

Now, if we cloned the mixed state $|0\rangle + |1\rangle$ by the same way, we will obtain

$$\hat{U} \cdot (|0\rangle + |1\rangle) |Ref\rangle |\mathcal{M}\rangle = (|0\rangle + |1\rangle) (|0\rangle + |1\rangle) |\mathcal{M}(1)\rangle = (|00\rangle + |01\rangle + |10\rangle + |11\rangle) |\mathcal{M}(1)\rangle . \tag{3.3.66}$$

However, it is evident that state (3.3.66) is not equal to the sum of states (3.3.65a) and (3.3.65b). In consequence, it is demonstrated that equation (3.3.64) can not be true, proving the no-cloning theorem.

3.3.2.2 Quantum cloning machine

However, while perfect cloning is impossible, it was soon proved that it is possible to obtain an unitary transformation of the way

$$\hat{U} \cdot |\Psi\rangle_A \otimes |Ref\rangle_B \otimes |\mathcal{M}\rangle_C = |\Psi_F\rangle_{ABC}\,, \tag{3.3.67}$$

where state $|\Psi_F\rangle_{ABC}$ holds the information of the original qubit $|\Psi\rangle_A$ shared between modes A and B as

$$\rho_A = \rho_B = F\,|\Psi\rangle\langle\Psi| + (1-F)\,|\Psi^{\perp}\rangle\langle\Psi^{\perp}|\,. \tag{3.3.68}$$

This means that, despite the original state has been modified, both modes A and B share the same amount of information about the original state that it is given by the parameter fidelity $F = \langle\Psi|\rho_j|\Psi\rangle$. Therefore, it is possible to realize an imperfect cloning of the state.

The first ones to obtain a transformation like equation (3.3.67) where Bužek and Hillery in 1996 [Bužek and Hillery, 1996]. They found that, for a qubit of the form $|\vartheta\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$,

$$\hat{U} \cdot |\vartheta\rangle_A \otimes |Ref\rangle_B \otimes |\mathcal{M}\rangle_C = \sqrt{\frac{2}{3}}\,|\vartheta\rangle_A\,|\vartheta\rangle_B\,|\vartheta^{\perp}\rangle_C - \sqrt{\frac{1}{6}}\left[|\vartheta\rangle_A\,|\vartheta^{\perp}\rangle_B + |\vartheta^{\perp}\rangle_A\,|\vartheta\rangle_B\right]|\vartheta^{\perp}\rangle_C\,, \tag{3.3.69}$$

where $|\vartheta\rangle = \alpha^*\,|0\rangle^* + \beta\,|1\rangle$. We can see in equation (3.3.69) that modes A and B can be exchanged without problem. Calculating the density matrix for both modes we obtain

$$\rho_A = \rho_B = \frac{5}{6}\,|\vartheta\rangle\langle\vartheta| + \frac{1}{6}\,|\vartheta^{\perp}\rangle\langle\vartheta^{\perp}|\,. \tag{3.3.70}$$

Thus, the fidelity of the cloned state respect to the original state is $F = \frac{5}{6}$, which means that the cloned state has a quite large proportion of information about the original state $|\vartheta\rangle$.

The Bužek-Hillery unitary transformation was the first quantum cloning machine (QCM). A quantum cloning machine is defined as the pair of the unitary transformation $\hat{U}$, implemented by a quantum processor, and the auxiliary quantum state $|\mathcal{M}\rangle$,

$$QCM = \left\{\hat{U}, |\mathcal{M}\rangle\right\}, \tag{3.3.71}$$

that implements any kind of shuffling of the quantum information of an original quantum system into all of the possible subsystems. In other words, a QCM implements a cloning of quantum states that can be expressed in general form as

$$\hat{U} \cdot \left(|\Psi_0\rangle^{\otimes N}\right) \otimes \left(|\Psi_0\rangle^{\otimes M-N}\right) \otimes |\mathcal{M}\rangle = |\Psi_F\rangle\,, \tag{3.3.72}$$

where N is the number of particles that carry the original pure state $|\Psi_0\rangle$ and M is the number of final copies that are going to be obtained. If all the copied states share the same information, the QCM is denominated *universal*. A QCM can be, as well, *symmetrical*, when the fidelity F_i is equal for each state $|\Psi_i\rangle$, and *optimal*, when the fidelity of the clones have the maximum value allowed by quantum mechanics. In this way, the Bužek-Hillery fulfils all the three definitions.

3.3.2.3 Quantum cloning attack on the BB84 protocol

Quantum cloning machines have been applied as incoherent attacks in quantum cryptography. In the case of BB84 protocol in two dimensions, it has been shown that an optimal attack can be obtained when Eve makes use of a phase-covariant cloner to copy both qubits, like the one described by Niu and Griffiths (1999) in [Niu and Griffiths, 1999]. In this case, the QCM implements a cloning transformation of a two-qubit system as follows

$$\begin{aligned} |0\rangle|0\rangle &\rightarrow |0\rangle|0\rangle, \\ |1\rangle|0\rangle &\rightarrow \cos\eta\,|1\rangle|0\rangle + \sin\eta\,|1\rangle|0\rangle. \end{aligned} \tag{3.3.73}$$

where $|Ref\rangle = |0\rangle$.

Let us suppose that Alice codes information by means of a phase shift θ_ξ between states $|0\rangle$ and $|1\rangle$. This is, she generates the following general qubit

$$|\xi\rangle_A = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta_\xi}|1\rangle\right), \tag{3.3.74}$$

where we have qubits $|\xi\rangle = |0_\otimes\rangle, |1_\otimes\rangle$ if $\theta_\xi = 0, \pi$ and $|\xi\rangle = |0_\odot\rangle, |1_\odot\rangle$ if $\theta_\xi = \frac{\pi}{2}, \frac{3\pi}{2}$. When Eve interferes state (3.3.74) and implements the cloning transformation (3.3.73), the following state is obtained

$$|\xi\rangle_B|0\rangle_E \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + \cos\eta e^{i\theta_\xi}|1\rangle|0\rangle + \sin\eta e^{i\theta_\xi}|1\rangle|0\rangle\right), \tag{3.3.75}$$

where indexes B and E refer to the states obtained by Bob and Eve. By calculating the partial density matrices of both modes we have

$$\rho_B = \frac{1}{2}\begin{pmatrix} 1+\sin^2\eta & \cos\eta e^{-i\theta_\xi} \\ \cos\eta e^{+i\theta_\xi} & 1-\sin^2\eta \end{pmatrix}, \quad \rho_E = \frac{1}{2}\begin{pmatrix} 1+\cos^2\eta & \sin\eta e^{-i\theta_\xi} \\ \sin\eta e^{+i\theta_\xi} & 1-\cos^2\eta \end{pmatrix}. \tag{3.3.76}$$

Therefore, it is straightforward to calculate the fidelities of both states respect to the original one sent by Alice (3.3.74)

$$\begin{aligned} F_B &= \langle\xi|\rho_B|\xi\rangle = \frac{1}{2}(1+\cos\eta), \\ F_E &= \langle\xi|\rho_E|\xi\rangle = \frac{1}{2}(1+\sin\eta). \end{aligned} \tag{3.3.77}$$

We can observe that both fidelities are independent of the phase θ_ξ and, thus, they are independent of the coded qubit that Alice sent. These fidelities have a range of values between $\left[\frac{1}{2}, 1\right]$ and, when $\eta = \frac{\pi}{4}$, they are equal $F_B = F_E = \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right) \approx 0.8535$. This is the optimal case, as Eve wants to have the maximum possible information of Alice qubit without perturbing to much the one that Bob receives. Trivially, this case generates an error rate of $E_R = 1 - F_B \approx 0.1465$.

The mutual information between Alice and both, Bob and Eve, is determined by their fidelities (3.3.77). Thus, Alice and Bob mutual information is given by $I(A;B) = 1 - H(F_B)$, meanwhile Alice and Eve's is given by $I(A;E) = 1 - H(F_E)$. For the optimal case, both quantities are the same $I(A;B) = I(A;E)$ and, in consequence, the key generation rate is going to be $R \geq 0$. Evidently, the optimal case is the limit case where Alice and Bob can transmit a key in a secure way. This reduces the original limit of the error rate from $E_R = 0.25$ to $E_R = 0.1465$. Others QCM involving an auxiliary state $|\mathcal{M}\rangle$ have also been proposed [Griffiths and Niu, 1997, Bruß et al., 2000].

3.3.2.4 Security of a HD-QKD system under quantum cloning attacks

Most of quantum cloning works applied to QKD have put too emphasis on the two dimensional case, as it is the most widespread. However, Cerf et al. analysed an attack based on quantum cloning machines for a BB84 protocol of dimension $D = N$ [Cerf et al., 2002]. They made an study of the security for different dimensions and number of basis used to obtain different expressions of the secret key rate R. The cloning transformation used by Cerf, as defined in [Cerf, 2000], transforms a state send by Alice in the way

$$|\Psi\rangle_A \rightarrow \sum_{n,m=0}^{N-1} a_{n,m} \hat{U}_{n,m} |\Psi\rangle_B , |B_{n,-m}\rangle_{E,E'} \tag{3.3.78}$$

where A, B, E, and E' stand for Alice's qudit, Bob's clone, Eve's clone and cloning machine, respectively. $|B_{n,-m}\rangle_{E,E'}$ states refer to the N-dimensional Bell states given by

$$|B_{n,-m}\rangle_{E,E'} = \frac{1}{\sqrt{N}} \sum_{k=0}^{n+m-1} e^{2\pi i \frac{kn}{N}} , |k\rangle_E |k+m\rangle_{E'} \tag{3.3.79}$$

and the unitary cloning transformation is

$$\hat{U}_{n,m} = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{kn}{N}} |k+m\rangle \langle k| , \tag{3.3.80}$$

where states $|k\rangle$ are the computational states $k = 0, 1, ..., N-1$.

Implementing this QCM attack, Cerf et al. obtained that the mutual information between Alice and Bob $I(A;B)$ is independent of the number of basis used and is given by

$$I(A;B) = \log_2 N + F \log_2 F + (1-F) \log_2 \left(\frac{1-F}{N-1} \right), \tag{3.3.81}$$

being Bob's fidelity $F = 1 - E_R$, with E_R the error rate, and N the dimension. However, the mutual information between Alice and Eve $I(A;E)$ depends on the used number of basis n_b.

In case that $n_b = 2$ basis are used in the protocol, then $I(A;B)$ is also given by equation (3.3.81), but trivially replacing F by the fidelity of Eve $F_E^{(2)}$. The relationship between Bob's and Eve's respective fidelities, while using two basis, is the following

$$F_E^{(2)} = \frac{F}{d} + \frac{(d-1)(1-F)}{d} + \frac{2}{d}\sqrt{(d-1)F(1-F)}, \tag{3.3.82}$$

this expression is, however, not valid if we want to use all the possible $N+1$ MUBs allowed by a cryptographic system of dimension N. In this case, the mutual information $I(A;E)$ is shown to be

$$I(A;E)^{(N+1)} = \log_2 N + (F + F_E^{(N+1)} - 1)\log_2\left(\frac{F + F_E^{(N+1)} - 1}{F}\right) + (1 - F_E^{(N+1)})\log_2\left(\frac{1 - F_E^{(N+1)}}{(N-1)F}\right), \tag{3.3.83}$$

while the relationship between Bob and Eve's fidelities also changes to

$$F_E^{(N+1)} = 1 - \frac{N-1}{N}\cdot\left(\sqrt{\frac{(N+1)F-1}{N}} - \sqrt{\frac{1-F}{N(N-1)}}\right)^2. \tag{3.3.84}$$

The secret bit rate for dimensions $N = 2, 4, 8$ is represented respect the quantum bit error rate in Figure 3.3.11. In the figure, we can observe how the rate goes down from the maximum value of secure bits transmitted, when there is no errors, to zero in a certain maximum QBER. If the QBER is bigger than this maximum, no secret key rate is distilled by the protocol. For each dimension, the rate is obtained for both cases of 2 and $N+1$ basis employed, and we can see how, the more basis used, the bigger the maximum QBER which guarantees security becomes. Consequently, the use of more basis improves the security of the protocol. We show these QBERs in Table P4.1, and they provide us with a quantitative security limit to our cryptographic system.

Table 3.4: Upper bound on QBER that guarantees security against individual attacks for different dimension and number of basis.

N	Q_2 (%)	Q_{N+1} (%)
2	14.64	15.64
4	25	26.66
8	32.33	33.44

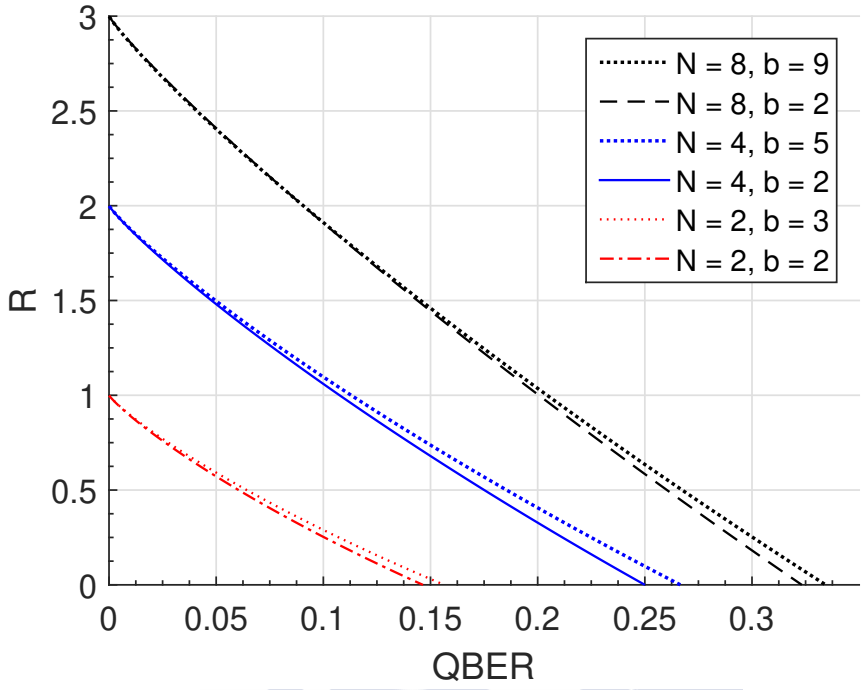


Figure 3.3.11: Bit rate in 2, 4 and 8 dimensions using 2 and $N+1$ basis.

3.3.3 Phase remapping attack

3.3.3.1 Overview

We have seen that side channel attacks like the PNS attack can be deployed over our system proposed in section 3.2. Fortunately, protocols based on decoy states can be applied to our system to solve this problem. However, certain attacks, such as Trojan attacks, can not be generally solved; and so, they have to be solved *ad hoc* or taken into account when studying the QBER of the protocol. In this way, we are going to analyse a very interesting attack that can be successfully employed against our system by Eve. This attack is the so called *phase-remapping* (PR) attack. This kind of intercept-and-resend attack was first proposed by Fung et al. in 2007 [Fung et al., 2007] and it is an attack that targets bidirectional system like the "plug and play" system, explained in section 3.1.2.1, or the Sagnac system. This bidirectional communication between Alice and Bob allows Eve to perform new attacks, not possible in unidirectional systems, by attacking the communication that goes from Bob to Alice.

In a "plug and play" system [Muller et al., 1997], Alice encodes the information by means of introducing a relative phase shift between two pulses. The PR attack is based on the fact that Alice's modulator has not an ideal square response. This opens the possibility for Eve to time-shift the unencrypted states that Bob sends to Alice, in such a way that they will arrive at Alice's phase modulator on its rising or falling edge, as shown

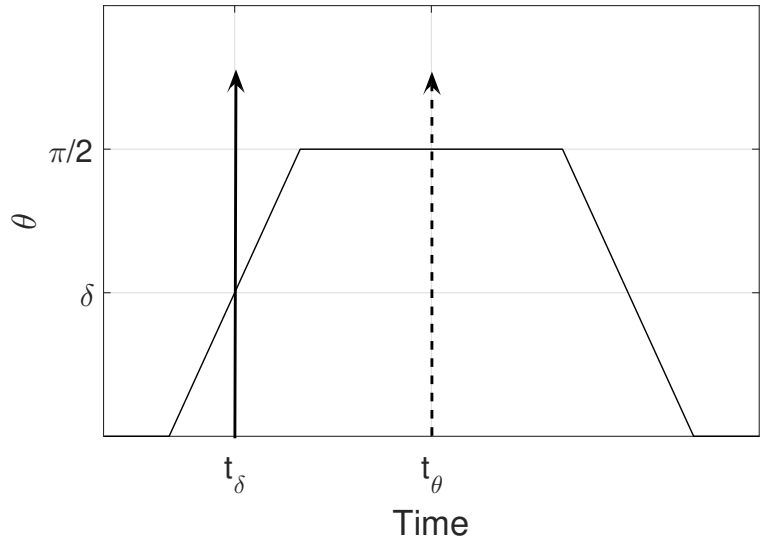


Figure 3.3.12: Time response of the phase modulator. The original pulse is time-shifted so it reaches the modulator at time t_δ instead of time t_θ.

in Figure 3.3.12. Therefore, if Alice introduces phases $\theta = \left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$ to code her four states, by controlling the amount of time shift, Eve can re-map the encoded information as $\theta = \{0, \delta, 2\delta, 3\delta\}$, where $\delta \in \left[0, \frac{\pi}{2}\right]$. This way, the actual state that Alice is sending, without her knowledge, is

$$|\tilde{\varphi}_k\rangle = \cos\left(\frac{k\delta}{2}\right)|0\rangle + \sin\left(\frac{k\delta}{2}\right)|1\rangle\,, \tag{3.3.85}$$

where $k = 0, 1, 2, 3$ are the indices that represents the four qubits $|\varphi\rangle = |0\rangle$, $(|0\rangle + |1\rangle)/\sqrt{2}$, $|1\rangle$ and $(|0\rangle - |1\rangle)/\sqrt{2}$ respectively.

After implementing the phase-remapping of the states sent by Bob to Alice, Eve intercepts the modified ones (3.3.85), that Alice sends back to Bob, and measures them. According to the qubit measured, Eve sends the corresponding unmodified qubit $|\varphi\rangle$ to Bob through an ideal channel. We are assuming that Eve has an ideal system to be unaffected by the perturbations and their compensation.

In [Fung et al., 2007], Fung determine the way to obtain the QBER while working with the two dimensional qubits (3.3.85). Eve performs a general positive-operator valued measure (POVM) that consists of five $\{M_{vac}, M_k : k = 0, 1, 2, 3\}$, where $M_{vac} + \sum_{i=0}^{3} M_i = \mathbb{I}$. When Eve gets a measure with M_k, she sends the corresponding state $|\varphi_k\rangle$ to Bob. Evidently, whenever she measures M_{vac} she would send a vacuum state. So, three cases need to be taken into account to obtain the QBER. First, if Alice sent the state $|\tilde{\varphi}_k\rangle$ when Eve measured M_k, then the QBER is 0, as Bob is always going to measure the right qubit when using the right basis. In the other way, if Alice was actually sending the orthogonal state to $|\tilde{\varphi}_k\rangle$, the QBER is 1, as Bob is always getting the wrong qubit.

Finally, in the case that Alice sent any of the other two possible states, this is, the qubits of the other basis to the qubit measured and resent by Eve, the QBER is $\frac{1}{2}$; as Bob has a 50% of chance of measuring the right qubit when using the same basis than Alice. Note that, to obtain the QBER, only the cases where Alice and Bob employ the same base is important. In this way, for example, in case that Eve is getting a measure with M_0 the QBER is the sum of the four cases normalized

$$\frac{1}{4}\left[\frac{1}{2}\mathrm{Tr}\left(M_0\left|\tilde{\varphi}_1\right\rangle\left\langle\tilde{\varphi}_1\right|\right)+\mathrm{Tr}\left(M_0\left|\tilde{\varphi}_2\right\rangle\left\langle\tilde{\varphi}_2\right|\right)+\frac{1}{2}\mathrm{Tr}\left(M_0\left|\tilde{\varphi}_3\right\rangle\left\langle\tilde{\varphi}_3\right|\right)\right], \tag{3.3.86}$$

where $\mathrm{Tr}\left(M_0\left|\tilde{\varphi}_k\right\rangle\left\langle\tilde{\varphi}_k\right|\right)$ is the probability of measuring state $\left|\tilde{\varphi}_k\right\rangle$ with the POVM operator M_0. Therefore, the total QBER is obtained by summing all the QBERs for each M_k and normalizing it with the probability of Eve causing clicks on Bob's detectors. Thus

$$\mathrm{QBER}=\frac{\sum_{s=0}^{3}\mathrm{Tr}(M_iL_i)}{\sum_{i=0}^{3}\mathrm{Tr}(M_iB_i)} \tag{3.3.87}$$

where

$$L_i=\frac{1}{2}\left|\tilde{\varphi}_{1+i}\right\rangle\left\langle\tilde{\varphi}_{1+i}\right|+\left|\tilde{\varphi}_{2+i}\right\rangle\left\langle\tilde{\varphi}_{2+i}\right|+\frac{1}{2}\left|\tilde{\varphi}_{3+i}\right\rangle\left\langle\tilde{\varphi}_{3+i}\right| \tag{3.3.88}$$

$$B=\sum_{i=0}^{3}\left|\tilde{\varphi}_i\right\rangle\left\langle\tilde{\varphi}_i\right| \tag{3.3.89}$$

3.3.3.2 Application to our four dimensional system

Now, we are going to study the influence of this attack on our proposed four-dimensional system [Balado Souto et al., 2019] and, therefore, generalize the results of Fung et al. [Fung et al., 2007]. First of all, by carefully observing the sixteen possible states belonging to the MUBs in four dimensions shown in (2.4.147) (Table P3.1 from section P3), it becomes clear that they are determined by only two phases. For example, we can take as the defining phases θ_{XV} and θ_{YH}, which take values $\theta_{XV},\theta_{YH}=0,\pi/2,\pi,3\pi/2$. Meanwhile, the third phase θ_{YV} is clearly fixed for each pair θ_{XV},θ_{YH} and their values take values according to the used basis. For basis $\bigotimes\oslash$ and $\bigodot\ominus$, $\theta_{YV}=\theta_{XV}+\theta_{YH}$, while for basis $\bigodot\ominus$ and $\bigoplus\bigcirc$, it is given by $\theta_{YV}=\theta_{XV}+\theta_{YH}+\pi$. In sum, θ_{YV} can be expressed as $\theta_{YV}=3\left(\theta_{XV}+\theta_{YH}\right) \mod 2\pi$.

3.3.3.2.1 QBER in our system

As explained before, in the PR attack Eve modifies the applied phase by shifting the original states sent by Bob. In our case [Balado Souto et al., 2019] (section P3), states (P3.6) make two round trips in order to achieve phase compensation. For simplicity, we assume that Alice only encrypts the information during the second loop. This way, the first trip only is only employed in the phase compensation and does not compromise

the system security with respect to the original plug and play system. However, as the dimension is bigger and each base state arrives to Alice's modulator delayed, Eve can re-map each of the phases θ_{GS} from $\{0, \pi/2, \pi, 3\pi/2\}$ to $\theta_{GS} = \{0, \delta_{GS}, 2\delta_{GS}, 3\delta_{GS}\}$. As $t_A < \Delta t$, there is no possibility of an overlapping between states. Of course, if she wants to obtain information while measuring the modified state, she can only apply two different δ_{GS} and apply the third one as explained. We are going to assume that Eve makes the same time-shift in the different modes, and thus, introduces the same δ. Apart from being easier for Eve, this is a reasonable strategy as she is going to obtain better results for lower δs, as we are going to see.

In consequence, the phase shifts actually introduced by Alice in state (P3.2) are $\theta_i = k_i\delta$, where $k_i = \{0, 1, 2, 3\}$, with $i = 0, 1, 2, 3$ referring to modes $GS = XH, XV, YH, YV$ respectively, and $k_3 = 3\,(k_1 + k_2) \mod 4$. So, state (3.2.49) is modified as

$$|\tilde{\psi}_{bs}\rangle = |\tilde{\psi}_{k_1k_2}\rangle = \frac{1}{2}\left(|XH\rangle + e^{ik_1\delta}\,|XV\rangle + e^{ik_2\delta}\,|YH\rangle + e^{ik_3\delta}\,|YV\rangle\right). \tag{3.3.90}$$

Written in the ququart basis, state (3.3.90) becomes

$$\begin{aligned} |\tilde{\psi}_{bs}\rangle &= |\tilde{\psi}_{k_1k_2}\rangle \\ &= \frac{1}{4}\left[\left(1 + e^{ik_1\delta} + e^{ik_2\delta} + e^{ik_3\delta}\right)|0\rangle + \left(1 - e^{ik_1\delta} + e^{ik_2\delta} - e^{ik_3\delta}\right)|1\rangle\right. \\ &\quad \left. + \left(1 + e^{ik_1\delta} - e^{ik_2\delta} - e^{ik_3\delta}\right)|2\rangle + \left(1 - e^{ik_1\delta} - e^{ik_2\delta} + e^{ik_3\delta}\right)|3\rangle\,,\right] \end{aligned} \tag{3.3.91}$$

For simplicity, we have renamed state (3.3.90) as $|\tilde{\psi}_{bs}\rangle$, where indices $b, s = 0, 1, 2, 3$ refer to base and state respectively. These indices correspond in an orderly manner, to the MUBs and states shown in (2.4.147), as written in Table 3.5. Trivially, for $\delta = \pi/2$, the original states are recovered, and we denote them as $|\psi_{bs}\rangle$.

Table 3.5: Quantum states represented in notations b, s and k_1, k_2

b	0				1				2				3			
s	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
k_1	0	2	0	2	1	3	1	3	0	2	0	2	1	3	1	3
k_2	0	0	2	2	1	1	3	3	1	1	3	3	0	0	2	2
k_3	0	2	2	0	2	0	0	2	3	1	1	3	3	1	1	3

The analysis of the influence of the attack is the same as before but generalizing it to four dimensions. So, Eve performs a POVM consisting of seventeen elements now $\{M_{vac}, M_{bs} : b, s = 0, 1, 2, 3\}$ in the modified states coded by Alice $|\tilde{\psi}_{bs}\rangle$, and sends to Bob the state $|\psi_{b_is_i}\rangle$ that corresponds to her measurement $M_{b_is_i}$. The probability of getting a measure with $M_{b_1s_1}$ when Alice sends an state $|\tilde{\psi}_{b_2s_2}\rangle$ is given by $\mathrm{Tr}(M_{b_1s_1}\,|\tilde{\psi}_{b_2s_2}\rangle\,\langle\tilde{\psi}_{b_2s_2}|)$. Just like before, the QBER is calculated by taking into account the three different possibilities happening when Eve measures $M_{b_1s_1}$ and sends the corresponding state $|\psi_{b_1s_1}\rangle$ to Bob:

- If Alice actually sent $|\tilde{\psi}_{b_1 s_1}\rangle$, no error is committed. QBER= 0
- If Alice sent a different state of the same basis $|\tilde{\psi}_{b_1 s_2}\rangle$ ($s_2 \neq s_1$), Bob always gets an error. QBER= 1
- If Alice sent a state of a different basis, there's a 75% chance of getting an error. QBER= 3/4

The total QBER (3.3.87) for the four dimensional case becomes

$$\text{QBER} = \frac{\sum_{b=0}^{n_b-1}\sum_{s=0}^{3}\text{Tr}(M_{bs}L_{bs})}{\sum_{b=0}^{n_b-1}\sum_{s=0}^{3}\text{Tr}(M_{bs}B)} \tag{3.3.92}$$

where n_b is the number of basis used and

$$L_{bs} = \sum_{\substack{j=0\\ j\neq s}}^{3} |\tilde{\psi}_{bj}\rangle\langle\tilde{\psi}_{bj}| + \frac{3}{4}\sum_{\substack{i=0\\ i\neq b}}^{n_b-1}\sum_{j=0}^{3} |\tilde{\psi}_{ij}\rangle\langle\tilde{\psi}_{ij}| \tag{3.3.93}$$

$$B = \sum_{i=0}^{n_b-1}\sum_{j=0}^{3} |\tilde{\psi}_{ij}\rangle\langle\tilde{\psi}_{ij}| \tag{3.3.94}$$

3.3.3.2.2 Minimization of the QBER

The QBER depends on the set of POVM $\{M_{vac}, M_{bs}\}$ employed by Eve to make her measures. However, it is possible to obtain a particular a lower bound for the QBER by studying the minimum possible value that the latter can take for a general POVM, as we are going to show.

The QBER expression (3.3.92) can be written as

$$\text{QBER} = \frac{\sum_{b=1}^{n_b}\sum_{s=1}^{N=4}\sum_{j=1}^{N=4}\langle j_z|W_{bs}L_{bs}W_{bs}^{\dagger}|j_z\rangle}{\sum_{b=1}^{n_b}\sum_{s=1}^{N=4}\sum_{j=1}^{N=4}\langle j_z|W_i B_i W_i^{\dagger}|j_z\rangle} \tag{3.3.95}$$

where $W_{bs}^{\dagger}W_{bs} \equiv M_{bs}$ are the POVM elements and $|j_z\rangle$ are the qubit basis. This is a ratio of sums, which is not the same as a sum of ratios like

$$\sum_{b=1}^{n_b}\sum_{s=1}^{N}\sum_{j=1}^{m}\frac{\langle j_z|W_{bs}L_{bs}W_{bs}^{\dagger}|j_z\rangle}{\langle j_z|W_{bs}B_{bs}W_{bs}^{\dagger}|j_z\rangle} \neq \text{QBER}. \tag{3.3.96}$$

Nonetheless, it can be shown that given two ratios $\frac{a_1}{a_2}$ and $\frac{b_1}{b_2}$, the following claim is true

$$\text{If} \quad \frac{a_1}{a_2} \leq \frac{b_1}{b_2} \quad \Rightarrow \quad \frac{a_1}{a_2} \leq \frac{a_1+b_1}{a_2+b_2} \tag{3.3.97}$$

In consequence, considering the claim (3.3.97) into expression (3.3.95), we can obtain a minimum bound to the QBER

$$\text{QBER} \geq \min \left\{ \frac{\langle j_z | W_{bs} L_{bs} W_{bs}^{\dagger} | j_z \rangle}{\langle j_z | W_{bs} B_{bs} W_{bs}^{\dagger} | j_z \rangle} \right\} \tag{3.3.98}$$

Making a state redefinition as $\langle c_{jbs}| = \langle j_z| \, W_{bs} B_{bs}^{1/2}$, the previous equation becomes

$$\text{QBER} \geq \min \left\{ \frac{\langle c_{ij} | B_{bs}^{-1/2} L_{bs} B_{bs}^{-1/2} | c_{ij} \rangle}{\langle c_{ij} | c_{ij} \rangle} \right\} \tag{3.3.99}$$

This equation is trivially minimized for the eigenvector $|c_{ij}^{eigen}\rangle$ corresponding to the minimum eigenvalue of the matrix $B_{bs}^{-1/2} L_{bs} B_{bs}^{-1/2}$. Therefore, the lower bound value of the QBER is the minimum eigenvalue of all matrices $B_{bs}^{-1/2} L_{bs} B_{bs}^{-1/2}$.

3.3.3.2.3 Minimization of QBER for the 4-dimensional case

Using all 16 modified states (3.3.90), with the values of k_1, k_2 shown in Table (3.5), we can calculate the same number of matrices L_{bs} and B_{bs} according to equations (3.3.94) and (3.3.93). Then, it is possible to obtain matrices $B_{bs}^{-1/2} L_{bs} B_{bs}^{-1/2}$ and calculate all its eigenvalues. The minimum eigenvalue is going to be the minimum possible value of the QBER. This must to be done for different values of δ, and so, the minimum possible QBER in function of δ is obtained.

Let's make the example of $\delta = \pi/4$. With our delta, we can calculate numerically the 16 states (3.3.90) and using then, the 16 matrices L_{bs} and the matrix B_{bs}. So, for example, if we calculate matrix $B^{-1/2} L_{11} B^{-1/2}$, we obtain

$$B^{-1/2} L_{11} B^{-1/2} = \begin{pmatrix} 0.4932 & -0.02334 & -0.02334 & -0.02334 \\ -0.02334 & 0.7971 & -0.007462 & -0.007462 \\ -0.02334 & -0.007462 & 0.7971 & -0.007462 \\ -0.02334 & -0.007462 & -0.007462 & 0.7971 \end{pmatrix} \tag{3.3.100}$$

Calculating the eigenvalues of this matrix, we have

$$eigen\left(B^{-1/2} L_{11} B^{-1/2}\right) = \{0.4865, 0.7888, 0.8045, 0.8045\}.$$

The minimum eigenvalue is 0.4865. Now, doing the same in the other 15 cases we have the following Table 3.6 of eigenvalues.

We see that the case $b = 1, s = 1$ still has the minimum eigenvalue. In consequence, for $\delta = \pi/4$

$$\text{QBER} \geq 0.4865 \tag{3.3.101}$$

Doing the same thing for different δ values, we can obtain the QBER in function of the δ used by Alice. The results are shown in Figure 3.3.13. The lower curve corresponds to

Table 3.6: Minimum eigenvalues of the different quantum states of 4-dimensional MUBs.

	s			
b	1	2	3	4
1	0.4865	0.6505	0.5405	0.5405
2	0.5963	0.5405	0.5405	0.6505
3	0.5963	0.5405	0.6505	0.5405
4	0.5963	0.5420	0.5420	0.5420

the 2-dimensional problem, where we can see that the QBER can be minimized from 25%, in the classical attack ($\delta = \pi/2$), to 15.5%, when $\delta \to 0$. The other curves correspond to our 4 dimensional case for a different number of basis n_b used. From top to bottom, in Figure 3.3.13, results for $n = 4, 3, 2$ basis are shown. If $\delta = \pi/2$, we obtain the expected results from a classical intercept-and-resend attack for each n, that is, QBER $= \{\frac{9}{16}, \frac{1}{2}, \frac{3}{8}\}$. With the PR attack, the QBER values can be minimized to 46.7%, 40.4% and 29.7%, respectively. Note that in all cases, the QBER is significantly larger than for the 2-dimensional case. It is also important to remark that the minimum QBER obtained is still higher than 25%. Recall that this value was the limit QBER at which it was possible to obtain a secret bit rate under a cloning machine attack.

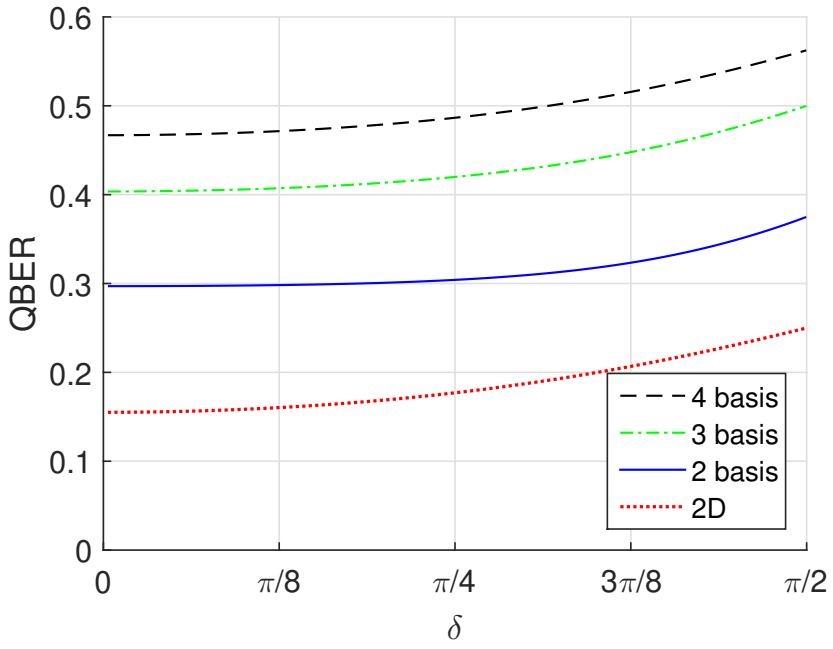


Figure 3.3.13: QBER achieved in a PR attack for different δ in dimension $N = 4$. From top to bottom, curves for 4, 3, 2 basis used. The lower curve correspond to the PR attack in two dimensions.

3.3.3.3 Generalization to more dimensions

3.3.3.3.1 General case

We are going to generalize the results of the PR attack [Fung et al., 2007] for a general high dimensional autocompensation system of dimension N. So, let us suppose that we have a multi-round-trip system, as explained in subsection 3.2.2, where Alice encrypts the information by phase shifts θ_i phases of different modes, generating the state (3.2.18), which we can write in a qudit form as

$$|\psi_{bs}\rangle \approx N^{-\frac{1}{2}}\{e^{i\theta_1}|1_1\rangle + e^{i\theta_2}|1_2\rangle + ... + e^{i\theta_N}|1_N\rangle\}. \tag{3.3.102}$$

where b represents the base of the state and s the qudit value of the state ($b, s = 0, 1, ..., N$). As it has been explained, Eve time-shifts the light pulses arriving to Alice before the encryption to modify the applied phase $\{\theta_i\}_{i=1}^{N}$ changing its values from $\{0, \pi/2, \pi, 3\pi/2\}$ to $\{0, \delta, 2\delta, 3\delta\}$. Consequently, the actual phases that Alice is introducing are $\theta_i = k_i\delta$. Therefore, Alice's coded state (3.3.102) is modified as follows

$$|\tilde{\psi}_{bs}\rangle \approx N^{-\frac{1}{2}}\{e^{ik_1\delta}|1_1\rangle + e^{ik_2\delta}|1_2\rangle + ... + e^{ik_N\delta}|1_N\rangle\}. \tag{3.3.103}$$

As in the previous cases, Eve intercepts states (3.3.103) and performs a POVM consisting of $n_b \cdot N + 1$ elements $\{M_{vac}, M_{bs} : b = 1...n_b, s = 1 \dots N\}$, where n_b is the number of used basis and N the dimension of the states. If Alice sends a state $|\tilde{\psi}_{b_0 s_0}\rangle$, the probability of Eve to measure $M_{b_1 s_1}$ is given by $\mathrm{Tr}(M_{b_1 s_1} |\tilde{\psi}_{b_0 s_0}\rangle \langle\tilde{\psi}_{b_0 s_0}|)$. Whenever Eve gets a measurement in $M_{b_1 s_1}$, she sends the corresponding unmodified state $|\psi_{b_1 s_1}\rangle$ to Bob. The QBER of the three possible situations when Bob measures this state and compares his results with Alice is

- If Alice actually sent $|\tilde{\psi}_{b_1 s_1}\rangle$, no error is committed.

  $b_1 = b_0$, $s_1 = s_0 \Rightarrow$ QBER$= 0$

- If Alice sent a different state of the same basis $|\tilde{\psi}_{b_1 s_2}\rangle$ ($s_2 \neq s_1$), Bob always gets an error.

  $b_1 = b_0$, $s_1 \neq s_0 \Rightarrow$ QBER$= 1$

- If Alice sent a state of a different basis, only in $\frac{1}{N}$ of the cases Bob will obtain the correct measure.

  $b_1 \neq b_0 \Rightarrow$ QBER$= \frac{N-1}{N}$

$$\mathrm{QBER} = \frac{\sum_{b=1}^{n_b}\sum_{s=1}^{N}\mathrm{Tr}(M_{bs}L_{bs})}{\sum_{b=1}^{n_b}\sum_{s=1}^{N}\mathrm{Tr}(M_{bs}B)}, \tag{3.3.104}$$

where n_b is the number of basis used, N is the dimension and

$$L_{bs} = \sum_{\substack{j=1 \\ j\neq s}}^{N} |\tilde{\psi}_{bj}\rangle \langle\tilde{\psi}_{bj}| + \frac{N-1}{N} \sum_{\substack{i=1 \\ i\neq b}}^{n_b} \sum_{j=1}^{N} |\tilde{\psi}_{ij}\rangle \langle\tilde{\psi}_{ij}|, \tag{3.3.105}$$

$$B = \sum_{i=1}^{n_b} \sum_{j=1}^{N} |\tilde{\psi}_{ij}\rangle \langle\tilde{\psi}_{ij}|. \tag{3.3.106}$$

3.3.3.3.2 Case $N = 2^m$

Finally, we are going to minimize the QBER for a general set $\{M_{vac}, M_{bs} : b = 1...n_b, s = 0 \dots N-1\}$ for dimension $N = 2^m$. To do this, we are going to use the same MUBs generated in [Tselniker et al., 2009]. Following the same procedure as before, we can calculate matrices L_{bs} and B_{bs} from equations (3.3.105) and (3.3.106) and obtain the lower bounds of the QBER with equation (3.3.99). The results are shown in Figure 3.3.14, where the QBER is represented for dimensions $N = 2, 4, 8$ using both $n_b = 2$ and $n_b = N$ basis in each case. We observe that, in every curve, the maximum QBER is obtained when $\delta = \pi/2$, this means, when there is no PR attack. We observe, as well, that Eve can reduce the QBER generated by her eavesdropping when the modified phase δ tends to zero. When $\delta = 0$ we have a singularity, because Alice always sends the same modified state and so, Eve acquires no information. The maximum and minimum QBER values obtained are shown in Table 3.7

By looking at Table 3.7, we see that we obtain the expected results from a classical intercept-and-resend attack to the BB84 protocol for dimension N and n_b basis used, which is $\frac{N-1}{N}\frac{n_b-1}{n_b}$. Regarding the values for $\delta \to 0$, we can see that the PR attack allows to reduce the QBER in a significant way. However, comparing these values with those shown in Table P4.1, this is, the maximum allowed values of the QBER for a quantum cloning attack, we can see that the latter are a bit lower than the values of the PR attack. In consequence, the PR attack does not achieve better results in a round-trip system than an optimal cloning attack in a one way system. Thus, the loop system does not compromise the security of the protocol respect to the one way system.

Table 3.7: Maximum and minimum QBER values under PR attack

N	n_b	$\delta \to 0$ (%)	$\delta = \pi/2$ (%)
2	2	15.5	25
4	2	29.7	37.5
8	2	38.8	43.75
4	4	46.6	56.25
8	8	70.4	76.56

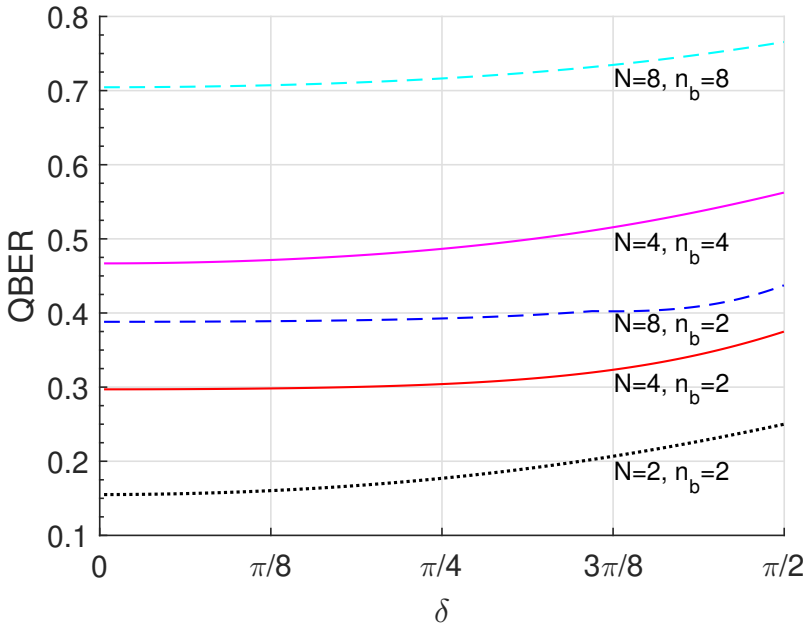


Figure 3.3.14: QBER achieved in a PR attack for different δ in different dimensions N and with n_b basis used.

3.3.3.4 Detector efficiency mismatch attack

The PR attack is an attack that exploits weakness in Alice's subsystem, in this case, the response of the electro-optic modulator. Another kind of time shift attack called the *fake state* (FS) attack, valid for one way systems, was proposed by Makarov et al. in 2006 [Makarov et al., 2006, Makarov and Skaar, 2007]. This attack aims instead Bob's subsystem, more specifically, the aim are Bob's detectors. Makarov's attack takes advantage of the efficiency mismatch of the single photon detectors (SPDs) used in the protocol. We are going to explain the basis of this attack and then combine it with the PR attack.

3.3.3.4.1 Fake states attack

Be η_0 and η_1 the efficiencies of two detectors (SPD_0 and SPD_1) used to measure qubits $|0\rangle$ and $|1\rangle$ respectively. As shown in Figure 3.3.15, their sensitive curves may not match in their operation time. In a safe situation, the encrypted state ψ is timed to arrive to Bob's detectors when they are working at time T, which means that $\eta_0(T) \approx \eta_1(T) \approx \eta_{max}$. However, Eve can interfere in the system by intercepting state ψ and resending a fake state $\bar{\psi}$ shifted in time to times t_0 or t_1 of Bob's detector efficiency curves, with the intention of increasing (and decreasing) the probability of Bob getting a click for bits 0 or 1. Therefore, Eve can basically set the bit value obtained by Bob. In the ideal case, when the mismatch is total, she literally controls Bob's measured bit.

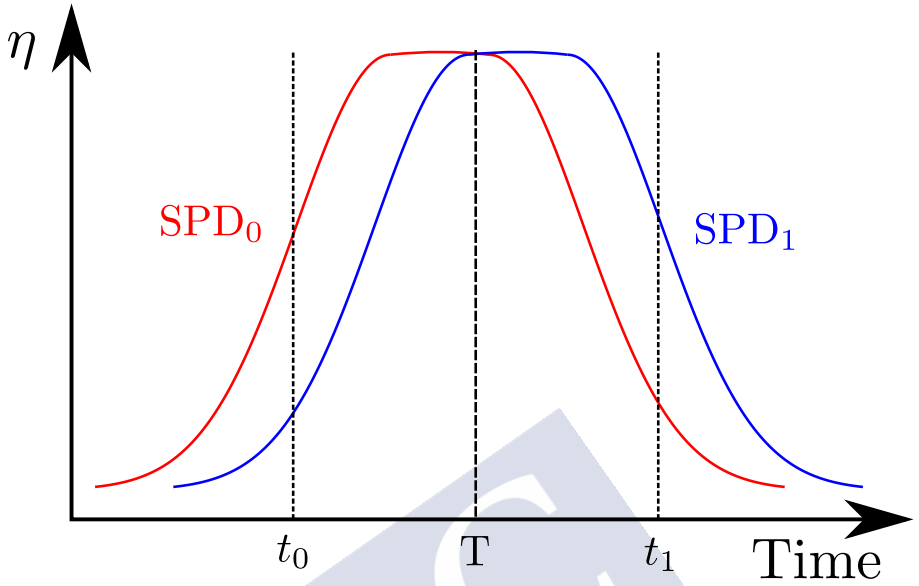


Figure 3.3.15: Detectors efficiency mismatch between two SPDs.

Table 3.8: Probabilities of Bob's detection for different cases. *det* refers to the state measured by Eve, while *str* refers to the state sent by her. The top three rows represent Makarov's strategy of sending the opposite bit in the opposed basis. In the lower three, Eve sends the same measured state.

Alice	Eve (det)	Eve (str)	Bob	Probabilities
$\|0_z\rangle$	$\|0_z\rangle$	$\|1_x\rangle$	0	$\frac{1}{2}\eta_0(t_0)$
			1	$\frac{1}{2}\eta_1(t_0)$
$\|0_z\rangle$	$\|0_x\rangle$	$\|1_z\rangle$	0	0
			1	$\eta_1(t_0)$
$\|0_z\rangle$	$\|1_x\rangle$	$\|0_z\rangle$	0	$\eta_0(t_1)$
			1	0
$\|0_z\rangle$	$\|0_z\rangle$	$\|0_z\rangle$	0	$\eta_0(t_0)$
			1	0
$\|0_z\rangle$	$\|0_x\rangle$	$\|0_x\rangle$	0	$\frac{1}{2}\eta_0(t_0)$
			1	$\frac{1}{2}\eta_1(t_0)$
$\|0_z\rangle$	$\|1_x\rangle$	$\|1_x\rangle$	0	$\frac{1}{2}\eta_0(t_1)$
			1	$\frac{1}{2}\eta_1(t_1)$

Makarov's FS strategy is that, whenever Eve detects a certain qubit, she resends to Bob the opposed qubit of the opposed basis. In this way, if Eve measures qubit $|0_z\rangle$, she sends the state $|1_x\rangle$, being x and z both qubit basis. In Table 3.8, we show the probabilities of Bob detecting bits 0 and 1 when Alice sends state $|0_z\rangle$ in function of Eve's measurement and chosen strategy (Makarov's or sending the measured state). We can see that Makarov strategy comes from the fact that it minimizes the error probability ($\eta_1(t_0)/4$). However, this does not necessarily minimize the QBER as it decreases the success probability ($(\eta_0(t_0)+\eta_0(t_1))/4$), as well.

In both cases, the probability that Alice's state $|0_z\rangle$ gets a click on Bob's detectors is the sum of all the probabilities (with the first row being double) divided by the four cases

$$P_{\neq}(arrive|0_z) = \frac{1}{4}\left(\eta_0(t_0)+\eta_0(t_1)+2\eta_1(t_0)\right) \tag{3.3.107}$$

$$P_{=}(arrive|0_z) = \frac{1}{8}\left(5\eta_0(t_0)+\eta_0(t_1)+\eta_1(t_0)+\eta_1(t_1)\right) \tag{3.3.108}$$

By symmetry, the total probability of Alice (Eve) getting clicks on Bob is given by

$$P_{\neq}(arrive) = \frac{1}{8}\left(\eta_0(t_0)+3\eta_0(t_1)+3\eta_1(t_0)+\eta_1(t_1)\right) \tag{3.3.109}$$

$$P_{=}(arrive) = \frac{1}{8}\left(3\eta_0(t_0)+\eta_0(t_1)+\eta_1(t_0)+3\eta_1(t_1)\right) \tag{3.3.110}$$

In the same way, the error probabilities are

$$P_{\neq}(error) = \frac{1}{4}\left(\eta_0(t_0)+\eta_1(t_1)\right) \tag{3.3.111}$$

$$P_{=}(error) = \frac{1}{8}\left(\eta_0(t_0)+\eta_0(t_1)+\eta_1(t_0)+\eta_1(t_1)\right) \tag{3.3.112}$$

As a consequence, the QBERs of bot methods are given by

$$\mathrm{QBER}_{\neq} = \frac{P_{\neq}(arrive)}{P_{\neq}(error)} = \frac{2\eta_0(t_0)+2\eta_1(t_1)}{3\eta_0(t_0)+\eta_0(t_1)+\eta_1(t_0)+3\eta_1(t_1)} \tag{3.3.113}$$

$$\mathrm{QBER}_{=} = \frac{P_{=}(arrive)}{P_{=}(error)} = \frac{\eta_0(t_0)+\eta_0(t_1)+\eta_1(t_0)+\eta_1(t_1)}{3\eta_0(t_0)+\eta_0(t_1)+\eta_1(t_0)+3\eta_1(t_1)} \tag{3.3.114}$$

3.3.3.4.2 Generalization for more dimensions

If we go up to four dimensions, like the system mentioned on subsection 3.2.5 and described in the published work annexed as subsection P3, we are going to have at least four detectors. It is important to note that in our system, eight detectors are used and, in general, $n_b \cdot N$ detectors can be used. For simplicity, and without much loss of generality, it can be assumed $\eta_{s_b}(t) = \eta_{s_{b'}}(t)$. Let us suppose that we make use of a system of dimension N that employs N detectors. Evidently, now we have a total of N detector sensibility curves $\{\eta_i(t)\}_{i=0}^{N}$). This greatly reduces the efficiency of the attack, because the efficiencies $\{\eta_i(t)\}_{i=0}^{N}$) are overlapped between them. As a consequence, unlike in the two dimensional case, Eve can not make maximum $\eta_i(t)$ for bit i in all cases. Trivially, the most interesting cases are going to be those that are similar to the two dimensional case.

In Figure 3.3.16, we show the case for four dimensions, as in our system. We can see that for times t_1 and t_2, η_1 and η_2 are maximized. However, η_0 and η_3 are respectively maximized as well, with $\eta_0(t_1) > \eta_1(t_1)$ and $\eta_2(t_2) < \eta_3(t_2)$. As a consequence, times t_1 and t_2 are not going to give Eve much advantage. At the same time, Eve is going to obtain better results in Alice and Bob's QBER for the limit cases where the two dimensional case is obtained, like $\eta_0 = \eta_1$, $\eta_2 = \eta_3$ or $\eta_1 = \eta_2 = \eta_3$.

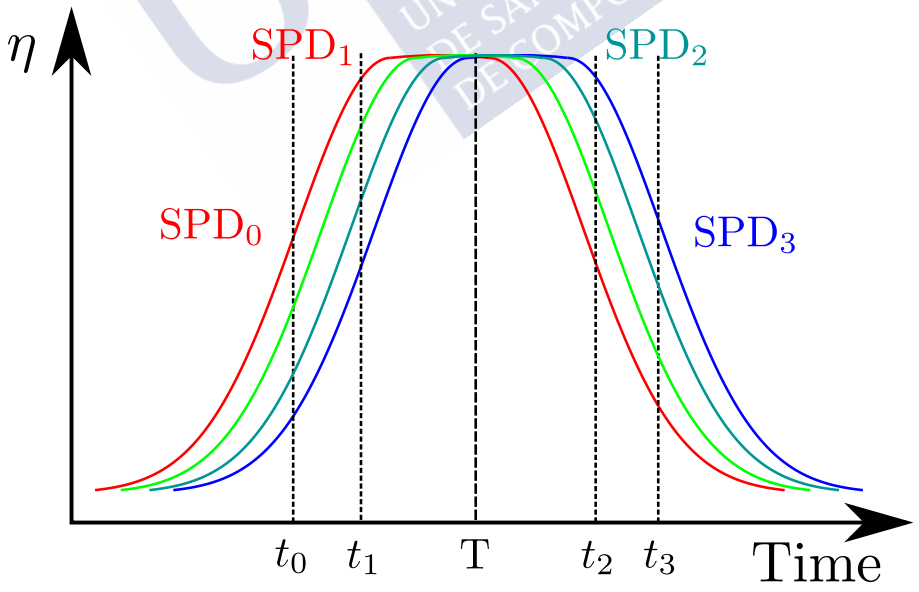


Figure 3.3.16: Detectors efficiency mismatch between four SPDs.

Table 3.9: Probabilities of Bob detection for different cases in four dimensions. Eve sends the same state that she measures.

Alice	Eve (det)	Eve (str)	Bob	Probabilities
$\|s_b\rangle$	$\|s_b\rangle$	$\|s_b\rangle$	s	$\eta_s(t_s)$
$\|s_b\rangle$	$\|i_j\rangle$	$\|i_j\rangle$	0	$\frac{1}{4}\eta_0(t_i)$
			1	$\frac{1}{4}\eta_1(t_i)$
			2	$\frac{1}{4}\eta_1(t_i)$
			3	$\frac{1}{4}\eta_3(t_i)$

Let us generalize the QBER of this attack for more dimensions, In Table 3.9 we show Bob measuring probabilities in four dimensions. The probability that Alice's state $|bs\rangle$ gets to Bob's detectors is as follows

$$P_{=}(arrive|0_z) = \frac{1}{n_b}\eta_s(t_s) + \frac{1}{n_b N}\sum_{\substack{j=0\\ j\neq b}}^{n_b-1}\sum_{i=0}^{N-1}\sum_{k=0}^{N-1}\frac{\eta_k(t_i)}{N}. \tag{3.3.115}$$

The total probability of Alice states arriving to Bob is obtained by summing over all possible states $|bs\rangle$

$$\begin{aligned} P(arrive) = \frac{1}{n_b N}\sum_{s=0}^{N-1}\sum_{b=0}^{n_b-1} P_{=}(arrive|0_z) = \\ = \frac{1}{N}\sum_{s=0}^{N-1}\eta_s(t_s) + \frac{n_b-1}{n_b}\sum_{j=0}^{n_b-1}\sum_{i=0}^{N-1}\sum_{k=0}^{N-1}\frac{\eta_k(t_i)}{N} \end{aligned} \tag{3.3.116}$$

In the same way, the error probabilities are

$$P_(error) = \frac{1}{n_b N}\sum_{s=0}^{N-1}\sum_{b=0}^{n_b-1}\left[\frac{1}{n_b N}\sum_{i=0}^{N-1}\sum_{\substack{j=0\\ j\neq b}}^{n_b-1}\sum_{\substack{k=0\\ k\neq s}}^{N-1}\frac{\eta_k(t_i)}{N}\right] = \frac{(N-1)(n_b-1)}{(n_b N)^2}\sum_{i=0}^{N-1}\sum_{\substack{j=0\\ j\neq b}}^{n_b-1}\sum_{\substack{k=0\\ k\neq s}}^{N-1}\frac{\eta_k(t_i)}{N}. \tag{3.3.117}$$

So, the QBERs of bot methods are given by the division between (3.3.116) and (3.3.117)

$$\text{QBER} = \frac{P(arrive)}{P(error)} \tag{3.3.118}$$

3.3.3.4.3 Combination of PR and FS attack

Now, we are going to employ this attack combined to the PR attack in order to explore if we can reduce the QBER in our four dimensional system. To do this we have to take into account the efficiencies η_{bs} of each ququart detector in matrices given by equations (3.3.93) and (3.3.94). The QBER is going to be minimised as it was previously explained (3.3.99).

For means of exemplification, let us suppose that in a two dimensional system Eve measures state $|\tilde{\psi}_{b=0,s=0}\rangle$ and sends Bob the corresponding state $|\psi_{b=0,s=0}\rangle$. Now, in matrix L_{00} we have to take into account the efficiencies that the wrong detector does click. In this way,

$$L_{00} = \eta_0(t_0)\,|\tilde{\psi}_{01}\rangle\,\langle\tilde{\psi}_{01}| + \frac{1}{2}\left(\eta_1(t_0)\,|\tilde{\psi}_{10}\rangle\,\langle\tilde{\psi}_{10}| + \eta_0(t_0)\,|\tilde{\psi}_{11}\rangle\,\langle\tilde{\psi}_{11}|\right) \tag{3.3.119}$$

Meanwhile, in matrix B_{00} we have to add up the probabilities that the right detector does click. Note that now, matrix B depends on the state.

$$B_{00} = \eta_0(t_0)\,|\tilde{\psi}_{00}\rangle\,\langle\tilde{\psi}_{00}| + \frac{1}{2}\left(\eta_0(t_0) + \eta_1(t_0)\right)\left(|\tilde{\psi}_{10}\rangle\,\langle\tilde{\psi}_{10}| + |\tilde{\psi}_{11}\rangle\,\langle\tilde{\psi}_{11}|\right) \tag{3.3.120}$$

Following the same idea,we can generalize this to any state and dimension generalization matrices (3.3.105) and (3.3.106). In sum, we have

$$L_{bs} = \eta_s(t_s)\sum_{\substack{j=0\\ j\neq s}}^{N}|\tilde{\psi}_{bj}\rangle\,\langle\tilde{\psi}_{bj}| + \frac{1}{4}\sum_{i=0}^{n_b}\left[\left(\sum_{j=0}^{N}\eta_j(t_s)\right)\left(\sum_{j=0}^{N}|\tilde{\psi}_{ij}\rangle\,\langle\tilde{\psi}_{ij}|\right) - \sum_{j=0}^{N}\left(\eta_j(t_s)\,|\tilde{\psi}_{ij}\rangle\,\langle\tilde{\psi}_{ij}|\right)\right] \tag{3.3.121}$$

$$B_{bs} = \eta_s(t_s)\sum_{j=0}^{N}|\tilde{\psi}_{bj}\rangle\,\langle\tilde{\psi}_{bj}| + \frac{1}{4}\sum_{i=0}^{n_b}\left[\left(\sum_{j=0}^{N}\eta_j(t_s)\right)\left(\sum_{j=0}^{N}|\tilde{\psi}_{ij}\rangle\,\langle\tilde{\psi}_{ij}|\right)\right] \tag{3.3.122}$$

Finally, employing matrices (3.3.121) and (3.3.122), QBER curves can be obtained for a detector attack combined with a PR one in the four dimensional. We show these curves in Figure 3.3.17, where we have plotted curves for $n_b = 2, 4$ basis used and compare it with the two dimensional case. The curves have been calculated for the limit case $\eta_1 = \eta_2 = \eta_3$ and with the ratio between these detectors and the fourth one being $\eta_1/\eta_0 = 0.08$. We observe that, by using both attacks, Eve can reduce the QBER as low as 15% with independence of the number of basis used. This is a clearly improvement respect to the values of 29.7% and 15.5% shown in Table 3.7, and it is also a better attack than the optimal QCM attack, 25% and 26.6% respectively as shown in Table P4.1.

In conclusion, this kind of combined attack must be taken into account when implementing this system. However, we must indicate that our assumption that the efficiencies are independent of the basis is too optimistic for Eve. In fact, with different mismatches in different basis this attack would become difficult to implement successfully.

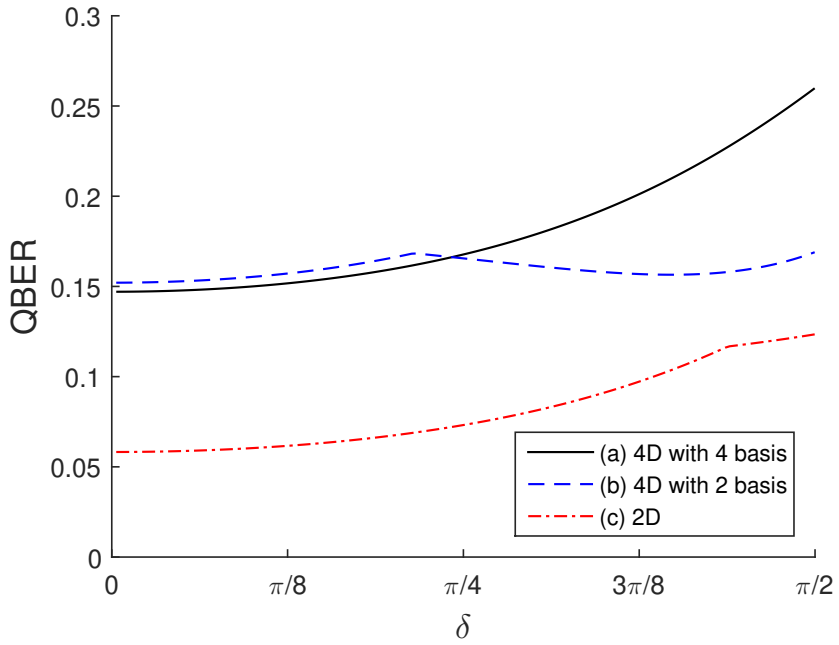


Figure 3.3.17: QBER achieved in a PR attack combined with a detector attack. The figure represents the QBER for the 4-dimensional case with 2 and 4 basis compared to the 2-dimensional case.

P3 Phase auto-compensating high-dimensional quantum cryptography in elliptical-core few-mode fibers

JOURNAL OF MODERN OPTICS
VOL. 66 NO. 9 PAGE 947-957
ISSN: 0950-0340 (PRINT), 1362-3044 (ONLINE)
doi: https://doi.org/10.1080/09500340.2019.1595198

PUBLISHED 1 APR 2019

BY DANIEL BALADO SOUTO[1] & JESÚS LIÑARES[1] & XESÚS PRIETO BLANCO

[1] UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Abstract: *High-dimensional quantum cryptography through optical fibers with several spatial modes requires an efficient quantum key distribution (QKD). However, optical modes acquire different phases and lags due to modal dispersion and random fluctuations, and a modal crosstalk appears under propagation. At present, special optical fibers for spatial multiplexing are being proposed in order to reduce notably the modal crosstalk, however, arbitrary relative phases and lags between modes are always present, which prevents getting an efficient phase encoding QKD. In this work, we take advantage of elliptical-core few-mode optical fibers presenting a very low modal crosstalk and propose an exact phase auto-compensating method by making photons travel several times the path between Alice and Bob (rounds) and by using appropriate modal inversions in each round trip. In order to make clear the proposed phase auto-compensating method, we study in detail a four-dimensional BB84 QKD case with single photon states excited in both polarization and spatial LP modes.*

P3.1 Introduction

Private-key cryptographic systems are based in the exchange of secret keys between the sender Alice and the receiver Bob. These secret keys are used to encrypt the information transmitted between Alice and Bob and, thus, can only be known to them. It is well known that quantum cryptography (QC) is based on the properties of quantum mechanics to obtain a secure quantum key distribution (QKD) by using different protocols. The seminal protocol has been the so-called BB84 one [Bennett and Brassard, 1984, Bennett et al., 1992b, Bennett, 1992], in which four states define a set of two mutually unbiased basis (MUBs) in a two-dimensional Hilbert space. Nevertheless, high-dimensional QKD (HD-QKD) based on qudit encoding is a better optimized technique to achieve efficient QKD systems and above all a larger security [Sheridan and Scarani, 2010, Mafu et al., 2013, Maslennikov et al., 2003, Islam et al., 2017]. In fact, these HD-QKD protocols exhibit higher resilience to noise [Cerf et al., 2002], which in turn means longer transmission distances [Niu et al., 2016, Cañas et al., 2017].

On the other hand, different optical techniques and systems have been proposed to implement QKD cryptography in optical fibers. In particular, since the beginning of cryptography, polarization or phase of very weak light pulses have been used since the beginning of cryptography as information carriers by most existing optical implementations of QC [Bennett et al., 1992b, Bennett, 1992, Marand and Townsend, 1995, Ma et al., 2007, Wang et al., 2016, Bussieres et al., 2006]. Polarization implements QKD only in a two dimensional Hilbert space, but the main problem with the polarization-based systems is the need to keep stable polarizations over distances of tens of kilometers of optical fiber in real telecommunications. To overcome this drawback, due to the polarization mode crosstalk, different polarization (two-dimensional) auto-compensating techniques have been proposed [Muller et al., 1997, Bethune and Risk, 2002, Bethune et al., 2002, Chen et al., 2008]. Obviously, such an optical crosstalk is a common problem in optical fibers for both polarization and spatial modes [Richardson et al., 2013], however, at present special optical fibers are being proposed for reducing modal crosstalk for space division multiplexing (SDM), as for example optical fibers maintaining polarization modes and spatial modes such as elliptical-core few-mode optical fibers (EC-FMF) [Milione et al., 2016b], multicore optical fibers [Xia et al., 2012], and so on, that is, by using a suitable design of the optical fibers. Nevertheless, phase fluctuations due to modal dispersion delay and random phase fluctuations generated by propagation can not be reduced by any special design of an optical fiber. This can become a serious drawback in high-dimensional QKD in optical fibers with several spatial (and polarization) modes [Chen et al., 2008], and therefore a phase auto-compensating method is required in order to get an efficient phase encoding QKD.

As commented, SDM has been proposed to further increase the data bandwidth due to the increase of bandwidth demands in optical fiber communications, and therefore multiplexing over new degrees of freedom is required. In fact, circular-core few-mode optical fibers (FMF) have been used to achieve transmission of up to Pb/s [Bai et al., 2012].

Likewise, spatial modes of a EC-FMF optical fiber for SDM have been also proposed and analyzed [Milione et al., 2016b, Milione et al., 2016a] because of their very low modal crosstalk between both normally degenerate spatial modes LP_{11x} and LP_{11y} and polarization modes. In fact, it has been proven that these modes do not couple even under fiber twisting/bending. This very low crosstalk is an strategic aim in SDM in order to avoid the MIMO technique [Ip et al., 2015]. Likewise, it is worthwhile to indicate that recently it has been reported that these FMF fibers present low losses [Liu et al., 2018].

Accordingly, SDM with EC-FMFs represents an unbeatable opportunity for using the corresponding high-dimensional modal space and thus to excite the optical quantum states to obtain HD-QKD implementations. Obviously, the modes of EC-FMF have different propagation constants, that is, lags between modes, due to birefringence arising from core asymmetry (ellipticity) or also due to local changes giving rise to small but accumulative changes of the modal phases. Moreover, as commented above, the corresponding relative phases and lags is a major drawback in HD-QKD using spatial modes, and they can not be minimized by any special design of an optical fiber. Therefore, we could take advantage of this low crosstalk in both polarization and spatial modes to implement HD-QKD by SDM if an auto-compensating method is found for the phase fluctuations. In particular, we will consider in detail a four-dimensional case, that is, ququarts states and four basis, although a lesser number of basis can be also used according to the practical interest. Moreover, we will propose an auto-compensating technique based on both making light travel several times the path between Alice and Bob (rounds) and choosing suitable modal inversions. For ququarts states two rounds and two appropriate modal inversions are needed, where each mode acquires the deterministic and random phases of the other three modes, as will be shown. We will use optical systems based on modal converters and Mach-Zehnder interferometers, which are usual components in spatial multiplexing [Liñares et al., 2017a]. Finally, we must stress that a similar method of phase auto-compensating with integrated optical components can be used for multicore optical fibers; preliminary results have been obtained [Balado et al., 2018]

The plan of this work is as follows: in section P3.2 we introduce the quantum states excited on optical spatial modes of a EC-FMF optical fiber and their use for implementing the BB84 protocol. In section P3.3 we present those optical elements and devices that we are going to use to manipulate such quantum states, such as mode converters, Mach-Zehnder interferometers and optical fiber delay device. Next the phase auto-compensating device is shown and explained in detail together with the Alice subsystem to generate the quantum states for QKD. In section P3.4 a quantum random detection system (projective measurements) or Bob's subsystem for the BB84 protocol is described. After the detailed presentation of our system, in section P3.5 we perform a security analysis of our system, by studying how it behaves under some specific attacks to our system. Finally, in Section P3.6 conclusions are presented.

P3.2 High-dimensional BB84 Protocol in EC-FMF fibers

It is well-known that the BB84 protocol requires working with K mutually unbiased bases (MUBs) $\{|\varphi\rangle_{1(k)},...,|\varphi\rangle_{d(k)}\}$ with $k=1,...,K$ and $2\leq K\leq d$ (d is the dimension of the Hilbert space), which means that the inner product between any basis states must fulfil

$$|\langle\varphi_{i(k)}|\varphi_{j(k')}\rangle|^2=\begin{cases}\frac{1}{d} & \text{if} \quad k\neq k' \quad \forall\, i,j=1,...,d\\ \delta_{ij} & \text{if} \quad k=k' \quad \forall\, i,j=1,...,d\end{cases} \tag{P3.1}$$

Table P3.1: Sixteen quantum states of four MUBs used in this work.

Basis	θ_{XH}	θ_{XV}	θ_{YH}	θ_{YV}	Final state
⊗ ⊘	0	0	0	0	$\|X'H'\rangle$
	0	π	0	π	-$\|X'V'\rangle$
	0	0	π	π	-$\|Y'H'\rangle$
	0	π	π	0	$\|Y'V'\rangle$
⊙ ○	0	$\pi/2$	$\pi/2$	π	$\|+L\rangle$
	0	$3\pi/2$	$\pi/2$	0	$\|+R\rangle$
	0	$\pi/2$	$3\pi/2$	0	$\|-L\rangle$
	0	$3\pi/2$	$3\pi/2$	π	$\|-R\rangle$
⊙ ⊖	0	0	$\pi/2$	$3\pi/2$	$\|+H\rangle+\|-V\rangle$
	0	π	$\pi/2$	$\pi/2$	$\|+H\rangle-\|-V\rangle$
	0	0	$3\pi/2$	$\pi/2$	$\|-H\rangle+\|+V\rangle$
	0	π	$3\pi/2$	$3\pi/2$	$\|-H\rangle-\|+V\rangle$
⊕ ○	0	$\pi/2$	0	$3\pi/2$	$\|XL\rangle+\|YR\rangle$
	0	$3\pi/2$	0	$\pi/2$	$\|XR\rangle+\|YL\rangle$
	0	$\pi/2$	π	$\pi/2$	$\|XL\rangle-\|YR\rangle$
	0	$3\pi/2$	π	$3\pi/2$	$\|XR\rangle-\|YL\rangle$

Although the study can be made with an arbitrary number of modes, we propose, for sake of simplicity, the quantum superposition of four LP modes to implement the quantum encryption protocol BB84 in four dimensions by using, for instance, a EC-FMF or a MCF with an elliptical central core supporting a few modes. Likewise, we choose four basis, although three or two basis can be also used. Let us consider $\mathrm{LP}_{11\alpha}$S optical modes, with $\alpha=c,s$ ($\cos\varphi$ and $\sin\varphi$ azimuthal dependence, respectively) and S=H,V (horizontal and vertical polarization). Examples of $\mathrm{LP}_{11\alpha}$ modes are the Hermite-Gaussian (HG) modes HG_{10} (X) and HG_{01} (Y), where X and Y directions are chosen parallel to the elliptical core of the fiber. We must stress that HG modes are a good approximation to the modes of a EC-FMF [Ip et al., 2015]. As commented, more states can be used, for instance, the LP_{o1} fundamental mode with H and V polarization. A more complicated system would be required but no new results would be obtained. Formally, the single photon quantum state excited in the modes $GS=XH,XV,YH,YV$ that we want to generate is

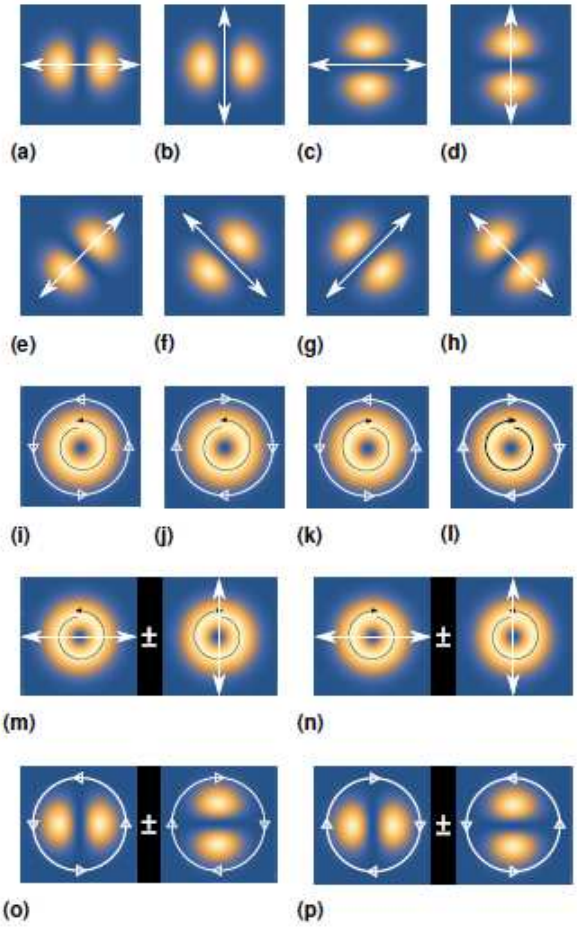


Figure P3.1: Spatial modes used in this work: (P3.1a) mode $|XH\rangle$, (P3.1b) mode $|XV\rangle$, (P3.1c) mode $|YH\rangle$, (P3.1d) mode $|YV\rangle$, (P3.1e) mode $|X'H'\rangle$, (P3.1f) mode $|X'V'\rangle$, (P3.1g) mode $|Y'H'\rangle$, , (P3.1h) mode $|Y'V'\rangle$, (P3.1i) mode $|+L\rangle$, (P3.1j) mode $|+R\rangle$, (P3.1k) mode $|-L\rangle$, (P3.1l) mode $|-R\rangle$, (P3.1m) modes $|+H\rangle \pm |-V\rangle$, (P3.1n) modes $|-H\rangle \pm |+V\rangle$, (P3.1o) modes $|XL\rangle \pm |YR\rangle$, (P3.1p) modes $|XR\rangle \pm |YL\rangle$.

the following ququart

$$|\psi\rangle = \sum_{GS} \frac{e^{i\theta_{GS}}}{2} |GS\rangle = \\ = \frac{e^{i\theta_{XH}}}{2} |XH\rangle + \frac{e^{i\theta_{XV}}}{2} |XV\rangle + \frac{e^{i\theta_{YH}}}{2} |YH\rangle + \frac{e^{i\theta_{YV}}}{2} |YV\rangle \tag{P3.2}$$

where θ_{GS} represents the phases of the single photon quantum states where the information will be encoded.

The four MUBs, as well as the sixteen states needed, are shown in Table P3.1, where the last column shows the resulting state after the phases are introduced. H', V' and X',

Y' modes refer to the polarization and spatial LP modes, respectively, rotated an angle of $\pi/4$ (diagonal bases: $\bigotimes$ and $\oslash$ for spatial and polarization modes, respectively) with respect to the original base (linear bases: $\bigoplus$ and $\ominus$ for polarization and spatial modes, respectively). L and R modes refer to left-handed and right-handed polarization (circular polarization basis $\bigcirc$), meanwhile + and − refer to the Laguerre-Gauss modes (LG) LG_{01} and LG_{10} (orbital angular momentum basis $\odot$) with orbital angular momentum ± 1. In Fig. P3.1 are shown all these modes. Likewise, it is interesting to write the matrix transformations of the photon absorption operators between these basis,

$$\begin{pmatrix} \hat{a}_{X'|H'} \\ \hat{a}_{Y'|V'} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \hat{a}_{X|H} \\ \hat{a}_{Y|V} \end{pmatrix} \tag{P3.3a}$$

$$\begin{pmatrix} \hat{a}_{+|L} \\ \hat{a}_{-|R} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix} \begin{pmatrix} \hat{a}_{X|H} \\ \hat{a}_{Y|V} \end{pmatrix} \tag{P3.3b}$$

Now, by following the principle of protocol BB84, an emitter (Alice) randomly generates any state (P3.2) and send it to the receiver (Bob). Only when Bob randomly uses a detector that measures in the base used by Alice then he will detect the same sent bit, otherwise will detect any other value. However, optical fiber communications QKD protocols fail if there are modal crosstalk, modal lags and relative modal phase shifts throughout the optical transmission to the receiver. As commented, modal crosstalk is solved by using EC-FMF optical fibers that minimize the coupling between them [Milione et al., 2016b,Ip et al., 2015]. As for compensating four relative lags and phases ϕ_{GS} between modes we will show that the optical system has to implement a double round loop together with appropriate inversions of quantum states. We must stress that, although Alice sends the ququarts, the double loop starts at Bob's subsystem, as will shown in the next section. Finally, BB84 protocol requires a random generator of the sixteen states of Table P3.1 and a detection device implementing projective measurements in a random basis as well. The random detection basis choice will be implemented by using beam-splitters.

P3.3 Phase auto-compensating cryptography in EC-FMF fibers

A sketch of the proposed encryption system formed by Alice and Bob subsystems is shown in Fig. P3.2. Alice subsystem starts with a circulator and is formed by a modal inversion device (MID) for modal auto-compensating purposes and a relative phase shifter device (RPS) to produce different quantum states. The generation of the primary quantum state $|\psi_p\rangle$ and the detection of the final quantum state $|\psi\rangle$ (projective measurements) is made in the Bob subsystem. This subsystem is composed by a primary quantum state generator device (QSG), an optical fiber delay device (OFD), a multi-round trip controller electro-optical device (RTC) and the detection system, where quantum states are measured once a double-round trip is made. In this section we present how all these devices work except the detection device, which will be analyzed in the next section. However, before starting the detailed study of the optical propagation of the quantum states through

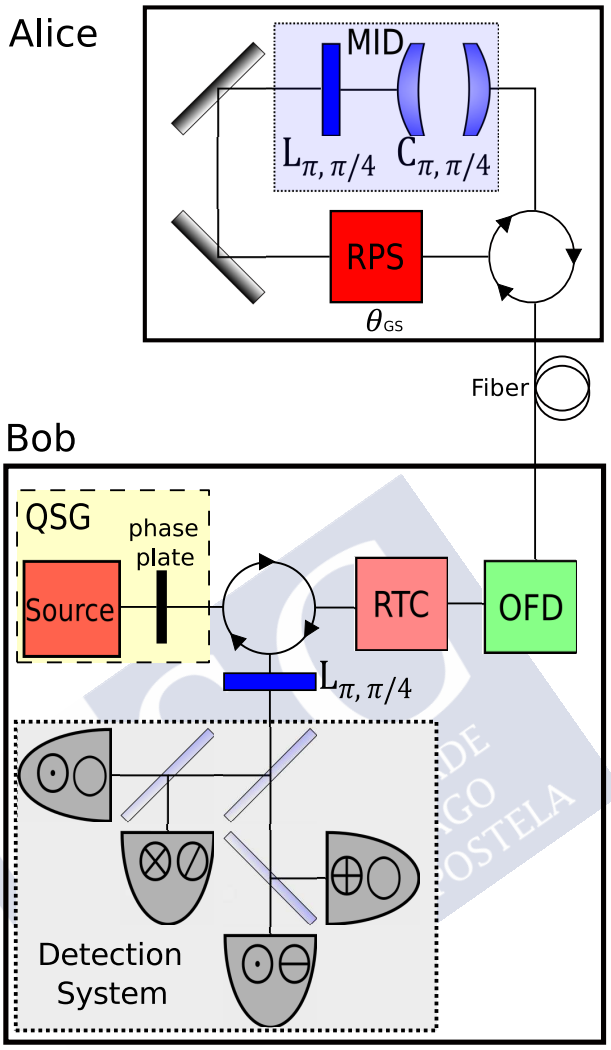


Figure P3.2: Sketch of the modal phase auto-compensating encryption system

the encryption system we describe two particular components which are the building-blocks of the main devices of the HD-QKD system presented, namely mode converters, based on introducing relative phases between spatial optical modes, and spatial mode multiplexers by using Mach-Zehnder interferometers.

P3.3.1 Mode Converter and Mach-Zehnder Interferometers

There are different approaches to get mode converters. We choose that one based on introducing relative phases between optical modes. For instance, a cylindrical lens converter (CLC) composed of two cylindrical lenses with focal f, separated a distance d and whose principal meridians are parallel [Beijersbergen et al., 1993]. If the distance between the lenses is $d = 2f$, then a relative phase $\gamma_G = \pi$ is introduced between LP_c and

LP_s modes when the main axis of the CLC are aligned with the X-Y basis of the modes. The matrix transformation of a CLC whose axis are rotated an angle α with respect to the X-Y basis is the following

$$C_{\pi,\alpha} = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} \tag{P3.4}$$

We see that it is analogous to the transformation introduced by a half wave plate (HWP) for polarization, which will be denoted as $L_{\pi,\alpha}$. The more interesting cases, and used in this work, are: $\alpha = 0, \pi/4, \pi/8$. On the other hand, if LP modes are Hermite-Gaussian modes then CLCs allow us to introduce an arbitrary phase γ_G between successive HG modes, such as X and Y modes, with total independence of the light polarization state. This phase γ_G appears due to the different Gouy phases acquired by the HG modes passing through the lenses. For example, if the distance between the lenses is $d = \sqrt{2}f$, the phase introduced is $\gamma_G = \pi/2$. This relative phase transforms HG modes into LG modes and vice versa. Its matrix transformation is as follows

$$C_{\pi/2,\alpha} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 - i\cos 2\alpha & -i\sin 2\alpha \\ -i\sin 2\alpha & 1 + i\cos 2\alpha \end{pmatrix} \tag{P3.5}$$

On the other hand, a Mach-Zehnder interferometer (MZI), also based on Gouy phases (Gouy phase interferometry), allows to manipulate optical modes and therefore quantum states [Liñares et al., 2017c]. The most basic operation is to control the output port by introducing selective phases $0, \pi$ for X and Y spatial modes, respectively, in one of its arms. Thus, if X and Y modes enter through the same input port then these modes exit through different ports and vice versa. Likewise, arbitrary relative phases between LP_c and LP_s modes (selective phases) can be required in order to implement optical transformations with quantum states excited in LP modes. If the modes exit through different output ports of a MZI, then arbitrary relative phases or long delays can be introduced. Next, modes can be recombined with another MZI, and a modal conversion is achieved. Obviously this transformation requires two MZIs, but it is an alternative to the above CLCs when necessary.

In short, we can use Gouy phase interferometry to manipulate spatial modes by employing Mach-Zehnder interferometers (MZI) with CLCs. As commented, if we introduce a phase π between X and Y modes in a MZI by means of a CLC with $\alpha = 0$ ($\mathrm{C}_{\pi,0}$) then the modes will exit through different outputs. This interferometer will be called $\mathrm{MZIC}_{\oplus}$ and allows us to use it as a beam splitter for spatial modes. In Fig. P3.3(b) a $\mathrm{MZIC}_{\oplus}$ is shown (it is inserted within a rectangle). Now, we can start the description of the devices of the HD-QKD optical system.

P3.3.2 OFD, MID and RTC

First of all, let us consider the QSG device consisting of a single photon source emitting a polarized photon and a mode converter (by a phase plate, a SLM...) producing a

HG mode [Liñares et al., 2017a]. Accordingly a single photon primary quantum state $|\psi_p\rangle = |X'H'\rangle$ of Table P3.1 is obtained, that is,

$$|\psi_p\rangle = |X'H'\rangle = \frac{1}{2}\left(|XH\rangle + |XV\rangle + |YH\rangle + |YV\rangle\right) \tag{P3.6}$$

Note that the corresponding relative phases θ_{GS} will be introduced in this state and therefore any ququart state given by Eq. (P3.2) can be obtained. Likewise, this state could also be generated by using an attenuated laser, in such a way that the protocol would work with weak coherent states, and therefore decoy states could be used. However, the optical implementation presented in this work would be the same.

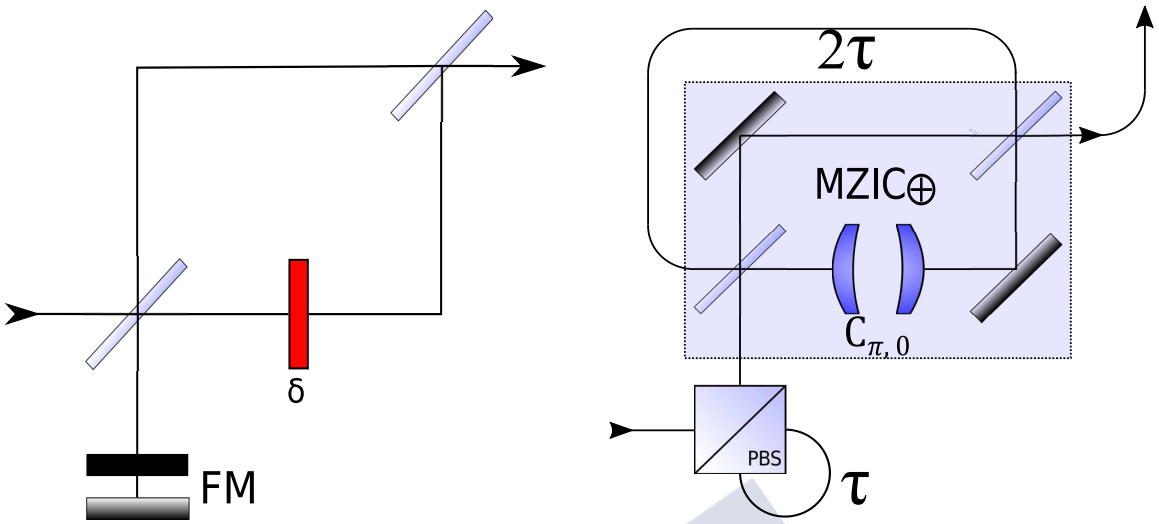
The primary quantum state given by Eq. (P3.6) will go into an optical circulator and will be sent to the delay optical device OFD as shown in Fig. P3.2. In this first loop the RTC device is switch off. An OFD device is needed in order to separate modes and introduce the phases θ_{GS} to the four base states that make up the state given by Eq. (P3.2). This device can be made with a $\text{MZIC}_{\oplus}$ and a polarization beam splitter (PBS) as shown in Fig. P3.3(b). Inputs and outputs of a $\text{MZIC}_{\oplus}$ and a PBS are coupled by loop paths to force all four states through the same output. The loops are set to introduce delays 2τ and τ in the Y and V optical modes, respectively. In addition, the fiber introduces different phases ϕ_{GS} to each mode which depends on their effective index but also contains a relevant random part that changes slowly. Therefore, for photons of frequency ω arriving to the Alice subsystem, we obtain the following state

$$\begin{aligned}|\psi_{A1}\rangle = \frac{1}{2}\Big(&e^{i\phi_{XH}}\,|XH\rangle + e^{i\omega\tau+i\phi_{XV}}\,|XV\rangle + \\ &e^{i2\omega\tau+i\phi_{YH}}\,|YH\rangle + e^{i3\omega\tau+i\phi_{YV}}\,|YV\rangle\Big)\end{aligned} \tag{P3.7}$$

Once the four delayed states reach the Alice subsystem the MID shown in Fig. (P3.2) transforms the quantum state by means of modal inversion in such a way that $|XH\rangle \rightarrow |YV\rangle$, $|XV\rangle \rightarrow |YH\rangle$, $|YH\rangle \rightarrow |XV\rangle$, $|YV\rangle \rightarrow |XH\rangle$. Note that Alice device contains a RPS, a HWP and a CLC. The former is off at this moment, so it does not alter the state. The axes of the HWP and the CLC are rotated at $\pi/4$, that is, the elements perform the transformations $\text{C}_{\pi,\pi/4}$ and $\text{L}_{\pi,\pi/4}$ as shown in Fig. P3.2. This is the modal inversion device (MID). As a result both the spatial and polarization modes are permuted with each other, that is,

$$\begin{pmatrix}\hat{a}_{XH}\\ \hat{a}_{XV}\\ \hat{a}_{YH}\\ \hat{a}_{YV}\end{pmatrix} = \begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}\begin{pmatrix}\hat{a}_{XH_0}\\ \hat{a}_{XV_0}\\ \hat{a}_{YH_0}\\ \hat{a}_{YV_0}\end{pmatrix} \tag{P3.8}$$

Next, the state returns to Bob, but the fiber introduces again the phases ϕ_{GS} in the



(a) (b)

Figure P3.3: (a) RTC and (b) OFD.

respective modes and the OFD also introduces new delays, resulting in the following state

$$|\psi_{B1}\rangle = \frac{e^{3i\omega\tau}}{2}\Big[e^{i\phi_{XH}+i\phi_{YV}}\left(|YV\rangle + |XH\rangle\right) + e^{i\phi_{XV}+i\phi_{YH}}\left(|XV\rangle + |YH\rangle\right)\Big] \tag{P3.9}$$

Therefore the delay is compensated when the OFD is crossed for a second time, but the phases introduced by the optical fiber are only compensated in pairs. In order to obtain a full compensation of these phases, a second loop is needed after a polarization inversion. Therefore a double-round trip controller (RTC) is required to send the states to Alice a second time. This can be achieved by using a standard MZI with an electro-optic phase modulator introducing phases $\delta = 0, \pi$ in one of its arms as shown in Fig P3.3(a). The phase modulator could be synchronized with the return time of photons in order to introduce a phase π when state (P3.9) arrives for the first time. Consequently, state (P3.9) leaves the interferometer on a different path where a Faraday mirror (FM) is found as also shown in Fig P3.3(a). The Faraday mirror returns the states to Alice for a second time, permuting the polarization modes in order to swap their phases (second inversion). The corresponding permutation of absorption operators can be written in matrix form as follows

$$\begin{pmatrix} \hat{a}_{XH} \\ \hat{a}_{XV} \\ \hat{a}_{YH} \\ \hat{a}_{YV} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \hat{a}_{XH_0} \\ \hat{a}_{XV_0} \\ \hat{a}_{YH_0} \\ \hat{a}_{YV_0} \end{pmatrix} \tag{P3.10}$$

However, when the state returns to Bob after the second round trip, the modulator of the RTC will not introduce any phase (it will be switch off) and the state will straightfor-

wardly go to the detection system through the circulator because the auto-compensating of the states will have been achieved, as shown in next section. Finally, it is worthwhile to comment that optical delays delays could also be achieved in a alternative way by taking into account the different propagation constants of the optical modes (intermodal dispersion). Thus, for an enough long optical fiber different delays would be obtained, which would also be cancelled by the auto-compensating method proposed in this work.

P3.3.3 Phase auto-compensating Process and Ququarts

Next, by taking into account all the steps formerly described we can check that auto-compensating process is achieved and ququarts reach the detection system. As explained before, state (P3.9) arrives to Bob's RTC for the first time and is sent back to Alice implementing transformations (P3.10). Taken into account the delays introduced by the OFD and transmission phases ϕ_{GS}, the following state will arrive to Alice during the second loop:

$$|\psi_{A2}\rangle = \frac{e^{3i\omega\tau}}{2}\Big[e^{i\phi_{XH}+i\phi_{YV}}\left(e^{2i\omega\tau+i\phi_{YH}}\,|YH\rangle + e^{i\omega\tau+i\phi_{XV}}\,|XV\rangle\right) + e^{i\phi_{XV}+i\phi_{YH}}\left(e^{i\phi_{XH}}\,|XH\rangle + e^{3i\omega\tau+i\phi_{YV}}\,|YV\rangle\right)\Big] \tag{P3.11}$$

Next, as a consequence of the OFD, Alice will always receive the four base states $|GS\rangle$ at different times and therefore she can introduce the θ_{GS} phases to each of them using the electro-optical phase modulator RPS in either of both loops. We must stress that, despite the fact that the order in which the base states got out of Bob subsystem is ($|XH\rangle$, $|XV\rangle$, $|YH\rangle$, $|YV\rangle$), as seen in Eq. (P3.2), the order in which they arrive by the second time is ($|XV\rangle$, $|XH\rangle$, $|YV\rangle$, $|YH\rangle$), as a consequence of the MID inversions in both loops and the polarization permutation introduced by the Faraday mirror between them. Accordingly, the order in which Alice must introduce the θ_{GS} phases with the RPS is the latter, in order to obtain the state given by Eq. (P3.2). Alternatively, she can use the former if states are reordered later by a $L_{\pi,\pi/4}$ at the input of the detection system, as shown in Fig. P3.2. In short, once the auto-compensation is completed, the following state is obtained

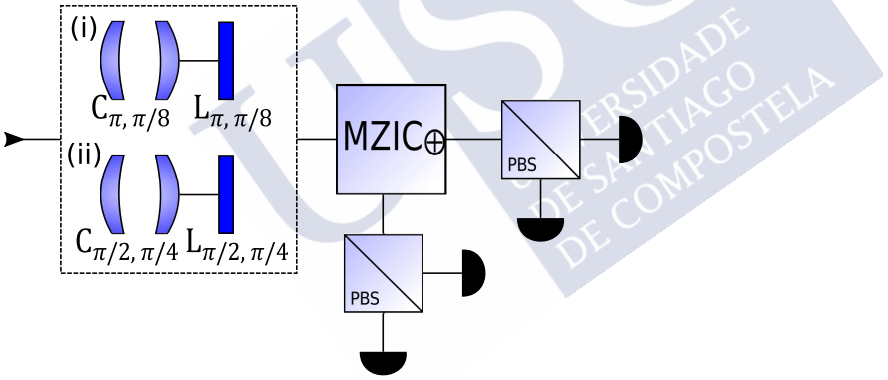
$$|\psi\rangle = e^{i\left(6\omega\tau+\sum_{GS}\phi_{GS}\right)}\sum_{GS}\frac{e^{i\theta_{GS}}}{2}|GS\rangle \tag{P3.12}$$

We can see that, excluding a global phase, the desired ququart is obtained, so the double round and appropriate modal inversion have allowed to correctly compensate all phase fluctuations and lags in the optical fiber communication system. Next, this state enters the detection system where a projective measurement is implemented such as explained in next section.

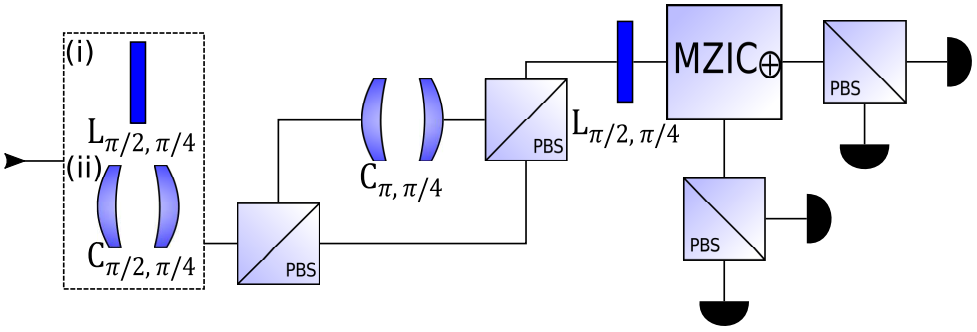
P3.4 Random detection system and measurement

The detection system consists of four devices arranged to measure state (P3.2) in the four basis of Table P3.1. BB84 requires that the measurement basis be chosen randomly, what can be easily implemented by using three beam splitters in the detection system as shown at the bottom of Fig P3.2, that is, the state can reach any of the four devices performing a projective measurement. The use of beam-splitters can avoid many of the attacks on the detection system whose quantum base choice has to be made by reconfigurable devices. All of the four devices make use of a $\text{MZIC}_{\oplus}$ with two PBSs at each output, as shown in Fig P3.4. The interferometer separates modes X and Y while the PBSs separates modes H and V. Therefore, states from Table P3.1 only need to be transformed into spatial and polarization linear basis X-Y and H-V, respectively, to get correct measurements. Once again, and for sake of simplicity, we consider that LP modes are Hermite-Gaussian ones.

We start with projective measurements in $\otimes\oslash$ and $\odot\bigcirc$ bases with the detectors shown in Fig P3.4.a. To measure the four states of $\otimes\oslash$ basis, such states have to be rotated at $\pi/4$, which can be easily done by using a CLC: $\text{C}_{\pi,\pi/8}$ and a HWP: $\text{L}_{\pi,\pi/8}$, that



(a)



(b)

Figure P3.4: (a): (i) detector $\otimes\oslash$, (ii) detector $\odot\bigcirc$ (b): (i) detector $\oplus\bigcirc$, (ii) detector $\odot\ominus$.

is, states $|XH\rangle$, $|XV\rangle$, $|YH\rangle$ and $|YV\rangle$ are obtained. Next, the $\text{MZIC}_{\oplus}$ separates the spatial modes, and the PBSs the polarization modes, therefore a projective measurement in the $\bigoplus \ominus$ base is obtained. Similarly, to measure in $\odot \bigcirc$ basis requires using a CLC and a quarter wave plate (QWP) rotated at $\pi/4$, that is, $\text{C}_{\pi/2,\pi/4}$ and $\text{L}_{\pi/2,\pi/4}$ to convert the LG modes and circular polarization modes into HG spatial modes and linear polarization modes, that is, $|XH\rangle$, $e^{-i\pi/2}|XV\rangle$, $e^{i\pi/2}|YH\rangle$ and $|YV\rangle$, where phases $e^{\pm i\pi/2}$ are not relevant. Next, the $\text{MZIC}_{\oplus}$ separates the spatial modes, and the PBSs the polarization modes, therefore a projective measurement in the $\odot \bigcirc$ base is obtained.

Measuring in $\bigoplus \bigcirc$ and $\odot \ominus$ bases is slightly more complicated. First of all, a QWP: $\text{L}_{\pi/2,\pi/4}$ for $\bigoplus \bigcirc$ base, and a CLC: $\text{C}_{\pi/2,\pi/4}$ for $\odot \ominus$ base, are required for turning the circular bases into the linear ones, as shown in Fig P3.4. Indeed, in both cases the following states, excluding global phases, are obtained: $|XH\rangle \pm i\,|YV\rangle$, $|XV\rangle \pm i\,|YH\rangle$. Next, the states go through an interferometer formed by two PBSs and a $\text{C}_{\pi,\pi/4}$ in one of its arms, so a permutation of spatial modes happens and the following states are obtained: $|XL\rangle$, $|XR\rangle$, $|YL\rangle$ and $|YR\rangle$. As a result, the original basis is transformed into the $\bigoplus \bigcirc$ basis. Finally, a QWP rotated $\pi/4$, that is, $\text{L}_{\pi/2,\pi/4}$, is required to turn the circular polarization basis L-R into the linear one H-V. Next, the $\text{MZIC}_{\oplus}$ separates the spatial modes, and the PBSs the polarization modes, therefore projective measurements in the $\bigoplus \bigcirc$ and $\odot \ominus$ bases have been obtained.

Finally, as our system consists in a double loop, we have to be careful that the states in the first loop do not overlap with those ones in the second loop, since Alice's modulator and Bob's interferometer operate differently on them. Accordingly, a temporal processing strategy must be used. Let us consider a light source sending states $|X'H'\rangle$ with a period T and being t_L the time that light takes to go from Alice to Bob through an optical fiber with length L. Obviously, a state will complete the loop in $t = 2t_L + 3\tau$, taking into account the total delay introduced by the OFD (P3.9), and the maximum number of photons in the fiber in just one loop will be given by $N = \left\lceil \frac{2t_L+3\tau}{T} \right\rceil$. When the first photon (photon 1) arrives to Bob for the first time and it is sent back to Alice, the time differences between this state and the last one (N), as well as the next one ($N+1$), sent by Bob are given by the following expressions:

$$\Delta t_{1,N} = 2t_L + 3\tau - (N-1)\,T \tag{P3.13a}$$

$$\Delta t_{1,N+1} = NT - 2t_L - 3\tau \tag{P3.13b}$$

As a result, the time difference between states sent for the first time and those sent for the second time will be given by $\Delta t = \min\left(\Delta t_{1,N}, \Delta t_{1,N+1}\right)$ and therefore $0 \leq \Delta t \leq T/2$. However, as a consequence of the generation of a delayed group of states (P3.7) and (P3.11) during transmission, the condition $\Delta t > 3\tau$ must be fulfilled to prevent delayed states in second loop to overlapping with those ones of the first loop. The value Δt marks the maximum operation time of Bob electro-optical modulator and it is optimal when

states of second loop travel in the middle of those in the first loop, that is,

$$\Delta t = \frac{T}{2} \tag{P3.14}$$

The electro-optical modulator used by Alice has a time operation limited by $t_A = \min(\tau, \Delta t - 3\tau)$, where τ is the difference between the delayed states (P3.7) and $\Delta t - 3\tau$ is the difference between the group of delayed states in the first and second loops. In order to ensure that the operation time is τ, it is needed that $\Delta t \geq 4\tau$. So, we have to select our delay to be

$$\tau \geq \frac{T}{8} \tag{P3.15}$$

Another possibility for temporal processing is to send a series of N states during a time $2t_L$ and stop during the same amount of time. It can be easily applied but the transmission rate is trivially reduced by half if the period T is the same.

P3.5 Security analysis

In this section we present a short study about security of the cryptographic system described along this work. By one hand, we must indicate that security analysis for attacks based on quantum cloning machines for one-way d-dimensional BB84 protocol qudits have been made in [Cerf et al., 2002]. In particular, a secret key rate R has been obtained, that is,

$$R \geq \max(I_{AB} - I_{AE}, I_{AB} - I_{BE}) \tag{P3.16}$$

where I_{AB}, I_{AE} and I_{EB} represent the mutual information shared between Alice and Bob, Alice and Eve, and Bob and Eve respectively. The mutual information is defined as $I(X;Y) = H(X) - H(X|Y)$, where H is the Shannon entropy, and in Alice and Bob's case is given by

$$I_{AB} = \log_2 d + F \log_2 F + (1-F) \log_2 \frac{1-F}{d-1} \tag{P3.17}$$

being $F = 1 - Q$, with Q the error rate, and d the dimension. By assuming that only $n = 2$ basis are used in the protocol, I_{AE} is given by equation P3.17 but replacing F by F_E, where

$$F_E = \frac{F}{d} + \frac{(d-1)(1-F)}{d} + \frac{2}{d}\sqrt{(d-1)F(1-F)} \tag{P3.18}$$

We show the bit rate obtained for $d = 2, 4$ in Fig. P3.5, where we observe that no secret key rate is distilled for QBERs greater than 25%. Note that if all the possible basis for the d-dimensional protocol are used, that is, $n = d + 1$, then the maximum QBER at which we can establish a secret key rate rises to 26.66% as stated in [Cerf et al., 2002]. In short, this analysis provides a quantitative security limit to our cryptographic system with $d = 4$.

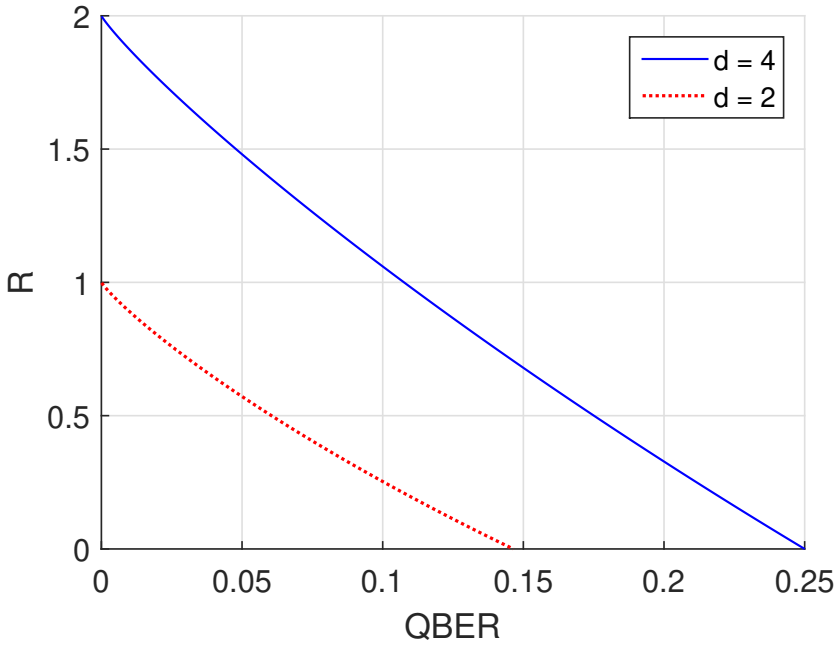


Figure P3.5: Bit rate in 2 and 4 dimensions using two basis.

On the other hand, it is well-known that side attacks can happen. However, MDI techniques can be used to avoid attacks to the receiver Bob, and thus a complete solution is achieved [Lo et al., 2012]. In our case a MDI protocol would have to be implemented for $d = 4$. Likewise, protocols based on decoy states can be used in order to increase the key secret rate [Hwang, 2003]. Both protocols will be applied to our system and presented in a next work. However, individual attacks, such as Trojan attacks have not a general solution, therefore they have to be solved *ad hoc*. Accordingly, we will analyze a very interesting attack that Eve can perform in our system which is called the phase-remapping (PR) attack [Fung et al., 2007, Xu et al., 2010], in order to make clear how our system improves the security.

Note that our protocol is not an one-way system, as our states go and return twice from Bob to Alice. This allows Eve to perform new attacks, not possible before, by attacking the communication that goes from Bob to Eve. Let us consider that Alice only encrypts the information during the second trip, the first trip is only used for achieving phase compensation and does not make much of a difference in terms of system security. This intercept-and-resend attack makes use of the fact that Alice's modulator has not an ideal square response. Therefore, Eve can time-shift the unencrypted states sent by Bob in such a way they will arrive at Alice's phase modulator on its rising edge, as shown in Fig. P3.6, and therefore, the phase θ_{GS} introduced by Alice. As $t_A < \Delta t$, there is no possibility of an overlapping between states. After the encryption, Eve intercepts the modified states and resends unmodified ones according with her measurements. If Eve

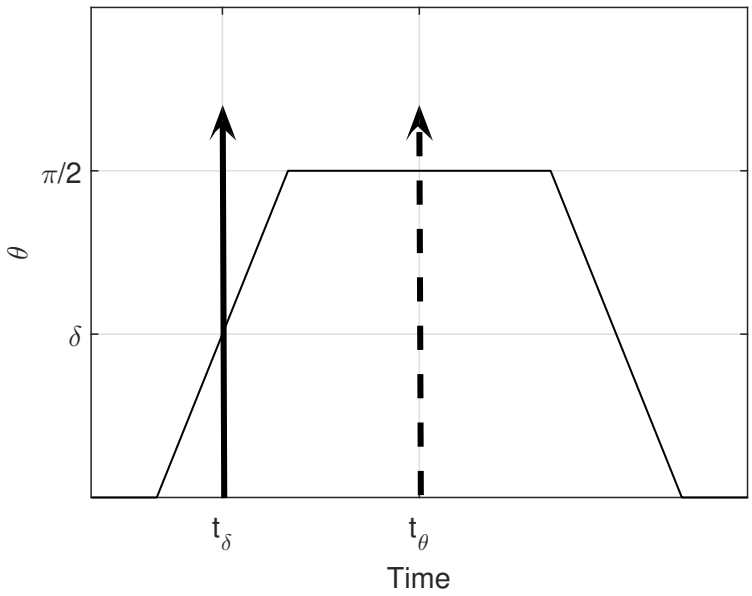


Figure P3.6: Time response of the phase modulator. The original pulse is time-shifted so it reaches the modulator at time t_δ instead of time t_θ.

intercepts and resends the states close to Bob, neither she nor Bob will have problems with uncompensated phases. Alternatively, we can assume that Eve has a system to precisely correct the phase difference between modes when she intercepts the states, and that she can send her states to Bob in an ideal manner. We will study the influence of this attack on our proposed system and, therefore, generalize the results of Fung et al. [Fung et al., 2007].

First of all, if we observe the sixteen possible states in Table P3.1 we can see that they are determined by only two angles, for example θ_{XV} and θ_{YH}, which can take values $\theta_{XV}, \theta_{YH} = 0, \pi/2, \pi, 3\pi/2$, while the third one is fixed for each pair of angles θ_{XV}, θ_{YH}. This third angle can be written as $\theta_{YV} = 3\left(\theta_{XV} + \theta_{YH}\right) \mod 2\pi$.

As said before, in the PR attack Eve time-shifts the states sent by Bob in order to modify the applied phase. In this way, Eve can change the phase information θ_{GS} from $\{0, \pi/2, \pi, 3\pi/2\}$ to $\theta_{GS} = \{0, \delta_{GS}, 2\delta_{GS}, 3\delta_{GS}\}$. Let us consider that Eve makes the same time-shift in the different modes, and, therefore, introduces the same δ, which is reasonable as she is going to obtain better results for lower δs. In consequence, Alice is actually introducing phases $\theta_i = k_i\delta$ in state (P3.2), where $k_i = \{0, 1, 2, 3\}$, with $i = 1, 2, 3$ referring to modes $GS = XV, YH, YV$ respectively, and $k_3 = 3\left(k_1 + k_2\right) \mod 4$.

In short, the actual state send by Alice in this attack (P3.2), written in the ququart

basis is

$$|\tilde{\psi}_{k_1k_2}\rangle = \frac{1}{4}\left[\left(1+e^{ik_1\delta}+e^{ik_2\delta}+e^{ik_3\delta}\right)|1_0\rangle + \left(1-e^{ik_1\delta}+e^{ik_2\delta}-e^{ik_3\delta}\right)|1_1\rangle \right. \\ \left. + \left(1+e^{ik_1\delta}-e^{ik_2\delta}-e^{ik_3\delta}\right)|1_2\rangle + \left(1-e^{ik_1\delta}-e^{ik_2\delta}+e^{ik_3\delta}\right)|1_3\rangle\right] \tag{P3.19}$$

where the states $|1_j\rangle$ correspond to states in base $\bigotimes \oslash$ from Table P3.1. For simplicity, we are going to rename our state as $|\tilde{\psi}_{bs}\rangle$, where $b, s = 0, 1, 2, 3$ refers to base and state respectively, and they correspond orderly, see Table P3.2, to the basis and states shown in Table P3.1. For $\delta = \pi/2$, we recover the original states which we denote as $|\psi_{bs}\rangle$

Table P3.2: Quantum states represented in notations b, s and k_1, k_2

b	0				1				2				3			
s	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
k_1	0	2	0	2	1	3	1	3	0	2	0	2	1	3	1	3
k_2	0	0	2	2	1	1	3	3	1	1	3	3	0	0	2	2
k_3	0	2	2	0	2	0	0	2	3	1	1	3	3	1	1	3

For analyzing the influence of the attack we will follow the same approach as in [Fung et al., 2007], but generalizing it to four dimensions. In this way, Eve performs a positive-operator valued measure (POVM), consisting in seventeen elements $\{M_{vac}, M_{bs} : b, s = 0, 1, 2, 3\}$, in the states sent by Alice $|\tilde{\psi}_{bs}\rangle$. For the measurement in M_{bs}, Eve sends the corresponding state $|\psi_{bs}\rangle$. The probability of obtaining $M_{b_1s_1}$ when Alice sends an state $|\tilde{\psi}_{b_2s_2}\rangle$ is given by $\mathrm{Tr}(M_{b_1s_1}|\tilde{\psi}_{b_2s_2}\rangle\langle\tilde{\psi}_{b_2s_2}|)$. In order to calculate the QBER in four dimensions, we have to take into account the three possibilities occurring when Eve measures $M_{b_1s_1}$ and next sends state the corresponding state $|\psi_{b_1s_1}\rangle$ to Bob. Since Bob and Alice only consider the results obtained in the same basis (they are the only results contributing to the QBER), then if Alice actually sent $|\tilde{\psi}_{b_1s_1}\rangle$, no error is committed (QBER= 0). If instead she sends a different state of the same basis $|\tilde{\psi}_{b_1s_2}\rangle$ ($s_2 \neq s_1$), Bob always gets an error (QBER= 1). Finally, if she sends a state from a different basis $|\tilde{\psi}_{b_2s_2}\rangle$ ($b_2 \neq b_1$), then Bob will get an error in 3/4 of his detections (QBER= 3/4). The total QBER will be given by the sum of the different QBERs weighted by the probabilities of each case happening for all the possible states and moreover normalized by the total probability of Eve sending states to Bob. Therefore, if n is the number of basis used the total QBER is given by

$$\mathrm{QBER} = \frac{\sum_{b=0}^{n-1}\sum_{s=0}^{3}\mathrm{Tr}(M_{bs}L_{bs})}{\sum_{b=0}^{n-1}\sum_{s=0}^{3}\mathrm{Tr}(M_{bs}B)} \tag{P3.20}$$

where n is the number of basis used and

$$L_{bs} = \sum_{\substack{j=0\\ j\neq s}}^{3}|\tilde{\psi}_{bj}\rangle\langle\tilde{\psi}_{bj}| + \frac{3}{4}\sum_{\substack{i=0\\ i\neq b}}^{n-1}\sum_{j=0}^{3}|\tilde{\psi}_{ij}\rangle\langle\tilde{\psi}_{ij}| \tag{P3.21}$$

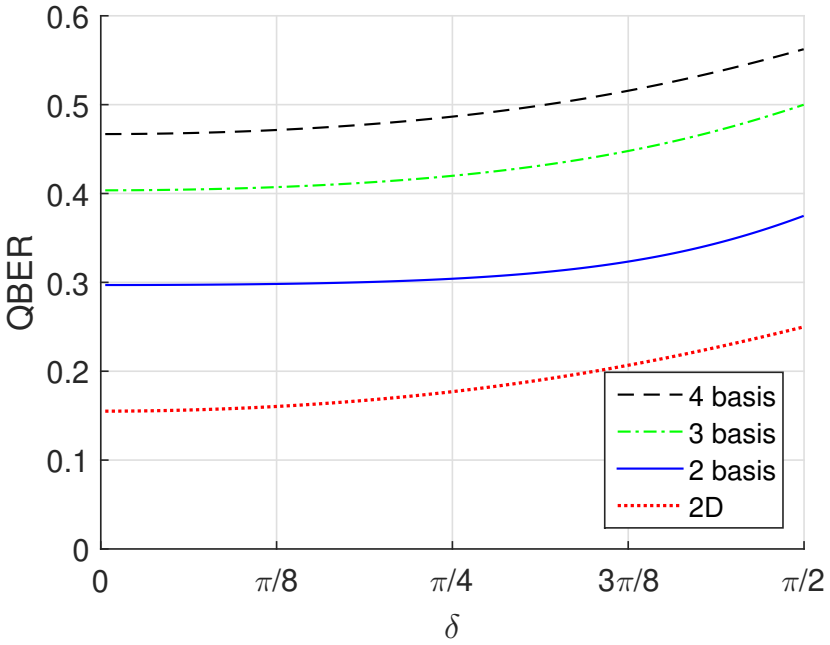


Figure P3.7: QBER achieved in a PR attack for different δs. From top to bottom, curves for 4, 3, 2 basis used. The lower curve correspond to th PR attack in two dimensions.

$$B = \sum_{i=0}^{n-1} \sum_{j=0}^{3} |\tilde{\psi}_{ij}\rangle \langle \tilde{\psi}_{ij}| \tag{P3.22}$$

Next, by using (P3.21) and (P3.22) and following closely the procedure in [Fung et al., 2007], we can minimize the QBER for a general set $\{M_{bs} : b, s = 0, 1, 2, 3\}$. The results are shown in Fig. P3.7. The lower curve corresponds to the 2-dimensional problem, where we can see that the QBER can be minimized from 25%, in the classical attack ($\delta = \pi/2$), to 15.5%, when $\delta \to 0$. The other curves correspond to our 4 dimensional case for a different number of basis n used. From top to bottom, in Fig. P3.7, results for $n = 4, 3, 2$ basis are shown. If $\delta = \pi/2$, we obtain the expected results from a classical intercept-and-resend attack for each n, that is, QBER $= \{\frac{9}{16}, \frac{1}{2}, \frac{3}{8}\}$. With the PR attack, the QBER values can be minimized to 46.7%, 40.4% and 29.7%, respectively. Note that in all cases, the QBER is significantly larger than for the 2-dimensional case. It is also important to remark that the minimum QBER obtained is still higher than 25%. Recall that this value was the limit QBER at which it was possible to obtain a secret bit rate under a cloning machine attack.

The PR attack is an attack exploiting the realistic weakness of Alice's subsystem, that is, the response of the electro-optic modulator. A very similar attack can also be employed in Bob's subsystem, with the aim being Bob's detectors [Makarov et al., 2006]. But in this case, the attack exploits the efficiency mismatch of the single photon detector

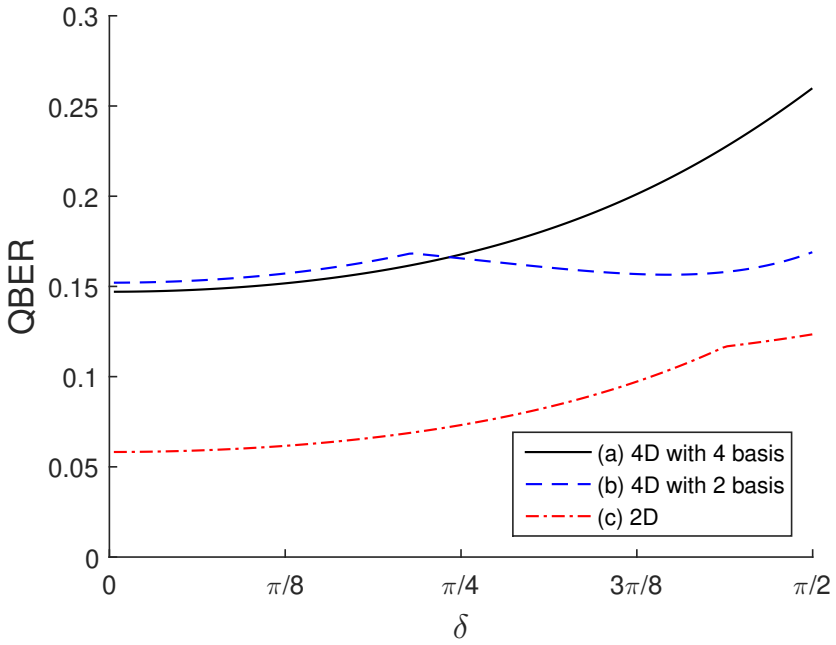


Figure P3.8: QBER achieved in a PR attack combined with a detector attack. The figure represents the QBER for the 4-dimensional case with 2 and 4 basis compared to the 2-dimensional case.

(SPD) [Makarov et al., 2006]. In other words, Eve can send her states to Bob at times in which the efficiency mismatch between detectors benefit her. By following the previous steps, and taking into account the efficiencies $\eta_b s$ of each ququart detector in matrices given by Eqs. (P3.21) and (P3.22), QBER curves can be obtained for a detector attack combined with a PR one. We will assume that the efficiency mismatch is the same in all the different detection systems proposed in Section P3.4, or in other words, the efficiencies are independent of the basis $\Delta\eta_{b_1 s} = \Delta\eta_{b_2 s}$.

In our analysis we have considered that, just like in the PR attack, if M_{bs} occurs then Eve sends the corresponding state $|\psi_{bs}\rangle$. In references [Makarov et al., 2006, Fung et al., 2007] fake-state attacks are used because they achieve lower QBERs for the regular case $\delta = \pi/2$. However, when $\delta \to 0$, the results are better in our case. Such results are shown in Fig. P3.8, where the QBER curves have been calculated for the limit case $\eta_1 = \eta_2 = \eta_3$ and with the ratio between these detectors and the fourth one being $\eta_1/\eta_0 = 0.08$. We can see that by employing both attacks Eve can reduce the QBER as low as 15%. However, we must indicate that our assumption that the efficiencies are independent of the basis is too optimistic for Eve. In fact, with different mismatches in different basis this attack would become difficult to implement successfully.

P3.6 Conclusions

In this work, we have shown that polarization an spatial modes can be combined to implement high dimension QKD through the use of EC-FMF optical fibers. For that, we have proposed a phase auto-compensating optical communication system in a four-dimensional encryption case based on two round trips together with appropriate spatial and polarization modal inversions. Both quantum states generation system and their detection (projective measurements) system of quantum states are based on modal converters, MZI, waveplates, PBSs, a Faraday mirror, optical fiber circulators and electro-optical devices, all of them available at the present photonics technology. We have chosen sixteen states and four basis, although three or two basis can also be chosen according our security/efficiency interest. Besides a quantum random detection based on beam-splitters has also been proposed. The procedure is quite general and therefore it could be applied to other kinds of FMF fibers. Finally, a study about the system performance under certain attacks has been realized, where it has been shown that the system behaves better than a plug and play system in two dimensions.

Funding

Authors wish to acknowledge the financial support of this work by Consellería de Cultura, Educación e Ordenación Universitaria, Xunta de Galicia with funds of the European Social Fund, and the partial financial support by Ministerio de Economía y Competitividad, Central Government of Spain, Contract number AYA2016-78773-C2-2-P (MINECO/FEDER, UE), and the partial support of Xunta de Galicia, Consellería de Educación, Universidade e FP under Grant (GRC) No. ED431C 2018/11.

4

Experimental Development of Quantum Projectors

In the previous chapter 3, we have designed an autocompensation system to implement HD-QKD in FMFs with colinear spatial modes. In particular, we presented in detail autocompensation systems for two and four dimensions. In these systems, we employed discrete photonic devices in order to mount bulk optic systems to perform the different operations required, like generation and measurement of states, etc. However, growing the dimension means that these bulk systems will become bigger and more complex, which can become a problem if we want to go to higher dimension. To solve this, integrated devices are a far more preferable approach to implement any quantum information processing operation. Colinear modes from FMF can be directly introduced in the codirectional path modes from integrated devices through the use of photonic lanterns. In this way, we have already proposed integrated quantum states generators in chapter 2, that could be used to generate high dimensional MUB quantum states in path modes in a random way.

The basic aim of this chapter lies in the fabrication and characterization of integrated quantum projectors (IQPs). These integrated devices are specially useful to measure quantum states transmitted in path modes of different waveguides. If we have a single photon state where the photon can be detected in different waveguides, an IQP makes such photon to be projected into one of them. Projecting different quantum states belonging to a MUB into different waveguides allow us to measure them. Thus, they are very interesting for performing HD-QKD utilizing path modes, which is going to be the focus of the next chapter 5.

Specifically, in the chapter we are going to design, fabricate and characterize the main components of an IQP, that is, integrated directional couplers. Couplers naturally work as IQPs for quantum states in path modes of dimension 2. But most importantly, they are also the basic block of any integrated device like, for example, quantum states generators, just as the two proposed in chapter 2. So, we are interested in being able to fabricate them by using the equipment and technology present in our photonics lab of the USC.

Our main objective in the chapter is to show that the fabrication of IQPs in glass by ion exchange technique is feasible in combination with a lithographic system having

a resolution of 2-3 μm. Lithography allows us to generate metallic masks with channel circuits of that size for being used in conjunction with ion exchange to produce waveguides in glass. We believe that ion exchange in glass is an ideal technique for different reasons, like its economical materials and processes required, its moderate losses and its good reproducibility Besides, the mode size in such is similar to that of optical fibers. Our aim is then, not only testing the possibilities of this technology, but preparing it to perform future experiments of quantum optics.

The structure of this chapter is structured as follows. In section 4.1, we present a theoretical introduction about IQPs. We explain how DCs can be used to implement SU(N) transformations (subsection 4.1.1) and how can we use this to measure quantum states of high dimension MUBs (subsection 4.1.2). Next, in section 4.2, the fabrication and design of our IQPs is explained in detail. We begin by explaining the ion exchange process for the fabrication of integrated waveguides and the characterization of said process to manufacture our wished waveguides with different salts (subsection 4.2.1). With this characterization we design the photomasks of our IQPs (subsection 4.2.2) and manufacture them through the preparation of a lithographic process in two steps (subsection 4.2.3). This section ends explaining the final processes (subsection 4.2.4) to get the IQPs ready: cutting, lapping and polishing. Finally, in section 4.3, our experimental IQPs are characterized. We use two different methods for characterization. First, we use polarizing interference microscopy (subsection 4.3.1) to analyse our fabricated IQPs, and last, we characterize their behaviour by coupling coherent light into them (subsection 4.3.2).

4.1 Integrated Quantum Projectors

4.1.1 Directional couplers (DC) for SU(N) transformations

In subsection 2.2.2, we solved Heisenberg's equations for the case of an integrated directional coupler 2×2 (2.2.45) obtaining, when the waveguides are synchronous, the transformation matrix

$$C_{\kappa z} = e^{i\beta z} \begin{pmatrix} \cos\kappa z & i\sin\kappa z \\ i\sin\kappa z & \cos\kappa z \end{pmatrix}. \tag{4.1.1}$$

The most interesting cases happen when κz takes values $\pi/2$ and $\pi/4$, for which matrix (4.1.1) takes the values

$$C_{\frac{\pi}{2}} = ie^{i\beta z} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{4.1.2}$$

$$C_{\frac{\pi}{4}} = \frac{e^{i\beta z}}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}. \tag{4.1.3}$$

By comparing these equations (4.1.2) and (4.1.3) with equations (2.2.42) and (2.2.43), we can see that DCs $C_{\frac{\pi}{2}}$ and $C_{\frac{\pi}{2}}$ behave for spatial modes like 45°-rotated HWP and

QWP, respectively, for polarization modes. In this way, a DC with $\kappa z = \pi/2$ works as a mode inverter, exchanging photons between both spatial modes. Meanwhile, a DC with $\kappa z = \pi/4$ acts as a entangling beam splitter by dividing the light from one spatial mode equally between both modes, with a $\pi/2$-phase shift between them. As a DC is a reciprocal element, it can work, as well, by joining light from two modes into a single one.

As it was already mentioned in subsection 2.2.2, to implement any unitary transformation SU(2), it is just needed to apply phase shifts between waveguides before and after a DC, as expressed in (2.2.49)

$$C(\delta_f, \kappa z, \delta_i) = e^{i\beta z} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta_f} \end{pmatrix} \begin{pmatrix} \cos\kappa z & i\sin\kappa z \\ i\sin\kappa z & \cos\kappa z \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta_i} \end{pmatrix} \tag{4.1.4}$$

In figure 4.1.1, the combination of a DC with two phase shifters required to implement any SU(2) transformation is shown. Integrated phase shifters can be build in different ways, depending if they have active or passive operation.

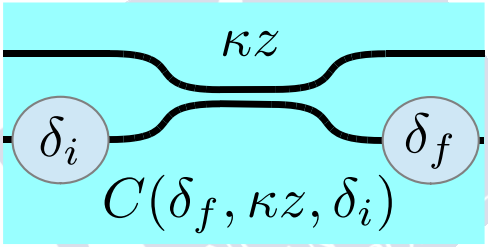


Figure 4.1.1: General directional coupler for implementing a SU(2) transformation.

Active phase shifters allow to actively tune the phase shift response for different wavelengths. There are several methods to build an active phase shifter. For example, thermo-optical shifters can be made by employing resistive micro heaters to modify the effective refractive index of the waveguides [Harris et al., 2014] through local temperature changes in the substrate. Apart from thermo-optical ones, other active phase shifters can be based on electro-optic effects [Soref and Bennett, 1987]. In this way, the refractive index can be modified through free-carrier plasma dispersion or absorption effects [Tang and Reed, 1995, Xu et al., 2005, Kim et al., 2014] or electro-mechanical actuators [Ikeda et al., 2010, Poot and Tang, 2014], which have faster response times that the thermic approach. Nonetheless, active phase shifters present the problem of being complex to implement, having high power consumption and control elements. Thus, they must be avoided if possible in favour of passive ones. Passive phase modulators are easy to design, although, as a drawback, any fabrication error in them is difficult to compensate. The main approaches to induce a passive phase shift consists of introducing a length difference between waveguides [Yegnanarayanan et al., 1997, Herrero-Bermello et al., 2017], increasing the optical path in one of them, or by changing the geometric dimension of one waveguide cross section [González-Andrade et al., 2018, Chen et al., 2018], modifying

the effective refractive index in it. Other approaches based on 1×1 multimode interference couplers [Morrissey and Peters, 2015, Han et al., 2015] or exploiting sub-wavelength metamaterial anisotropies [González-Andrade et al., 2020] have also been proposed.

We may want to design $N \times N$ DC with the aim of implementing different SU(N) transformations like a N-dimensional state projection into 1-dimensional. Let us suppose that we have N spatial modes in N different waveguides. The general coupling interaction between the N modes is given by Heisenberg's equations (2.1.12), as explained. Nonetheless, if we design an integrated $N \times N$ coupler, coupling interaction will mostly occur between adjoint waveguides. Thus, the general transformation of a $N \times N$ DC will be described by the equation system

$$\left\{ -i\frac{d\hat{a}_\nu}{dz} = \tilde{\beta}_\nu \hat{a}_\nu + \kappa_{\nu,\nu-1}\hat{a}_{\nu-1} + \kappa_{\nu,\nu+1}\hat{a}_{\nu+1}, \right\}_{\nu=0}^{N} \tag{4.1.5}$$

where ν is the mode number and being $\kappa_{0,-1} = \kappa_{\nu,\nu+1} = 0$. For example, for the case $N = 3$, that is, for a 3×3 DC, Heisenberg's equations (4.1.5) become

$$\begin{aligned} -i\frac{\partial \hat{a}_1}{\partial z} &= \beta_1 \hat{a}_1 + \kappa_{12}\hat{a}_2 \\ -i\frac{\partial \hat{a}_2}{\partial z} &= \kappa_{21}\hat{a}_1 + \beta_2 \hat{a}_2 + \kappa_{23}\hat{a}_3 \\ -i\frac{\partial \hat{a}_3}{\partial z} &= \kappa_{32}\hat{a}_2 + \beta_3 \hat{a}_3. \end{aligned} \tag{4.1.6}$$

Taking into account that $\kappa_{\nu,\nu'} = \kappa_{\nu',\nu}$ and considering the homogeneous case $\beta_1 = \beta_2 = \beta_3$, the solution to the system (4.1.6) is given by

$$\begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \\ \hat{a}_3 \end{pmatrix} = \frac{e^{i\beta z}}{2} \begin{pmatrix} 1+\cos(\sqrt{2}\kappa z) & i\sqrt{2}\sin(\sqrt{2}\kappa z) & -1+\cos(\sqrt{2}\kappa z) \\ i\sqrt{2}\sin(\sqrt{2}\kappa z) & 2\cos(\sqrt{2}\kappa z) & i\sqrt{2}\sin(\sqrt{2}\kappa z) \\ -1+\cos(\sqrt{2}\kappa z) & i\sqrt{2}\sin(\sqrt{2}\kappa z) & 1+\cos(\sqrt{2}\kappa z) \end{pmatrix} \begin{pmatrix} \hat{a}_{1_0} \\ \hat{a}_{2_0} \\ \hat{a}_{3_0} \end{pmatrix} \tag{4.1.7}$$

However, creating a $N \times N$ DC with predefined values of β_ν and $\kappa_{\nu,\nu+1}$ is not easy in practice, and what it is more, the number of free parameters is not enough for implementing a general SU(N) transformation in a single coupler. Therefore, another approach is required to implement it. Fortunately, it has been demonstrated that any SU(N) matrix can be factorized in terms of SU(2) matrices [Reck et al., 1994, Clements et al., 2016, de Guise et al., 2018]. In consequence, 2×2 DCs can be used to generate devices to perform any transformation $N \times N$. In this way, in [Reck et al., 1994], Reck et al. show that by using 2x2 BS matrices (2.2.34) in N, a particular case of matrix (4.1.4), it is possible to reduce the dimension of a unitary SU(N) matrix $U^{(N)}$ as

$$U^{(N)} \cdot C_{N,N-1} \cdot C_{N,N-2} \cdots C_{N,1} = \begin{pmatrix} U^{(N-1)} & 0 \\ 0 & e^{i\gamma_N} \end{pmatrix}, \tag{4.1.8}$$

where $C_{i,j}$ refers to transformation (4.1.4) between modes i and j. So, the effective dimension of the matrix U is reduced to $N-1$, with a phase shift γ in mode N. By recursively applying (4.1.8) and correcting phases γ_i in each mode with a diagonal matrix D, transformation $U^{(N)}$ can be factorized as

$$U^{(N)} = \left(C_{N,N-1} \cdots C_{N,1} \cdot C_{N-1,N-2} \cdots C_{N,1} \cdots C_{2,1} \cdot D\right)^{-1}. \tag{4.1.9}$$

More recently, de Guise et al. have shown [de Guise et al., 2018] that any SU(N) transformation $U^{(N)}$ can be written in terms of two SU($N-1$) matrices coupled by an SU(2) entangling beam splitter, as expressed by

$$U^{(N)}(\Omega) = U^{(N-1)}(\Omega') \cdot C_{12}(\delta_f, \kappa z, \delta_i) \cdot U^{(N-1)}(\Omega''). \tag{4.1.10}$$

The process (4.1.10) can be recursively continued in a straightforward way, ending in a triangular arrangement of SU(2) transformations.

4.1.2 An introduction to integrated quantum projectors (IQP)

As told, because of their reciprocal operation, DCs can be used to join light modes of different waveguides into a single one. In this way, and taking into account the factorization law, it is possible to build a device based in 2×2 DCs that projects quantum states of high dimension in quantum states of a lower dimension. We can denominate them integrated quantum projectors (IQPs). For example, if we have a single photon state entangled in N modes, we can introduce each mode into a single waveguide of an IQP reducing the dimension from N to n, as shown

$$\hat{P}_{N\to n}\left(e^{i\theta_1}\left|1_1\right\rangle + e^{i\theta_2}\left|1_2\right\rangle + \cdots + e^{i\theta_N}\left|1_N\right\rangle\right) \to e^{i\tilde{\theta}_1}\left|1_1\right\rangle + \cdots + e^{i\tilde{\theta}_n}\left|1_n\right\rangle. \tag{4.1.11}$$

Particularly, we are interested in the case when $n = 1$. In section 2.4 from chapter 2, we have shown a way of generating MUBs to implement HD-QKD with integrated devices. An IQP that projects a quantum state of dimension N into dimension $n = 1$ can be used as a quantum state detector. To work like this, it is required that an $N \times N$ IQP projects each quantum state of the different N possible states of one particular base, into a different of the N output waveguides. Thus, by detecting the photon in a particular waveguide, the received quantum state is identified.

Let us give some examples. Trivially, in dimension $N = 2$, a single $\pi/4$-DC works as an IQP with the right phase shifts. In equations (2.4.146), we showed the MUBs for dimension 2, which we can express in matrix form as

$$\mathcal{B}_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \mathcal{B}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \tag{4.1.12}$$

where each column represents a quantum state. The general expression of a DC with phase shifts was (4.1.4). As said, a $\pi/4$-DC projects the four possible states into a single

waveguide, with an appropriate initial phase shift δ_i, as

$$\begin{aligned} C\left(\frac{\pi}{2}, \frac{-\pi}{4}, 0\right) \cdot \mathcal{B}_1 = \mathbb{I}, \\ C\left(\frac{\pi}{2}, \frac{-\pi}{4}, \frac{\pi}{2}\right) \cdot \mathcal{B}_2 = \mathbb{I}. \end{aligned} \tag{4.1.13}$$

The final phase shift $\delta_f = \frac{\pi}{2}$ is not required and was just used to obtain the identity matrix $\mathbb{I}$ for aesthetic reasons. We can see how by applying different initial phases $\delta_i = 0, \frac{\pi}{2}$ we can correctly detect the quantum states in basis $\mathcal{B}_1$ and $\mathcal{B}_2$ respectively, as each state of a base is reduced to states $(1,0)$ and $(0,1)$.

Let us consider now the case of dimension $N = 3$. MUBs of dimension 3 can be obtained as show in [Brierley et al., 2009], and are given by matrices

$$\begin{aligned} \mathcal{B}_1^{(3)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} \\ 1 & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} \end{pmatrix}, \\ \mathcal{B}_2^{(3)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & 1 \\ e^{\frac{2i\pi}{3}} & 1 & e^{-\frac{2i\pi}{3}} \end{pmatrix}, \quad \mathcal{B}_3^{(3)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & 1 \\ e^{-\frac{2i\pi}{3}} & 1 & e^{\frac{2i\pi}{3}} \end{pmatrix}, \end{aligned} \tag{4.1.14}$$

where, again, each column represents a quantum state. Now, by following the factorization process of de Guise (4.1.10), three couplers in a triangular arrangement, as shown in figure 4.1.2, would be required. To obtain an IQP, the two DCs working between modes 2 and 3 have to be $\kappa z = \pi/4$ while the one between modes 1 and 2 must be $\kappa z = \arccos 3^{-1/2}$. At the same time, phase shifts $-\pi/2$ are needed before and after each DC. So, the IQP for dimension 3 will work as shown

$$C_{23}\left(\frac{-\pi}{2}, \frac{\pi}{4}, \frac{\pi}{4}\right) \cdot C_{12}\left(\frac{-\pi}{2}, \arccos\left(\frac{1}{\sqrt{3}}\right), \frac{-\pi}{2}\right) \cdot C_{23}\left(\frac{\pi}{4}, \frac{\pi}{4}, \frac{-\pi}{2}\right) \cdot \mathcal{B}_1^{(3)} = \mathbb{I}, \tag{4.1.15}$$

Now, this projector only works for base $\mathcal{B}_1^{(3)}$. To work for the other basis, the initial phase shifts must be different. Checking (4.1.14), we can observe that basis $\mathcal{B}_2^{(3)}$ and $\mathcal{B}_2^{(3)}$

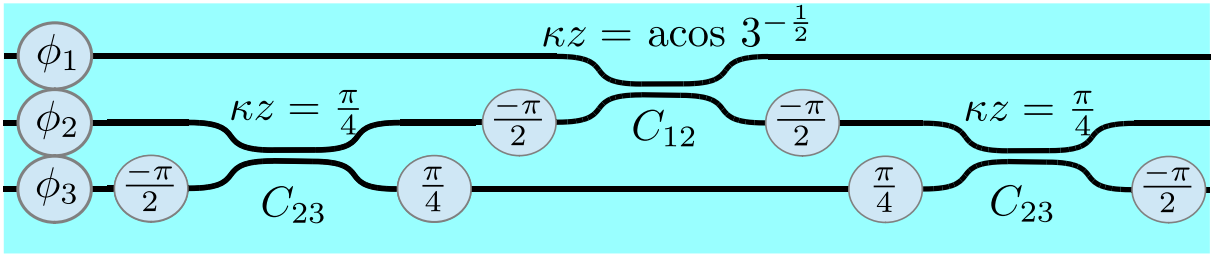


Figure 4.1.2: IQP for dimension 3.

can be derived from base $\mathcal{B}_1^{(3)}$ as follows

$$\mathcal{B}_2^{(3)} = D \cdot \mathcal{B}_1^{(3)}, \quad \mathcal{B}_3^{(3)} = D^2 \cdot \mathcal{B}_1^{(3)}, \tag{4.1.16}$$

where $D = \text{diag}\left(1, e^{\frac{2i\pi}{3}}, e^{\frac{2i\pi}{3}}\right)$. Thus, by introducing phase shifters $\Phi_{b\to 1}$ before the general DCs, we can transform the incoming quantum state of base $\mathcal{B}_b^{(3)}$ into a state of basis $\mathcal{B}_1^{(3)}$. Therefore, the IQP of base b for dimension 3 has the form

$$\hat{P}_b^{(3)} = \cdot C_{23}\left(\frac{-\pi}{2}, \frac{\pi}{4}, \frac{\pi}{4}\right) \cdot C_{12}\left(\frac{-\pi}{2}, \arccos\left(\frac{1}{\sqrt{3}}\right), \frac{-\pi}{2}\right) \cdot C_{23}\left(\frac{\pi}{4}, \frac{\pi}{4}, \frac{-\pi}{2}\right) \Phi_{b\to 1}, \tag{4.1.17}$$

where $\Phi_{1\to 1} = \mathbb{I}$, $\Phi_{2\to 1} = D^{-1}$ and $\Phi_{3\to 1} = D^{-2}$.

Finally, we can increase the dimension for $N = 4$. The four MUBs for this case were shown in expressions (2.4.147). Following de Guise's factorization (4.1.10) again, we need six different couplers with their shifts, as shown in figure 4.1.3. It can be demonstrated that the projector transformation can be given by

$$\begin{aligned}\hat{P}_b^{(4)} \cdot \mathcal{B}_b^{(4)} = C_{34}\left(\frac{-\pi}{2}, \frac{\pi}{4}, \frac{\pi}{8}\right) \cdot C_{23}\left(\frac{-\pi}{2}, \arccos\left(\frac{1}{\sqrt{3}}\right), \frac{-\pi}{4}\right) \cdot C_{12}\left(\frac{-\pi}{2}, \frac{\pi}{3}, \pi\right) \cdot \\ C_{34}\left(\frac{\pi}{8}, \frac{\pi}{3}, \frac{\pi}{8}\right) \cdot C_{23}\left(\frac{-\pi}{4}, \arccos\left(\frac{1}{\sqrt{3}}\right), \frac{-\pi}{2}\right) \cdot C_{34}\left(\frac{\pi}{8}, \frac{\pi}{4}, \pi\right) \cdot \Phi_{b\to 2} \cdot \mathcal{B}_b^{(4)} = \mathbb{I},\end{aligned} \tag{4.1.18}$$

where, once again, phase shifters are needed to transform any incoming basis b into basis 2, for which the projector is naturally configured. The required phase shifts are the following

$$\begin{aligned}\Phi_{1\to 2} &= \text{diag}\,(1, i, i, -1), \\ \Phi_{3\to 2} &= \text{diag}\,(1, 1, i, -i), \\ \Phi_{4\to 2} &= \text{diag}\,(1, i, 1, -i).\end{aligned} \tag{4.1.19}$$

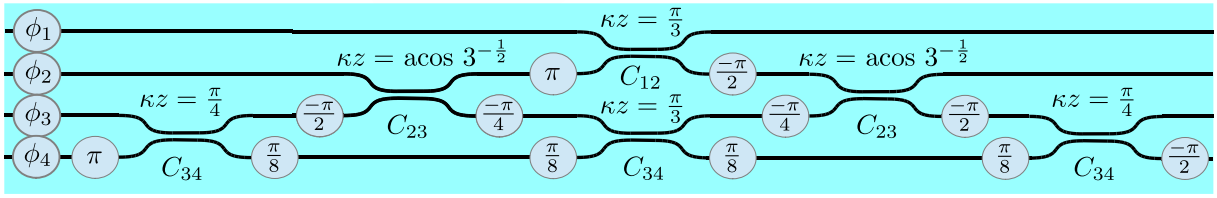


Figure 4.1.3: IQP for dimension 4.

Following the same procedure, we can design IQPs for the rest of dimensions. Nonetheless, in subsection P4.4 of chapter 5, we are going to present a different strategy to build IQPs. Our factorization works only for dimension $N = 2^m$ but has several advantages respect to de Guise's factorization. It requires a small number of couplers and phase shifter, five couplers as opposed to six for dimension 4 as an example, and these only consist of $\kappa z = \pi/2$ (4.1.2) and $\kappa z = \pi/4$ (4.1.2) DCs, instead of those general phases seen in (4.1.17) and (4.1.18). It is also worth noting that to find the right couplers for a given dimension N is not trivial, while in our case they always work the same way.

4.1.3 Introduction to ion exchange in glass and lithography for IQPs fabrication

As we have shown in the above examples, IQPs are essential devices in many applications of quantum information processing like in quantum cryptography. In next chapter (chapter 5), we are going to propose IQPs as measurement devices. For this reason, it is of great interest to employ and optimize technology present at our Lab to develop such integrated devices. In this thesis, we are going to use selective ionic exchange in glass for the fabrication of directional couplers, which are the basic blocks that constitute IQPs and work as IQPs of dimension 2. The fabrication process is going to be explained in next section 4.2.

Ion exchange is a process that can be applied to glass and other materials in order to change their chemical composition in a small superficial layer of few micrometers of thickness with the objective of making integrated devices [Najafi, 1992, Prieto Blanco, 2016, Prieto and Liñares, 1998], or even bulk optical elements [Montero-Orille et al., 2013,Liñares et al., 2017b,Balado Souto et al., 2016] for different applications. Basically, it consists of introducing doping ions from a salt solution into the substrate through different diffusion processes, like thermal or electric field-assisted diffusion [Prieto Blanco, 2016]. These processes are described by diffusive models where the refractive index $n(x, y, z)$ of the substrate is proportional to the concentration of doping ions $C(x, y, z)$. In this way, the concentration of doping ions inside the superficial layers of glass after the diffusion results in the increase of the refraction index in these regions. The index change allows certain wavelengths of light to be confined within a micrometric layer (where ion exchange was implemented) and to be propagated through total effective internal reflection. Thus, a integrated planar waveguide is done inside the glass.

If we want to fabricate IQPs like those shown in previous subsection 4.1.2, through ion exchange in glass, thermal diffusion must be done only in certain wished regions of the glass in order to obtain a circuit of channel waveguides. Therefore, to implement this selective ion exchange, photo-masks are required. Particularly, metallic masks are much more easily fabricated and patterned than dielectric ones. These photo-masks refer to a layer placed over the glass with the IQP pattern "printed" in it. This layer acts as a shield against ion exchange, allowing it only in the "printed" unprotected regions of the substrate not covered by metal. As a consequence, only such regions of the glass will experiment an increase in the refraction index. In this way, by opening small lines in the metal layer, channel waveguides can be created [Najafi, 1992, Prieto Blanco, 2016]. Other integrated optical elements, like diffraction gratings or phase discontinuities, can be created as well with through photo-masks [Liñares et al., 2000, Balado Souto et al., 2016].

Photo-masks are fabricated over a glass through photolithography [Levinson, 2005]. The photolithographic process consists of illuminate a certain original motif in order to obtain a image of its geometric pattern over a photosensitive photoresist previously deposited on the metallic layer. After that, through different chemical process, the geometric

pattern is imprinted on the metal, obtaining the photo-mask. This technique has been employed as the standard method for the fabrication of microelectronic integrated circuits since 1960 [Jaeger, 2002].

The original motif can be another photo-mask, to get the image through transmission, or a printed surface, getting the image through reflection. If the original motif is much bigger than the wished final pattern of the photo-mask, the lithographic optical system must implement an optical reduction. Photo-reduction lithography has the advantage that we can depart from a low resolution but big enough original printed pattern and generate a high resolution reduced image. Although reductive photolithography has been used for years in our laboratory, a new system had to be mounted and optimized to meet the resolution requirements needed to fabricate monomode channel waveguides.

4.2 Fabrication of IQPs by ionic exchange

4.2.1 Ion exchange

Once the metallic masks of the IQPs are obtained, the channel waveguides can be made inside the glass through ion exchange [Najafi, 1992, Findakly, 1985]. Commercial glasses often contain sodium (Na_2O) or potassium (K_2O) oxides to lower their glass transition temperatures. These alkali metals are in monovalent ion form (Na^+) and have an appreciable mobility for temperatures from around 200°C This high mobility of Na^+ ions allows them to be replaced by other monovalent ions from inside the glass or from an external source, like a salt solution. This exchange is done one by one to prevent charge accumulations keeping charge balance. Then, an equilibrium equation is established between salt and glass, which determines the dopant concentration at the glass surface, that is, a boundary condition is established. Common doping ions used in literature are other alkaline metals (lithium, potassium, rubidium and caesium) [Findakly, 1985], with potassium K^+ being the most used one, and other transition monovalent elements, like silver, thallium, and copper [Marquez et al., 1995].

The mobility of each cation is given by a diffusion equation, which, according to [Prieto-Blanco, 2008], can be written in a general way as

$$\frac{\partial c_i}{\partial t} = \nabla \frac{\mathbf{J}_i}{C_0} = \nabla \left(D_i g_i \nabla c_i + \frac{e D_i}{k_0 T} \mathbf{E} c_i \right), \tag{4.2.20}$$

where c_i is the molar fractions of each exchanged ions $i = A, B$, dependent of their concentrations C_i like

$$c_i = \frac{C_i}{C_A + C_B}, \tag{4.2.21}$$

while g_i and D_i are the thermodynamic factors and diffusion coefficients of both ions, respectively. The diffusion coefficients D_i rise with temperature, following an Arrhenius

equation as

$$D_i = D_{i0} \exp\left(-\frac{Q_i}{\kappa_B T}\right), \tag{4.2.22}$$

where Q_i is the activation energy, κ_B is Boltzmann constant and T is the temperature. However, when there are two alkaline ions involved in the process, the diffusion coefficients D_i also depend on the molar fraction of each ion. Both cations equal their diffusion coefficients when their molar fractions are similar, but if a cation specie is much more diluted than the other, it is also the slower one. This is called *mixed ion effect* or *mixed alkali effect* [Isard, 1969, Day, 1976]. Due to the one by one exchange between both ions, both diffusions are coupled resulting in an effective diffusion coefficient D_{eff}, which is roughly limited by the slow ion. D_{eff} can change about one order of magnitude as a function of c_A, having a maximum for the dopant mole fraction of $0.6 \leq c_A \leq 0.8$. Thus, equation (4.2.20) can be written as

$$\frac{\partial c_A}{\partial t} = \nabla \left(D_{eff}(c_A) \nabla c_A\right), \tag{4.2.23}$$

where the effective diffusion coefficient is

$$D_{eff} = \frac{(g_B c_A + g_A c_B) D_A D_B}{D_A c_A + D_B c_B} \tag{4.2.24}$$

As D_{eff} depends strongly on the molar fraction, the diffusion process is non linear. Particularly if a wide range of c_A values occur in the sample. This results in convex index profiles in planar waveguides.

4.2.1.1 Thermal diffusion

Ion exchange can be done through a diffusion process into a salt, being it thermic or field-assisted. In our case, we employ thermal diffusion using two different kinds of salts: a salt mixture containing silver nitrate ($AgNO_3$) and a pure salt of potassium nitrate (KNO_3). Thermal diffusion consists of submerging a glass into a melted salt at a high temperature. In this conditions, Na^+ ions inside the glass have a great mobility, so they come out of the glass and dissolve into the salt. At the same time, as explained, the doping Ag^+ (K^+) ions solved in the salt can get inside the glass occupying the vacuum left by the Na^+ ions. As a result, the concentration of Ag^+ (K^+) ions grows inside the superficial layers of glass resulting in the already mentioned increase of the refraction index (Δn) in this region.

The concentration of incoming ions on the glass surface is constant during the process and depends on an equilibrium equation, that is, it depends on the concentration of these ions in the salt. However, the concentration of dopant ions inside the glass gradually decreases with depth, and this fall is given by a non linear equation [Najafi, 1992, Liñares et al., 1994]. Particularly, $c_A = f\left(x/\sqrt{t}\right)$, that is, the boundary conditions are compatible with the Boltzmann's change of variable. As a consequence, the index change

also decreases with depth until reach the substrate index. The maximum index does not depend on the diffusion time, while the penetration depth does. A good experimental function to describe the index increase is the gaussian $\Delta n(x) = \Delta n_{max} exp\,(-x^2/d^2)$ being $d = \sqrt{4D \cdot t}$ the depth, where t is the diffusion time and D takes some value from that of $D_{eff}(c_A)$. The dependence of D_{eff} with the molar fraction of Ag^+ in the glass allows to obtain waveguides of similar depth, either with a diluted silver salt at 307°C or with a high concentrated one at 200°C.

Thermal diffusion can be used once again to perform a burial process of the waveguide. The objective is to "bury" the current superficial waveguide deep inside the glass, so that the waveguide is no longer in contact with air. In this case, the already diffused glass is submerged into a melted salt of $NaNO_3$ for a second diffusion. The Na^+ ions present in the salt replace surface doping cations, remaining those that are deeper in the glass. The concentration of doping ions (Ag^+ or K^+) also expand inside the glass, which lowers the increase of refraction index (Δn). This process is interesting because it moves the light mode away from the surface, which is full of irregularities. Thus, losses are highly reduced.

4.2.1.2 Experimental setup

The thermal diffusion is made in a furnace *Techne Fluidised Bath SBL-2*, which is able to heat up and maintain the salt at the right temperature, with oscillations below 1°C (except by a brief transition period after dip the sample and its holder). The furnace is made by an open cylindrical container with a porous base, to allow air circulation, and three electric resistors placed near the bottom, that provide heat. The cylinder is filled by a layer of alumina sand (aluminium oxide). Air is pumped through the porous base lightening the sand and turning it into a "fluid". This fluid behaviour of the sand, similar to a boiling liquid, allows an homogeneous heating throughout the medium, distributing the heat provided by the resistors. To control the temperature in the furnace, a thermal probe is introduced into the sand and connected to an electronic controller. This controller regulates the power supplied to the resistors according to the set temperature and the measured one.

With the purpose of avoid sand losses, to not disturb the set temperature, but allowing air outlet at the same time, two concentric metal casings were added at the furnace. The interior one has a cylindrical part to fit into the container and two frustoconical parts that create a wider region in the middle part. In the widest region, air velocity decreases, allowing the fall of grains of sand that could have been suspended in the air. The residual sand that manages to come out is collected in the outer casing, which rests on the upper base of the furnace while wrapping the inner casing. Air outlet is allowed thanks to the presence of small holes in the casings. Both of them have a larger hole of 105 mm in diameter each, centered and aligned between them. A steel tube is inserted through these holes, containing a certain amount of salt at the bottom. The tube rests on the outer casing, but its bottom is fully buried into the sand allowing a good thermal contact. In



(a)



(b)



(c)

Figure 4.2.4: Experimental setup to realize thermal diffusion. Figure (a) shows the furnace whose temperature is controlled by the temperature controller (b). The glasses are introduced in the central tube using the wire holder (c)

.

the lab, we have a set of different tubes, each one with its own salt mixture, to make easier the change between them for different purposes. We use silver eutectic salt mixtures, as they had the advantage of lower melting points respect to pure salts. This allows the high concentration silver exchange to be done at a low enough temperature to be controllable. On the contrary, we employ a pure salt of potassium at higher temperature since it diffuses much slower.

The glass samples are placed on a wire support. This is attached to a steel rod that goes through a tube cover to which it can be fixed. This way, we can introduce the sample into the salt at the desired height. We also had a bigger holder made of steel to introduce the sample. However, the former holder is preferable because, having less mass, it disturbs less the temperature of the salt when immersed. Indeed, we observed that ion exchange was more uniform in test samples made with the wire holder than in the ones made with the steel one. In the latter case, the effective index of flat waveguides varied between the two sides of the glass, as well as between the center and edges of each surface.

The process of ion exchange begins by introducing the tube with the wished salt into the furnace. Then, the wanted temperature is introduced in the controller, which starts to heat up the furnace. Between 1 and 2 hours are needed until the furnace reaches the set temperature and the salt is fully molten. Once the temperature is stabilized, the sample is introduced in the salt for the amount of time required. In some cases, the sample is situated first at 10 cm over the molten salt in order to do a warm-up before fully immerse it. This is done by two reasons. First, the warm up prevents a thermic shock when the sample is submerged into the molten salt, that can cause glass breakage. Second, it also reduces the temperature disturbance in the salt, or even its solidification around the glass, during the submersion.

Finally, after the sample has been submerged long enough in the molten salt, it is extracted. Cooling it down too quickly by immersing it in water would also cause a thermic shock and break the glass. This is avoided by shaking a bit the sample over the tube, which also allows some salt to be recovered by dripping. After a brief time, the remaining salt on the glass solidifies over it. After waiting another minute, the sample is washed with hot water to remove salt remains and then submerged into cool water to cool it down. Finally, the sample is dried with pressurized air.

In summary, the ion exchange process consists of the following steps:

- Furnace preheating up to the working temperature T_w.
- Placement of the glass at approximately 10 cm over the salt for 5-10 min. (optional)
- Immersion of the glass into the salt mixture for the time of diffusion t_{diff}.
- Glass extraction, cooling in water and drying.

4.2.1.3 Selection of the fabrication parameters by planar waveguides

Our objective is to get monomode channel waveguides. Assuming the effective index approximation, this requires that the waveguide presents only one mode in each dimension. The condition of getting a mode in depth can be studied in planar waveguides, while the condition in the perpendicular direction must be simulated.

The working substrate where we are going to make our IQPs consists of soda-lime glasses, commonly used as microscope slides. Despite being commercial glasses, which supposes a quite low cost, they are required to meet certain conditions of homogeneity of index and flatness that are enough to achieve our purposes. Their high content of Na^+ ions (approximately 15% in Na_2O) also makes them suitable for ion exchange, since these ions have a considerable mobility at high temperatures and are exchanged with doping ions such as Ag +, K +, etc. One last advantage these substrates have is the ease with which they can be cut and polished with conventional techniques explained later, in order to achieve samples of suitable sizes where the IQPs are located. Specifically, we employed glasses of the brand *Gold Seal* ® of dimensions $75\times25\times1$ mm^3 to fabricate our IQPs by ion exchange.

Before beginning with thermal diffusion in our IQPs, it was necessary to choose the right salt to employ, as well as, the appropriate parameters of temperature (T_w) and diffusion time (t_{diff}) in order to achieve monomodal waveguides. Several thermal diffusions in test glasses were made with this purpose. In this way, planar waveguides were obtained, which are easy to characterize. The effective index of the different modes of the waveguide were measured by prism coupling (also known by *M-lines method*), which was done with an automated system called *Metricon* (Model 2010/M) [Metricon-Corporation,]. In this system, samples are placed in contact with the base of a prism. A beam of light hits another side of the prism and it is reflected towards a photodetector. By rotating the system, for certain angle light is coupled inside the planar waveguide of the glasses, leading to a decrease in the intensity of light detected. From these angles, the effective index is calculated. This method is fast, precise and non invasive and also allows to get the depth of the waveguide. [Tien and Ulrich, 1970, Ulrich and Torge, 1973]

To begin with our testing process we start to employed a previously employed process that makes use of an eutectic salt mixture composed of 3% $AgNO_3$, 55% KNO_3, 26% $Ca(NO_3)_2$ and 16% $NaNO_3$ in weight, whose melting temperature is $T_m \approx 140$°C. The parameters used to make tests with this salt were a furnace temperature about $T_w = 30°$ C and a diffusion time of $t_{diff} = 30$ min. Silver was initially chosen over potassium because the latter presents anisotropic effects. Nonetheless, we ended using potassium as well to produce IQPs for reasons that will be explained later.

Several tests were made changing different parameters like times or holders. To begin, we check what holder to utilize between a steel one or a wire one. The former protects more the glass, but its bigger mas disturbs the salt temperature more than the latter. Effectively, with the first one, we observed large variations of the effective indexes between both sides of each sample, as well as smaller, but significant variations, from

the center to the sides of each surface of the glass. This did not happen with the wire holder, so we proceeded to use the wire holder in the following proves. However, the greatest problem observed in all of our testing was a lack of reproducibility, this is, two planar waveguides fabricated under the exact same conditions gave different results. In particular, we measured variations of $\Delta n_{eff}^{rep} \approx 0.002 \pm 0.0013$, which represents a high value considering the effective indexes we will need. This lack of reproducibility can be a serious problem when ion exchange is done to our IQPs, as it would be difficult to control the number of modes inside them. For this reason, it was decided to change the silver salt mixture to try to solve this.

4.2.1.3.1 Silver salt characterization

The next salt employed was a mixture composed of 0.05% $AgNO_3$ and 99.95% $NaNO_3$. The lower silver content in the salt results in a lower refractive index change. Therefore, the allowed range of effective indexes and their dispersion is expected to be reduced accordingly. Tests done with this mixture resulted, not only, in a high reproducibility (identical to the four decimal order), but the observed variation along the glass surface, and even between sides, was about $\Delta n_{eff}^{surf} \approx 0.0001$. Thus, all mayor problems encountered before were solved.

Table 4.1: Salt characterization. Number of modes, Δn and penetration depth in function of time.

t (min)	Modes	Δn (10^{-3})		d (μm)		$n_{eff} = 1.51$XX							
		Gauss	erf	Gauss	erfc	1	2	3	4	5	6	7	8
5	1	-	-	-	-	05							
10	1	-	-	-	-	11							
15	1	-	-	-	-	18							
20	1	-	-	-	-	24							
26	1	6.134	8.307	3.444	4.060	28	00						
30	2	6.821	9.245	3.245	3.819	31	01						
35	2	6.735	8.942	3.537	4.257	33	03						
40	2	6.744	8.883	3.654	4.436	34	04						
60	2	6.812	8.655	4.311	5.473	39	10						
120	3	7.153	8.722	5.922	7.876	49	23	07					
180	4	7.255	8.750	6.934	9.257	53	29	13	02				
300	5	6.992	8.279	9.088	12.454	55	36	21	10	03			
420	6	7.311	8.571	10.47	14.515	60	42	28	17	08	02		
900	8	7.745	8.911	14.754	21.131	68	54	42	32	23	16	10	04

The melting temperature for this salt is $T_m \approx 307$°C. As a consequence of the bigger melting point, we end up setting our working temperature to 330°C. The glass drying step was mostly removed. To characterise our salt at such temperature, we realized several ion

exchange process at different times and we measured the number of modes employing the Metricon. With our measures, it is possible to estimate the values of the index increase Δn and depth d of the planar waveguide [Montero-Orille et al., 2013]. This data is shown on Table 4.1, while the evolution of the number of modes and their effective indexes is shown in figure 4.2.5(a).

4.2.1.3.2 Potassium salt characterization

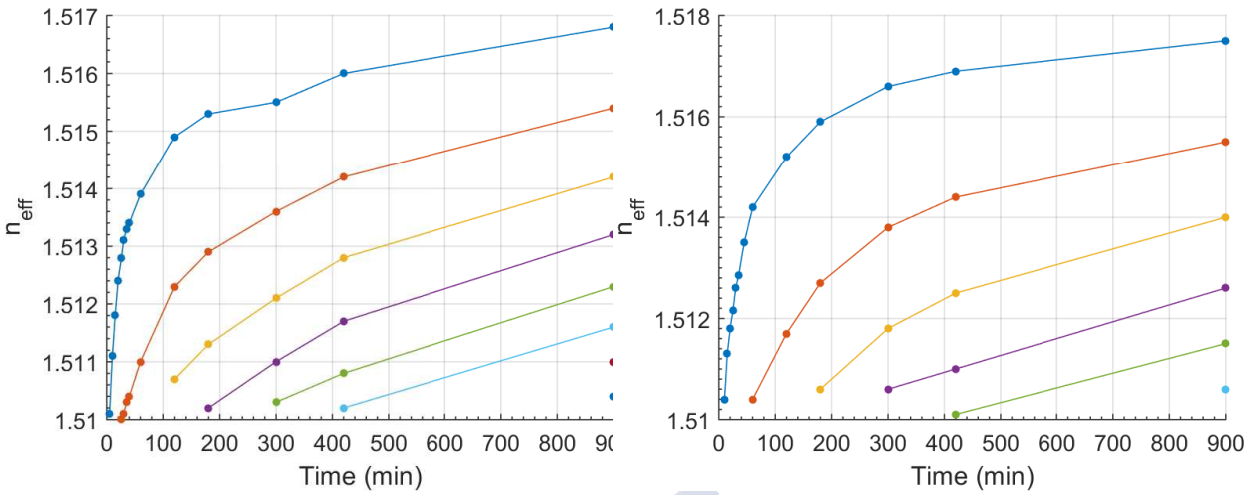
Although the previous silver nitrate salt mixture gave us good results in the diffusion step, certain problems arose during the waveguide characterization step and the coupling experiment, which would be explained latter. This leaded us to change our salt for a pure salt of potassium nitrate (KNO_3), despite the fact that potassium generates anisotropy in the diffused waveguides. As the melting point of KNO_3 is at $T_m \approx 334$°C, the new working temperature was set to 400°C. After several tests of reproducibility and uniformity for potassium at this working temperature, we proceeded with an identical salt characterization like the one for silver. The different modes in function the diffusion time are shown in Table 4.2 and represented in Figure 4.2.5(b). The estimated values of the index increase Δn and depth d of the planar waveguide are also calculated in the table.

Table 4.2: Potassium salt characterization for polarization mode TE. Number of modes, Δn and penetration depth in function of time.

t (min)	Modes	Δn (10^{-3})		d (μm)		$n_{eff} = 1.51$XX					
		Gauss	erf	Gauss	erfc	1	2	3	4	5	6
5	0	-	-	-	-	-					
10	1	-	-	-	-	04					
15	1	-	-	-	-	13					
20	1	-	-	-	-	18					
25	1	-	-	-	-	22					
30	1	-	-	-	-	26					
35	1	-	-	-	-	29					
45	1	-	-	-	-	35					
60	2	8.510	11.27	3.156	3.804	42	04				
120	2	8.560	10.68	4.214	5.484	52	17				
180	3	8.750	10.74	5.130	6.740	59	27	06			
300	4	8.850	10.59	6.687	9.068	66	38	18	06		
420	5	8.880	10.57	7.620	10.306	69	44	25	10	01	
900	6	8.910	10.38	10.639	15.003	75	55	40	26	15	06

4.2.1.3.3 Effective index analysis

In figure 4.2.5, we can see how n_{eff} of the different modes evolves with the diffusion time. As time grows, the effective index of each mode must tend to a limit value. This limit



(a) (b)

Figure 4.2.5: Experimental evolution of n_{eff} in function of time for the different modes and for the silver (a) and potassium (b) salts. Lines are guides to eye.

corresponds to the maximum value of the index profile of the waveguide; the difference between this value and the substrate index n_s is our index change $\Delta n = n_{max} - n_s$.

The first mode index seems to tend to $n_{max} \approx 1.517$ for silver and to $n_{max} \approx 1.518$ for potassium. This coincidence is partially intentional, as the working temperature for K^+ (400°C) was set in order to achieve similar effective index of the fundamental mode, than that in Ag^+, for the same diffusion time ranges where only one mode appears. We can see how potassium presents a lower number of modes than silver, taking more diffusion time for them to appear. In fact, we observe in both, figures and tables, that the first mode is already present at 5-10 min of thermal diffusion for both salts, while the second one does not appear until clearly surpassed 26 min in silver and 60 min in potassium. Thus, these are the time intervals within which we worked for making the ion diffusion in our IQPs in order for them to be monomode.

4.2.1.3.4 Index profile characterization

Employing the experimental effective indexes it is possible to theoretically calculate the index profile of the waveguide, which is proportional to the percentage of ionic exchange Ag^+/Na^+, given by a non linear ionic diffusion equation [Najafi, 1992, Liñares et al., 1994, Liñares et al., 2000]. The index profile in depth of the planar waveguide can be mathematically modelled as follows

$$n(x) = n_s + \Delta n\, f\,(x/d)\,, \tag{4.2.25}$$

where $n_s = 1.51$ is the substrate index, Δn is the index change, d is the penetration depth and the function $f(u)$ can be approximated by a gaussian ($\exp\{-(x/d)^2\}$) or a

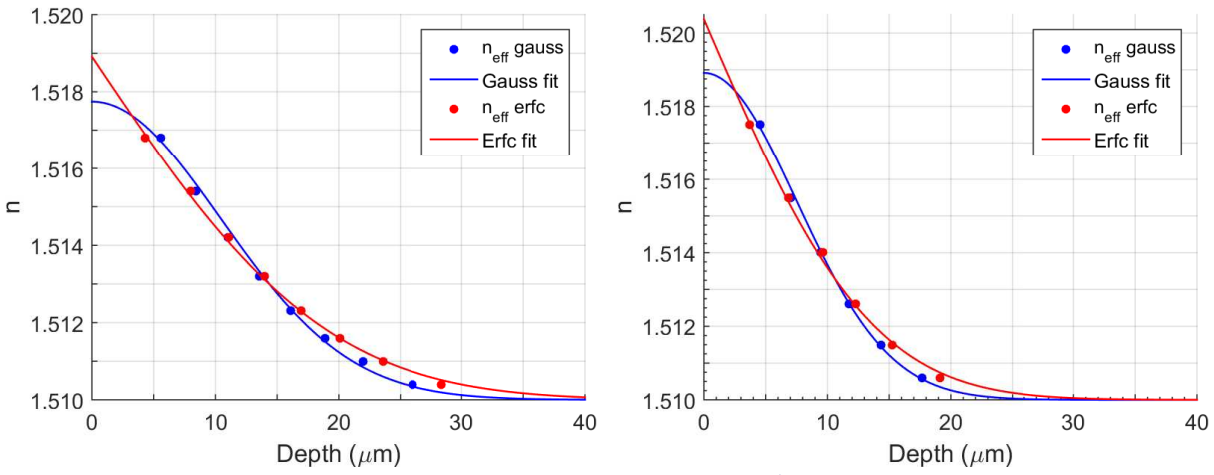


Figure 4.2.6: Gaussian and complementary error function fitting of the planar waveguide index n in function of its depth d for the silver (a) and potassium (b) salts.

complementary error function (erfc $\{x/d\}$). Note that the values of d for each function are not comparable. In Tables 4.1 and 4.2, we show the results of fitting parameters for each test, while the index profile is represented in figure 4.2.6 for the last row of said table, which has the greater number of modes.

Table 4.3: Index change.

Δn (10^{-3})	Silver	Potassium
Gauss	7.745	8.914
Erfc	8.911	10.380

Therefore, our index changes are shown in Table 4.3. Both values are similar, as we wanted, which allows, together with a temperature adjust, similar diffusion times to obtain the desired effective index n_{eff}. However, in the case of silver, it is of the utmost importance to note that silver ions concentration in the salt mixture is quite low (0.05%). This resulted in the decrease of said value with several thermal diffusions, as the Ag^+ concentration in the mixture lowers with each diffusion and this decrease can be appreciated after a certain number of diffusions. As a consequence, the times required to obtain a single mode of an specific index (shown in Table 4.1) were increased after a certain number of diffusions. This was easily checked by making a test before implementing thermal diffusions to each series of IQPs.

4.2.2 Design of IQPs

As we have explained in previous subsections, our IQPs are fabricated in glass through an ion exchange process. This process, explained in previous subsection 4.2.1, modifies the refractive index inside the glass when it is submerged into a salt mixture at a high temperature, as a consequence of the ion exchange between the glass an the salt. Thus, a waveguide is generated in the glass. With purpose of ensuring a selective exchange that creates channel waveguides in the glass, a photomask over it to act as a shield is required; that is, a metal layer with our IQP design imprinted in it. This photomask is fabricated through the lithographic process explained in subsection 4.2.3.

Now, we are going to proceed to explain the selection of the right diffusion times to achieve mono-modal waveguides, as well as the design of our IQPs photomasks.

4.2.2.1 Design parameters for ion exchange

4.2.2.1.1 Effective index and WKB approximation

Starting from Maxwell's equations it is trivial to obtain the classical wave propagation equation [Born and Wolf, 1999], which is

$$\nabla^2\mathbf{E}_r - \nabla\left(\nabla\mathbf{E}_r\right) + \omega^2\mu_0\epsilon_0 n^2\mathbf{E}_r = 0. \tag{4.2.26}$$

Searching solutions for (4.2.26) of the form

$$\mathbf{E}_r = \mathbf{E}_0 e^{-ik_0 n_{eff} z}, \tag{4.2.27}$$

where $k_0 = \omega\sqrt{\mu_0\epsilon_0}$. Considering, for simplicity, the case for transverse electric mode (TE), that is, $E_{0y} \neq 0$ and $E_{0x} = E_{0y} \neq 0$, we obtain the following Helmholtz equation

$$\frac{d^2E_{0y}}{dx^2} + \frac{d^2E_{0y}}{dy^2} + k_0\left[n^2(x,y) - n_{eff}^2\right]E_{0y} = 0. \tag{4.2.28}$$

This equation is similar to the Schrödinger equation, so it is evident that the effective index n_{eff} has a discrete range of possible values, this is, there is a discrete number of transmitted modes.

Now, we can apply an effective index approximation [Sammut and Pask, 1991, Liñares et al., 2001, Hammer and Ivanova, 2009] in order to decompose the 2-dimensional equation (4.2.28) in two 1-dimensional equations. This approximation considers that $\frac{\partial n^2(x,y)}{\partial y} << \frac{\partial n^2(x,y)}{\partial x}$; so, the index can be supposed to depend on the depth alone $n^2(x,y) \approx n^2(x)$, while the index in the transversal y direction is taken constant being the effective index of the planar case. Thus, considering a solution of the form $E_{0y}(x,y) = E_{0y}^{(x)}(x,y)E_{0y}^{(y)}(y)$, equation (4.2.28) can be decomposed in the following equations

$$\begin{aligned}
&\frac{\partial^2E_{0y}^{(x)}(x,y)}{\partial x^2} + k_0\left[n^2(x,y) - n_{eff,x}^2(y)\right]E_{0y}^{(x,y)}(x) = 0,\\
&\frac{\partial^2E_{0y}^{(y)}(y)}{\partial y^2} + k_0\left[n_{eff,x}^2(y) - n_{eff}^2\right]E_{0y}^{(y)}(y) = 0,
\end{aligned} \tag{4.2.29}$$

where $u = x, y$, $n(u)$ and $n_{eff,u}$ are the index and effective index respectively in each 1-directional problem, and n_{eff} is a constant.

Now, the WKB (Wentzel, Kramers, Brillouin) [Wentzel, 1926, Kramers, 1926, Brillouin, 1926] approximation searches for a solution of the 1-dimensional equations (4.2.29) of the form

$$E_{0y}^{(u)} = \exp\left\{i\left[k_0 S_0(u) + S_1(u) + S_2(u)/k_0 + S_3(u)/k_0^2 \cdots\right]\right\}. \tag{4.2.30}$$

Taken into account only the two first terms that give information about the phase and amplitude, the TE field is approximated as

$$E_{0y}^{(u)} = \frac{A \exp\left\{\pm i k_0 \int \sqrt{n^2(u) - n_{eff,u}^2}\, du\right\}}{\left(n^2(u) - n_{eff,u}^2\right)^{-\frac{1}{4}}}. \tag{4.2.31}$$

4.2.2.1.2 WKB analysis of fabrication parameters

Let us suppose that we have a planar waveguide made by three different regions, cover, waveguide and substrate, whose refractive indexes are n_c, n and n_s respectively. Light is going to be trapped in the middle region and is going to be propagated in it by continuously reflecting on the separation surfaces between regions. Thus, the electric field is described by two planar waves in the middle region and by evanescent ones in the other regions. This means the existence of four different free constants in the solution, that can be calculated by applying continuity and differentiability conditions in the limits between regions. This is possible only under certain values of n_{eff} and, which are going to be given by the following phase condition

$$k_0 d \sqrt{n^2(x) - n_{eff}^2} - \phi_c - \phi_s = m\pi, \tag{4.2.32}$$

where $m = 0, 1, 2$ is the mode number corresponding to that n_{eff}, s is the depth and ϕ_c and ϕ_s are the phases of the side regions, which are given by

$$\phi_c = \arctan \sqrt{\frac{n_{eff}^2 - n_c^2}{n^2 - n_{eff}^2}}, \quad \phi_s = \arctan \sqrt{\frac{n_{eff}^2 - n_s^2}{n^2 - n_{eff}^2}} \tag{4.2.33}$$

If we have a gradual index (GRIN) waveguide, like in our case, expression (4.2.32) must be modified. In particular, for a superficial waveguide, the index of the waveguide $n(x)$ is now given by equation (4.2.25) and the phase of this middle region must be integrated from the waveguide surface to the so called turning point, that is, the coordinate $x = x_r$ that verifies $n(x_r) = n_{eff}$. Now, there is not a discontinuity in the refractive index, and, in consequence, the phase of the substrate ϕ_s is not exactly given by expression (4.2.33). However, this phase can be obtained through different methods

of joining the field solutions of the waveguide and substrate [Galindo and Pascual, 1989]. All methods lead to $\phi_s = \pi/4$. Therefore, the WKB equation becomes

$$k_0 \int_0^{x_r} \sqrt{n^2(x) - n_{eff}^2} dx = m_x \pi + \frac{\pi}{4} + \arctan \sqrt{\frac{n_{eff}^2 - n_c^2}{n^2(0) - n_{eff}^2}}, \tag{4.2.34}$$

where $n(x_r) = n_{eff}$ and $m_x = 0, 1, 2 \cdots$. Considering equation (4.2.25), the return point x_r is given by

$$x_r = d\, f^{(-1)} \left(\frac{n_{eff} - n_s}{\Delta n} \right), \tag{4.2.35}$$

where $f^{(-1)}(u)$ is the inverse of function $f(u)$, which could be a Gaussian or a complementary error function approximation, and so, it is given by expressions $f_{gauss}^{(-1)}(u) = \sqrt{-\ln u}$ and $f_{erfc}^{(-1)}(u) = \mathrm{erfc}^{-1}(u)$. In the case that the GRIN waveguide is buried under the glass surface, the integral must be done between the two return points, that is in the region accessed by the ray that predicts the geometric optics. and both phases resulted from evanescent fields are $\phi_c = \phi_s = \pi/4$. Thus, equation (4.2.34) will turn into

$$k_0 \int_{x_{r0}}^{x_{rf}} \sqrt{n^2(x) - n_{eff}^2} dx = m_x \pi + \frac{\pi}{2}. \tag{4.2.36}$$

In any case, the limit situation where mode m_x starts to be propagated in the waveguide happens when the effective index of said mode is equal to $n_{eff} = n_s$ cut-off condition.

Now, in our case, we want to obtain monomode channel waveguides. In this case, the index of the waveguide $n(x, y)$ is function of x and y, that is, the depth and transversal directions. This adds a new problem because a different number of modes can be allowed in the different directions (assuming effective index approximation). In other words, although we diffuse a waveguide for a short enough time to obtain a single mode in x-direction, which according to Table 4.1 must be $t < 26$ min, more modes can actually appear in the waveguide because they are allowed in the y-direction. It is required, then, to obtain an upper bound of the diffusion time to avoid this problem by finding a limiting planar index n_{eff}.

Let us suppose that the index is given by

$$n^2(x, y) = n_s^2 + \Delta n f(\frac{x}{d}) g(y), \tag{4.2.37}$$

being $f(\frac{x}{d})$ the same than in expression (4.2.25) and $g = \mathrm{erf}\left(\frac{y+s_w/2}{d}\right) - \mathrm{erf}\left(\frac{y-s_w/2}{d}\right)$, with s_w, the width of the waveguide [Liñares et al., 2001]. The WKB method in direction y can be analyzed considering the parameter x constant with the grounded equation (4.2.36) as

$$k_0 \int_{-\frac{s_w}{2}}^{\frac{s_w}{2}} \sqrt{n^2(y) - n_{eff,y}^2} dx = m_y \pi + \frac{\pi}{2}, \tag{4.2.38}$$

where $m_y = 0, 1, 2$ is the mode number in direction y and n_{eff} is the effective index. Under the effective index approximation (4.2.29), we can approximate $g(y) \approx \text{rect}(\frac{y}{s_w})$, with the index in direction y being the effective index of the planar (depth) case: $n(y) = n_{eff,x}$ if $\|y\| < s_w/2$ and $n(y) = n_s$ if $\|y\| \geq s_w/2$. Therefore, considering the limit case for which the second mode $m_y = 1$ appears ($n_{eff} = n_s$), equation (4.2.38) becomes

$$k_0 s_w \sqrt{n_{eff,x}^2 - n_s^2} = \frac{3\pi}{2}, \tag{4.2.39}$$

It is important to note that lateral diffusion during ion exchange also occurs, which means that the exchanged zone extends below the mask as well. This lateral penetration of ions is of the same order of the depth of the diffusion d. Therefore, if we design a channel waveguide mask with size s_m, the final width s_w of the waveguide can be approximated by $s_w = s_m + 2d$. Therefore, we can employ equation (4.2.39) to calculate an approximate relationship between depth d and the planar refractive index $n_{eff,x}$

$$d = \frac{3\lambda_0 - 4s_m\sqrt{n_{eff,x}^2 - n_s^2}}{8\sqrt{n_{eff,x}^2 - n_s^2}}. \tag{4.2.40}$$

Introducing this $d(n_{eff})$ into the index expression (4.2.25), we can employ equation (4.2.34) for the fundamental mode $m_x = 0$ to calculate the upper limit of n_{eff} planar, and so the diffusion time, to obtain monomode channel waveguides. In our case, the waveguides are designed to work with the red wavelength of a He-Ne laser $\lambda_0 = 633$ nm. As was mentioned in subsection 4.2.1.3, the refractive index of the glass substrates employed was measured with the Metricon to be $n_s = 1.5100$, while the refractive index of the cover is the index of the air $n_c = 1$.As the value of the index change Δn in equation (4.2.25), we can use the fitted values of Tables 4.1 and 4.2: $\Delta n_{gauss}^{Ag} = 0.00774$, $\Delta n_{erfc}^{Ag} = 0.00891$, $\Delta n_{gauss}^{K} = 0.00891$ and $\Delta n_{erfc}^{K} = 0.01038$, depending on the approximation function employed and the salt used. Finally, the ideal waveguide width in the photomask must be low enough, at most of the same order as the depth, but not too much to avoid problems in the photo-reduction process, which act as limitations. Our reduction system allows to resolve waveguides of few μm, an thus, an ideal size taking into account the limitations is $s_m = 3$ μm. Therefore, calculating (4.2.34) for these values, we obtain the upper limit values shown in Table 4.4

Table 4.4: Upper limits of effective index and penetration depth of monomode waveguides.

	Silver		Potassium	
Function	n_{eff}	d (μm)	n_{eff}	d (μm)
Gauss	1.51163	1.884	1.51180	1.721
Erfc	1.51124	2.375	1.51139	2.160

Consequently, the upper effective index of the slab waveguide compatible with monomode channel waveguides is between $n_{eff} = 1.5112 - 1.5116$ for silver and $n_{eff} = 1.5114 - 1.5118$

for potassium. Similarly, the expected depth (and lateral extension) of our waveguides will be of about $d = 2$ μm for both salts. Regarding silver, observing the experimental values of Table 4.1 and figure 4.2.5(a), we see that the diffusion time needs to be lower than 15 min for a temperature of $T = 330$°C. As a high effective index minimize bent losses in the waveguide, we tried to achieve a diffusion just before the bimode cut-off condition, so, the ideal range of diffusion times to employ is between 10-15 min. Nonetheless, as a consequence of the low concentration of Ag ions (0.05%), Δn decreases after several samples have been diffused ($\Delta n \approx 0.007$). This leads to the increase of the required diffusion times and, at the same time, decreases the upper bound of the effective index to $n_{eff} = 1.5113$. Now, taking into account that several approximations were assumed in the above estimate, we also risked to obtain higher indexes of about $n_{eff} = 1.5120$. Thus, diffusion times up to 25 min were used. When using potassium instead, if we look into the values of Table 4.2 and figure 4.2.5(b), we see that the expected range of diffusion times to get a monomode waveguide is between 15-20 min.

4.2.2.1.3 Burying channel waveguides

Now, for the samples that are going to be subjected to a burial process, it is needed to use greater times, cause the burial tends to expand and reduce the index profile of the waveguide resulting in a lower effective index. Burial proves were made, always considering that we wanted the index to vary as lesser as possible. We observed that the burial in silver barely reduced the effective index of planar waveguides, with a reduction of about 12.5% for equal times of diffusion and burial at the same temperature. On the other side, for potassium the reduction reached values of about 50% for identical times. This different influence of the burial time between silver and potassium is consequence of the concentration. The lower concentration of silver results in a linear and slow decrease of the effective index with time, while, the high concentration of potassium ions leads to a non-linear decrease with time. Therefore, for silver we choose to use the same times for both diffusions, maintaining it at 25 min in the last samples, obtaining effective indexes of $n_{eff} = 1.5118$ after the first one and $n_{eff} = 1.5116$ after the second one. Meanwhile, for potassium the time of the first diffusion was raised to 30 min, while in the second diffusion a third was used (10 min). While the effective index obtained in the first diffusion was of about $n_{eff} = 1.5125$, it was reduced to $n_{eff} = 1.5116$ after the burial.

In conclusion, the main parameters employed in the ion exchange process of the main samples can be summed up as shown on Table 4.5

Table 4.5: Main parameters used to obtain the main samples analysed latter.

Salt	T (°C)	Superficial		Buried			
		t_{dif} (min)	n_{eff}	t_{dif} (min)	n_{eff}	t_{bur} (min)	n_{eff}
Silver	330	25	1.5118	25	1.5118	25	1.5116
Potassium	400	20	1.5116	30	1.5125	10	1.51165

4.2.2.2 Geometrical design of photomasks

Our final objective is to characterize directional couplers regarding their coupling length and the distance between both waveguides. For that, a set of couplers with different values of these parameters must be designed. Moreover, the reduction scale must be enough to pixelation and border roughness in the final mask mask be negligible, and the curvature of the sections that connect couplers must be low enough. Otherwise, scattering and bent losses will appear.

We must explain the design of our IQPs photomasks, which will be printed into regular paper and be subjected to lithographic process. As explained in subsection 4.2.3, it fundamentally involves a double photo-reduction process where the IQP design of several cm^2 is reduced to a motif of few μm^2 and printed into the metallic layer over the glass meant to be subjected to ion exchange. The magnification of the optical systems to perform the first and second photo-reduction are of $\times 14.11$ and $\times 5$ respectively as will be explained in subsection 4.2.3.4, and thus, this means that the lateral magnification of the entire process is of $M = 1/(14.11)(5) = 1/70.55$.

In figures 4.2.8 and 4.2.9 we show the designs of two IQPs patterns, labelled as AC1 and AC2 respectively. All designs were made using the vector graphics editor *Inkscape*. The size of AC1 is of 420×594 mm, while AC2 has a size of 320×594 mm. Trivially, this means a size of the final element of around 6×8.4 mm for AC1 and 4.5×8.4 mm for AC2. Both designs are similar. Black structures in the figures correspond to the metallic regions of the final photo-mask, while the white ones correspond to the regions of the final glass not protected with metal, and thus, the regions that are going to be diffused.

The basic design of the IQPs, which we can denominate IQP unit (see figure 4.2.7), consist of a set of 2-to-3 waveguides of size s_m with a coupler and a Y union. The Y union splits into two one of the initial two waveguides. The unsplit waveguide and one of the two split ones are approached, through curves following the Minford function ($y = \pm \Delta y \left[\frac{z}{L} - \frac{1}{2\pi} \sin\left(2\pi \frac{z}{L}\right)\right]$ with $0 \leq z \leq L$) [Salgueiro et al., 1998, Salgueiro-Piñeiro, 2001], forming a directional coupler (DC), and then are separated again through the same way. Minford curve has no curvature at the endpoints $z = 0, L$ where it meets straight sections, avoiding losses that occur at curvature discontinuities even if there is no direction change at these points. Meanwhile, the other split waveguide follows unaltered to work as a reference. The purpose of this design is to introduce light into the waveguide that goes to the Y union, where it is split 50%-50% between both waveguides. Light going to the coupler is going to be split between the waveguides in a certain way, while the light of the reference waveguide is going to be unaltered. Therefore it is possible to study how the coupler works by comparison.

Four IQP units, differentiated in the distance between the waveguides d_m of the DC are grouped in a block. In both designs we have four block of four units, with each block having a different coupler length l_m (straight section of the coupler). Two additional blocks with two linear waveguides each were placed at each side of the four main blocks of AC1 to serve as references. Meanwhile, in AC2, four couplers with the same waveguides

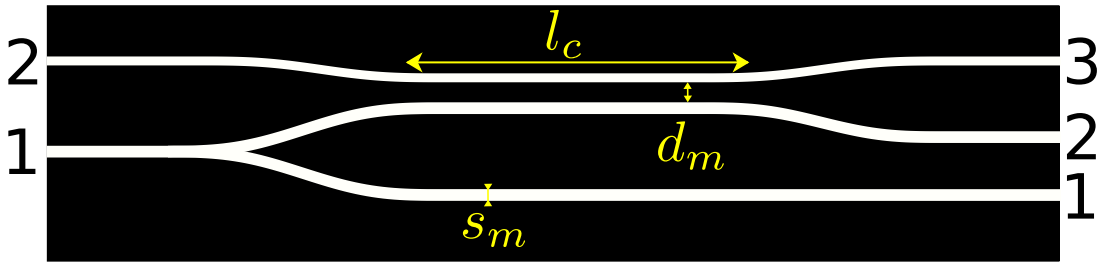


Figure 4.2.7: IQP unit.

distances d_m as before, but with the same length of the block (no curvatures), were added in these additional blocks. This results helpful to study the work of the couplers without bent losses in the curves that were observed experimentally in some samples.

The main parameters of these IQPs are summed up in Table 4.6. The size s_m of the waveguides in the AC1 and AC2 motifs was designed to theoretically obtain waveguides mask widths of 4 and 3 μm, respectively, in the final reduced photo-masks. The distances between the apertures of both waveguides of each directional coupler were set for obtaining final values between 5 and 11 μm in the AC1, and between 3 and 7.5 μm in the AC2. The interaction length of the couplers was also lowered for AC2, with theoretical reduced values between 0.5 and 2 mm, with respect to those of AC1, with final values between 1 and 3 mm. The lower distance between waveguides and their lower size in AC2 were motivated by an improvement in the resolution of the optical system for reduction. Meanwhile, the change in the lengths was a result of a decrease by a fifth of the original curvatures of the waveguides (as we can see in Table 4.7), in order to minimize bent losses that were observed in AC1 tests.

Table 4.6: IQPs parameters. First column (Original print) refers to the values of the printed design, while the second one are the theoretical final values in the photo-mask after a double photo-reduction of total increase 1/70.55. s_m is the waveguide sizes. Waveguide distances d_m vary between the four units of a same block, while interaction lengths l_m vary between blocks.

IQPs	Original print			Reduced photo-mask		
	s_m (mm)	d_m (mm)	l_m (mm)	s_m (μm)	d_m (μm)	l_m (mm)
AC1	0.27	0.37	80	4	5.5	1.1
		0.50	120		7	1.7
		0.62	160		9	2.3
		0.76	200		11	2.9
AC2	0.21	0.21	35	3	3	0.5
		0.32	70		4.5	1.0
		0.42	105		6.0	1.5
		0.53	140		7.5	2.0

In addition to this, we also shown in Table 4.7 the curvature parameters of the original design and of the final reduced photo-mask. These parameter consists of the width Δy and length L of the curve, and its radius of curvature, which depends from the others as $R_c = \frac{L^2}{2\pi\Delta y}$. Originally, in AC1, we designed our waveguides to obtain final radius of $R_c = 5$ mm. However, due to high losses observed in the final samples from this design, we choose to reduce the curvature to 20%, growing the radius proportionality, in our following design AC2.

Table 4.7: Minford parameters of the IQPs. Δy Minford constant. L length of the curve. R_c minimum radius of curvature.

IQPs	Original print			Reduced photo-mask		
	Δy (mm)	L (mm)	R_c (mm)	Δy (μm)	L (μm)	R (mm)
AC1	1.52	57	344	21.6	814	4.9
AC2	1.09	107	1683	15.4	1520	23.9

Finally, reference marks are added at the sides of the blocks of waveguides to works as references of the sample. First, four rules of about 84 mm were added at the corners of the design. The rules are designed for its lowest division corresponds to 0.1 mm in the final photo-mask, having a final size of 1.2 mm. These rules are going to be of great help for correct orientation of the sample during lapping and polishing process (subsection 4.2.4).Then, four complementary crosses are added to make a precise alignment of several samples for creating and stack (subsubsection 4.2.4.1). Last, two diffraction gratings of about 6 μm of period are placed at each side. The gratings act as test regions in the photoresist development step and can also help during alignment.

It is also worth noting that the design of AC1 is bigger (420 $\times$ 594 mm) than that of the AC2 (320 $\times$ 594 mm) because of bigger dimensions in the elements design, as was explained. This was a problem as the printer could not work with that width. For this reason, the design of AC1 was printed in two different sheets by a A4 printer (in banner mode) that were tied together afterwards. To help with this, reference cross marks were added to the design, as can be observed in figure 4.2.8. These reference marks were removed in AC2, since it was printed in a single sheet by a A3 printer that allows a paper size up to 320$\times$1200 mm^2.

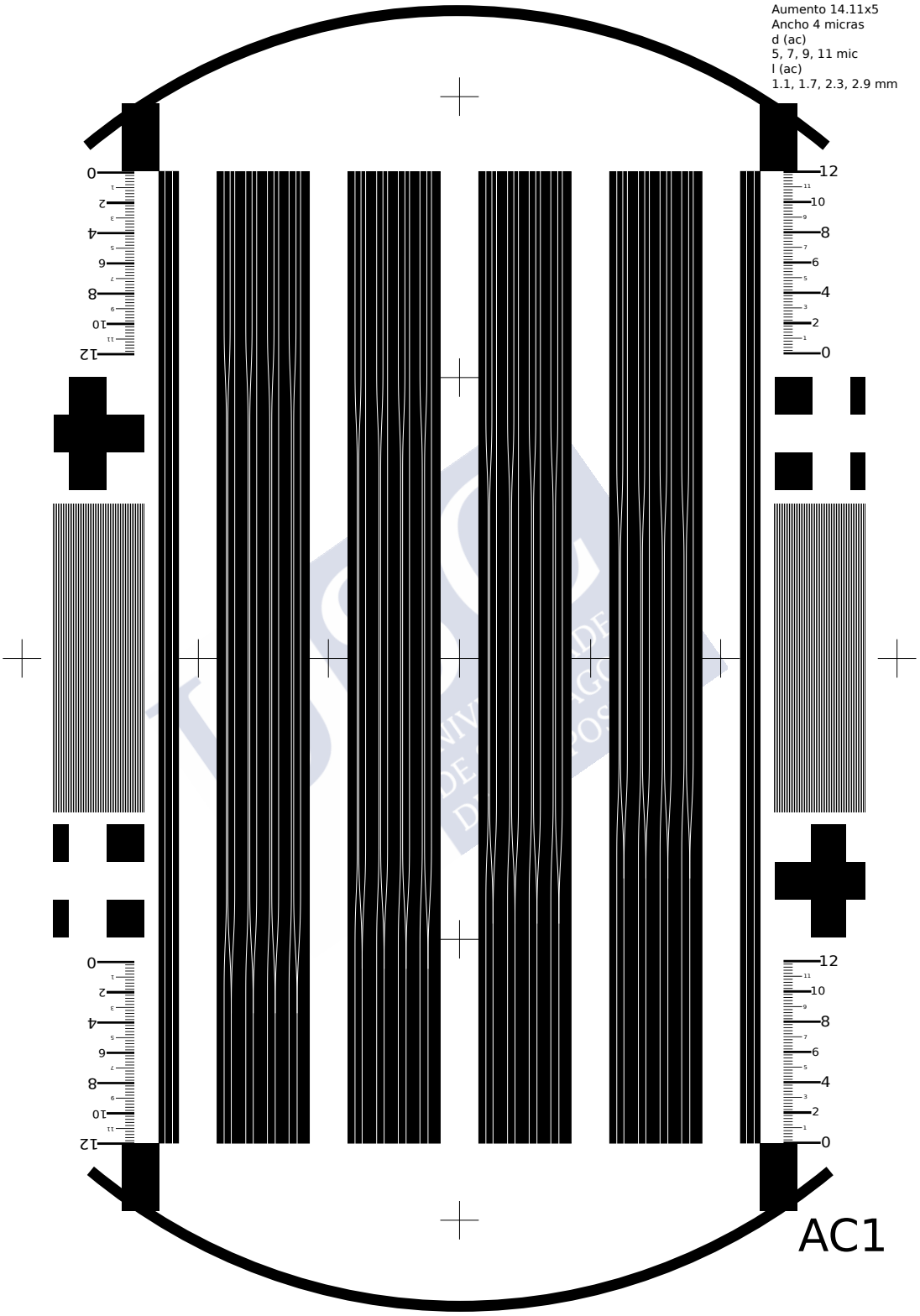


Figure 4.2.8: Design IQP AC1.

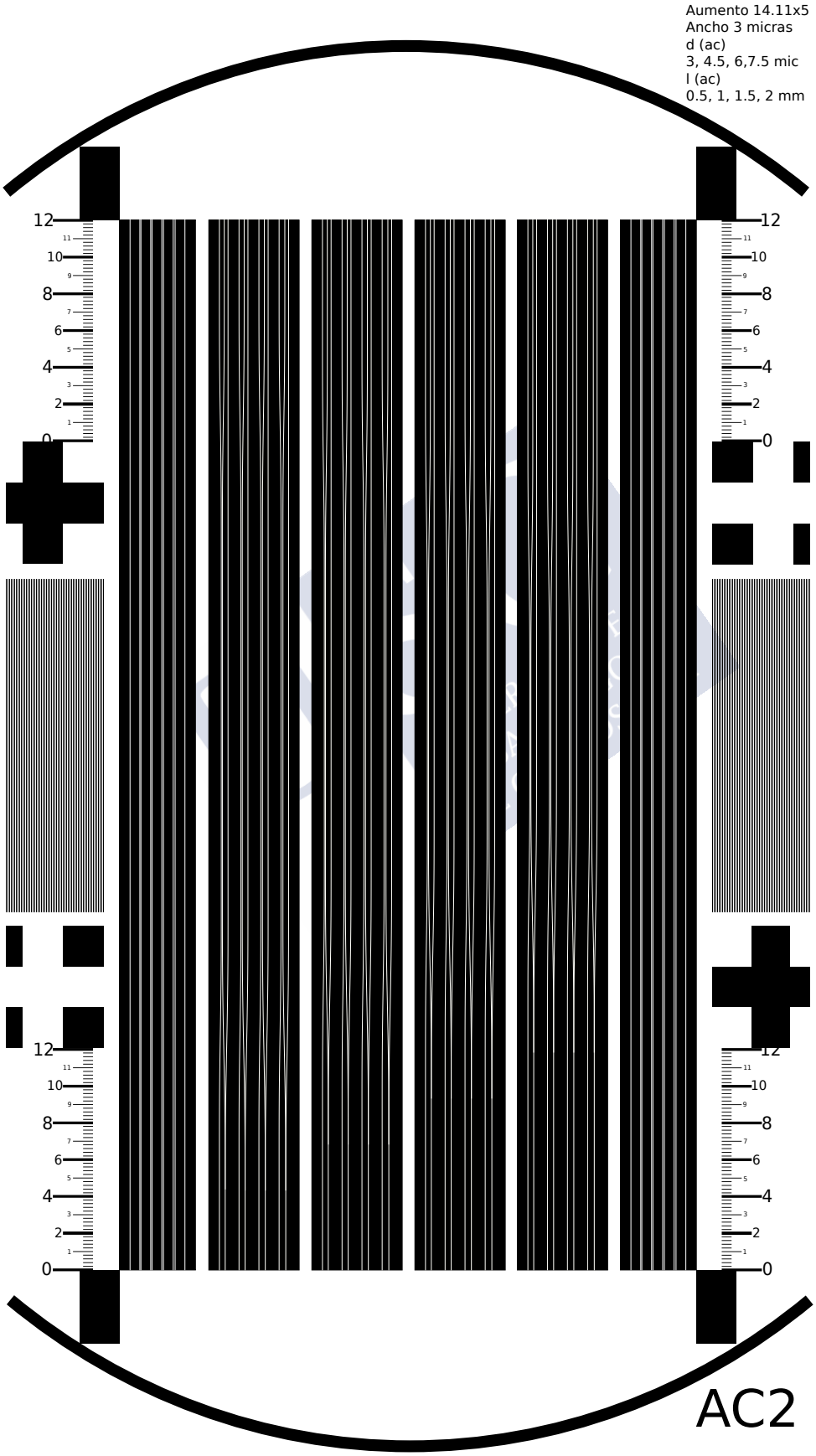


Figure 4.2.9: Design IQP AC2.

4.2.3 Fabrication of the metallic motifs of our IQPs

The fabrication process of metallic photomasks of our IQPs can be resumed in the following steps:

1. Cleaning of the glass that is going to be used for develop our IQPs.
2. Deposition of a metal layer through the Physical Vapour Deposition technique.
3. Deposition of a photoresist over the metallic layer by spin coating.
4. Exposition to light or ultraviolet radiation (UV) of the photoresist employing the design of our IQPs.
5. Development of the exposed photoresist.
6. Pattern transference to the metal layer through the use of a etching acid.
7. Removal of the photoresist by means of an organic dissolver (acetone).

The process is valid for generating both the intermediate and final metallic photomasks. The former being used as the original design for a second photo-reduction process to create the latter.

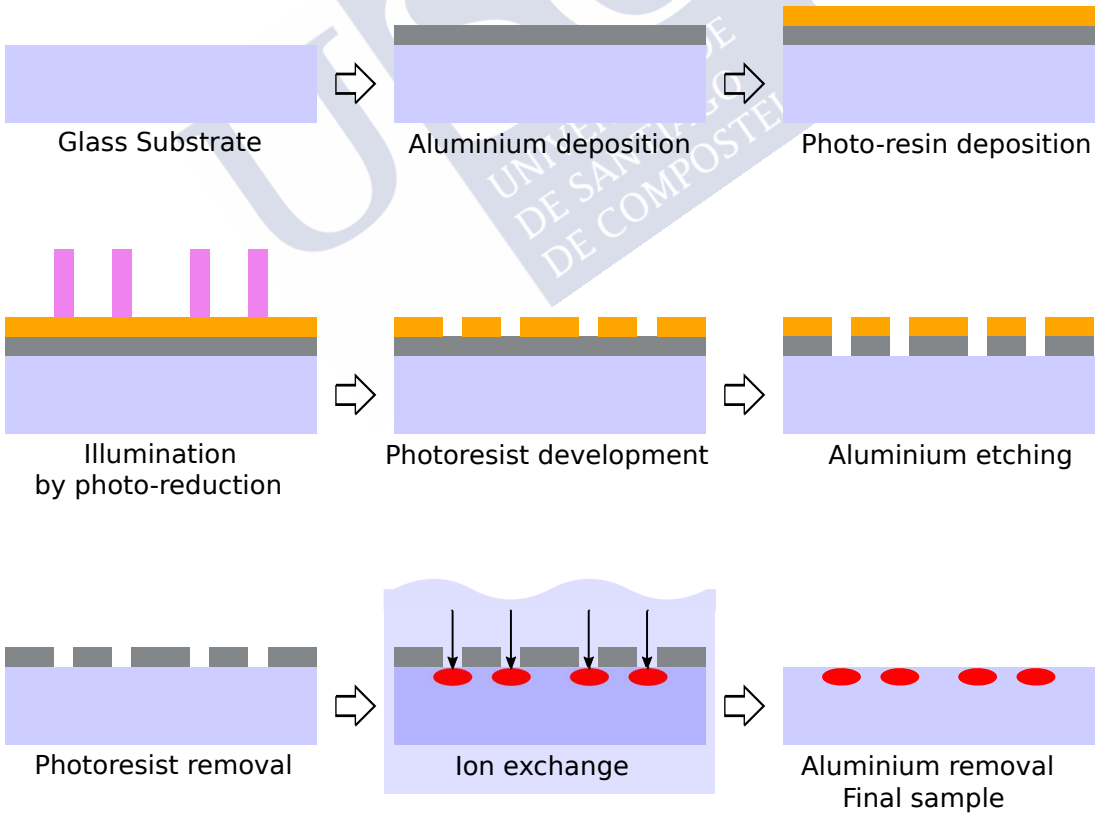


Figure 4.2.10: Photo-lithographic and ionic exchange processes.

4.2.3.1 Substrate cleaning

As previously explained, the substrates selected for implementing ion exchange are soda-lime glasses of the brand *Gold Seal* of dimensions 75×25×1 mm^3 (microscope object holder type). Additionally, glasses of dimensions 75×50×1 mm^3 from *Corning* were also used to create a metallic mask that works as an intermediate in the photo-lithography process (object of the second photo-reduction), as explained in the latter subsection 4.2.3.4.3.

The very first step in the fabrication process is the thorough cleaning of the glasses before the deposition, in order to prevent the appearance of pores in the metal layer due to dust in the glasses. This cleaning can be summed up as follows.

First, the glasses can be washed with scourer and commercial detergent and then rinsed with deionized water. Next, the glasses are washed with ultrasounds in deionized water for 30 min at 30°C and dried with compressed air. Finally, they can be washed again with ultrasounds (30 min at 30°C), but this time in isopropyl alcohol, and dryed again with compressed air.

Immediately afterwards, the metallic deposition must be done to prevent any grain of dust to land on the glass surface. Even with a deep cleaning, the presence of porosity is inevitable without a clean room and can reach values of 200 pores/cm^2 [Pantchev and Danesh, 1997]. We use a laminar flux chamber for the more delicate steps. Moreover, a domestic air cleaner reduces the air dust to 5% after 1 hour of work inside a well closed room.

4.2.3.2 Metal layer deposition

Next step is the deposition of a metallic layer over the glass. As it was explained, the purpose of this layer is to act as a barrier during ion exchange in order to guarantee that only the unprotected zone of the glass that constitutes our motif is diffused by cations. This zone is going to experiment an increase in the refraction index respect to the glass protected by the metallic layer.

In our case, we use mainly aluminium as mask material, which is also the most employed metal in literature along with titanium [Zhou and Duan, 2006]. In some tests, we also utilized chrome [1], but only to create intermediate metallic masks [2] or *master* masks. These last ones are employed to generate multiple copies in *Al* by contact lithography with UV. The advantage of chrome against aluminium is its higher scratch resistance and a an observed lower porosity during deposition, but it is not resistant to the salts used in ion exchange, being useless to create a final metallic photomask. Also, the adherence to the glass is poorer than that of *Al* and the mask tends to chip over time.

The metallic deposition over the glass is done by the method of evaporative deposition in "high" vacuum, which belongs to the set of vacuum deposition methods known as *Physical Vapour Deposition* (PVD). The technique consists of evaporating the metallic

[1] Chrome photomasks are widely used in the microelectronic industry.

[2] Used as the original design for a second photo-reduction.



(a) (b)

Figure 4.2.11: Two types of glasses employed in the fabrication process metallized with aluminium and covered by photoresist. (a) Slide of dimensions 75×25 mm. (b) Slide of dimensions 75×50 mm.

material by Joule effect, which is then condensed over the surface of the glass. All PVD methods are based on this last point, varying only in the way of turning the metal into gaseous state [Pulker, 1984].

Our depositions are made in a machine from *Balzers*, model *BAE 250 Coating System*. It consists of a water-cooled cylindrical chamber at whose bottom is placed the metallic material, in the form of small balls, into a tungsten bowl, while the glass substrates are placed in a holder at the top of the cylinder. Respect to its way of working, first, the air is extracted from the chamber until reaching pressures of $2 \cdot 10^{-5}$ mbar. Then, a high electrical current is applied to the bowl funding the metal in it. The vacuum allows for the metal atoms to reach without problems or oxidation the surfaces of substrates, where they are condensed upon impact. As each metal has an optimal deposition speed (5 nm/s for *Al*), a metallic barrier is situated over the bowl to prevent deposition and it is retired when the speed reaches that optimal value.

A sensor located at the top of the cylinder measures the thickness of the deposited metallic layer through the reduction in the vibration frequency of a crystal when metal is deposited in it. To ensure uniformity in the deposited layer, the holder for glass samples has a spherical shape whose center point is oriented downwards and rotates around the vertical axis of the cylinder. In this work, we have used thicknesses around 0.2 μm.

Finally, it is important to note that the metallic layer deposited in the interior walls of the cylinder must be removed and cleaned.

4.2.3.3 Photoresist deposition and development

A photoresist is a photo-sensible organic material that alters its chemical properties when exposed to certain wavelengths of light. It is used to imprint our IQPs design in it by forming image of the design over the resin. In our case, we employed the photoresist

Micro-posit S1813 from manufacturer *Shipley*, which is sensible in the wavelength spectral range from 350 to 450 nm, but, particularly, it is optimized for the G-line of mercury of 436 nm (blue-violet colour). It is composed of a phenol formaldehyde resin, a dissolver of it (Propylene glycol methyl ether or PGME) and a photo-sensible compound (diazonaphthoquinone or DNQ). The PGME gives the photoresist its viscous liquid state and evaporates during deposition leaving a solid layer. Meanwhile, the DNQ form hydrogen bonds with the resin preventing its solubility in the development step. However, the chemical properties of DNQ change after light exposure making the resin highly soluble in a base medium.

4.2.3.3.1 Photoresist deposition

The deposition of the photoresist over the metallized glasses was done by spin coating using a centrifuge from the manufacturer *Headway Research, Inc.* The glass is clamped by suction on a rotating support. A drop of resin is dropped over the metallized surface of the glass and then, a spin cycle is run reaching 5500 rpm for 30 s. Due to the spinning, the drop is extended over all the surface leaving a uniform film of thickness around 1-2 μm [3]. The spinning contributes as well to evaporate the dissolver PGME leaving the resin layer hardened.

Once the photoresist has been deposited, our prepared glasses must be inspected. A good uniformity and the absence of defects is crucial in the following process of exposition and development to achieve the better possible resolution of our motif. This can be checked by mere sample inspection under the yellow light of a sodium lamp observing the interference patterns over it. Observed defects can be marked in the opposite surface to that of the film, in order to determinate the better regions of the resin layer. Therefore, glasses with the best films must be employed for the exposition. The exposition step is going to be explained in detail in subsection 4.2.3.4.

4.2.3.3.2 Photoresist development

After the exposition of the sample, the latter must be developed. This is done by submerging the sample into a developer and shake it lightly. The higher the radiation dose was, the faster the sample is developed. In our case, we have used *Microposit Developer*, a developer from the same manufacturer as the photoresist, whose recommendation is a development between 40 and 60 seconds for a specific dose of 150 mJ/cm^2. If these times are surpassed, the non exposed photoresist starts to develop as well. In our case, as the dose is not easily controllable or measured, exposition times were adjusted by trial-error process to achieve development times of the same order.

It is important to note that, the smaller the details of the design are, more light is spread over the dark zones losing contrast and limiting resolution. This is in part corrected by the non linear behaviour of the resin, but, nonetheless, stopping development

[3] Over the edge of the glasses uniformity is lost due to air turbulence during spinning

at the right moment is still required. The development process is stopped by washing the sample in deionized water. To precisely control this stop we make the assumption that optimal development point happens when regions that received half the maximum dose are developed. For this reason, during exposition, a density scale glass was put at the motif that we wanted to photo-reduce as a reference for the development step. When the zone that received half the dose is fully developed, the process must be stopped. If by looking at the microscope we see that the development is still not optimal, the process can be reinitiated; although it is preferably to avoid this as it deteriorates the layer.

4.2.3.4 Photoresist exposition

One of the most important stages is the exposition of the photoresist with the design of our IQPs, for later being developed and then etched into the aluminium for ion exchange. To achieve this, we use a double photo-reduction method, or reduction lithography in two steps, that was developed in our Lab at the USC. Reduction technique uses an optical system to form a small image of high resolution from a motif of higher dimensions easier to make. Another lithography method based in laser writing was previously developed in the USC [Salgueiro-Piñeiro, 2001], but it is too slow to being used to fabricate our IQPs.

4.2.3.4.1 Printing the original design

Before starting with the photo-lithography, the design of our IQP must be printed. The IQPs were designed using a vector graphics editor like *Inkscape* as previously explained. The design is printed in glossy paper with a conventional laser printer of 1200 dots per inch. This value determines the precision of the center of a toner point, not the size of the printed one which can be of 75 μm. Thus, the smallest printed point is bigger than the theoretical pixel value of 21 μm and it clearly becomes a limiting factor of the resolution of the image that we are going to obtain when photo-reducing it. Moreover, the printed transition between black and white white regions sometimes presents a bias (around 1-2 pixels) respect to the design, resulting in wider waveguide openings than desired. The design had to be corrected accordingly. To obtain a high resolution that allows us to get waveguides of 3 μm, it is required to print the image in a size big enough. The roughness of border of a horizontal or vertical straight line is also about 20 μmin the original printed design, that is, it is similar in size to the pixelation effects occurring in a diagonal line. Both defects are detectable in the final mask, despite the pixel size becoming 0.3 μm. However, they are much lower than both the waveguide opening and the lateral diffusion, which smooths these irregularities along the waveguide borders. The reduction scale is also conditioned by lithographic optics, which is optimized for a narrow range of magnification. This obligates us to implement a double reductive lithography.

For printing the designs, two printers were used: a *Ricoh-SP-C410DN* and later a *Ricoh-SP-C840DN* that supports up to A4 and A3+ paper respectively. Both of them were used in "banner" mode. Some of the printings were made on sheets of dimension 330×594 mm, but others required a width bigger than the paper dimensions. The solution

to this is to print the design in half into two different sheets and then, tie them together, achieving a width of 420 mm. It is important that both sheets share a certain region of the design, where the cut is made, to correctly tie them. Reference crosses were added to the design in order to help with the alignment of the two sheets. In our case the cutting region is covered by crosses to not affect any of the waveguides of the design in any way. To prevent any lifting or moving of one sheet over the other, both of them must be adhered.

4.2.3.4.2 First photo-reduction

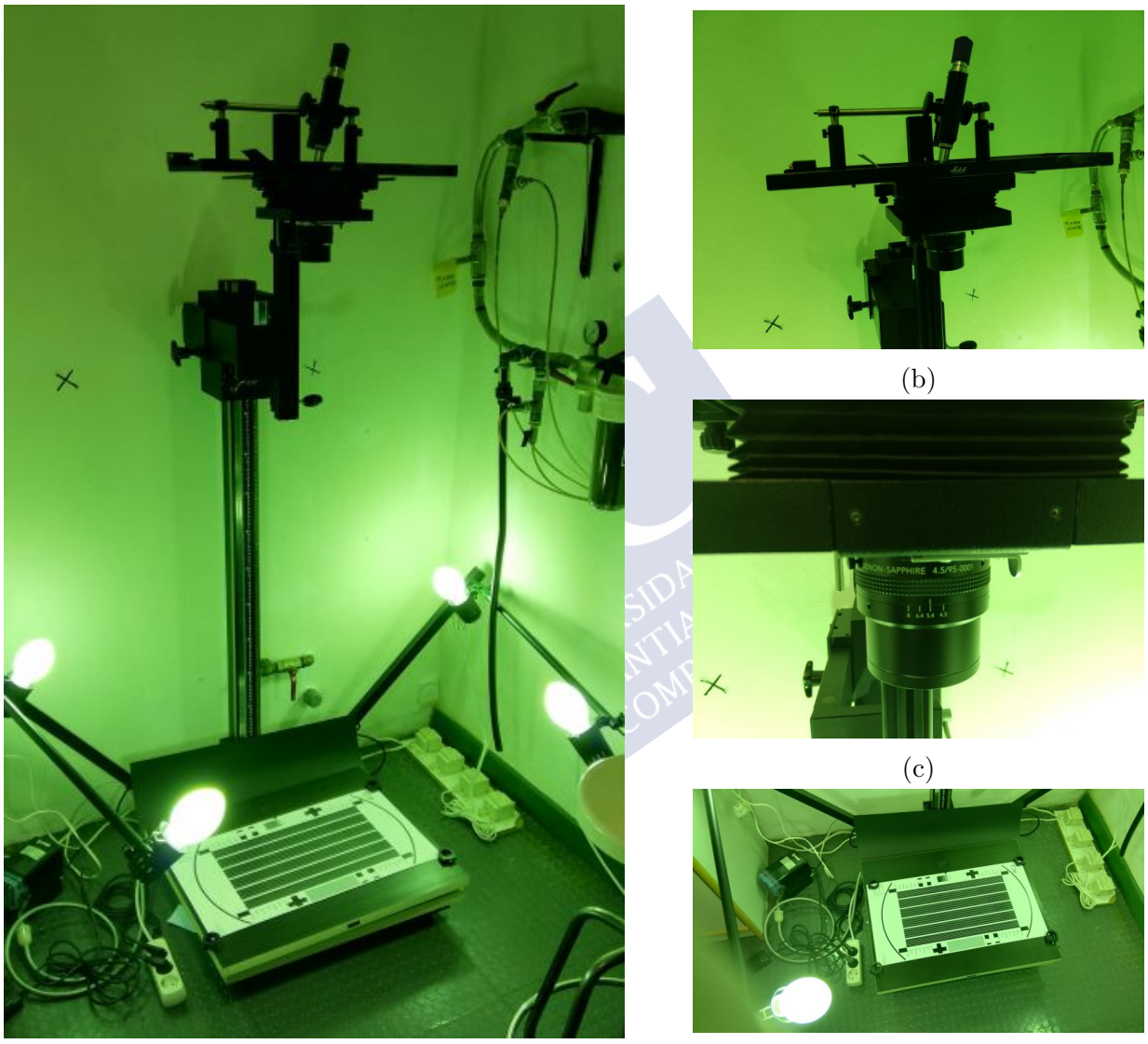
To implement the first photo-reduction, we make use of a photographic enlarger *Linhof* which is composed by an horizontal table of 510 mm × 630 mm, four lamp-holders uniformly distributed and an adjustable column where the reductive objective is situated in a conventional film reel system. In the table, the paper is fixed with help of a suction system. The paper is illuminated in a uniform way by four mercury lamps of 125 W placed in the lamp-holders. Reflected light from the paper is collected by a camera lens placed below the platform, following a vertical optical axis, which focus the image over said platform. The glass with photoresist is situated in this platform with resin placed down in order to be exposed by the image of the printed design. The height of the column can be freely adjusted to correctly focus the image with the appropriate size.

The objective utilized is an **Schneider Xenon-Sapphire 4.5/95 mm** from *Schneider-Kreuznach* which has an image field of 62 mm diameter, a modulation transfer function (MTF) of 80% of contrast for a spatial frequency of 36 line pair/mm (11 μm/pair) with white light at $f/5.6$ and a lateral magnification of $0.07\times$ $(-1/14.28)$ according to the manufacturer [Schneider-Kreuznach,].

To rightly focus the image over the photoresist of the sample, we make use of a small microscope and a marked auxiliary glass and we open the lens diaphragm at maximum to reduce spotlight background. Putting the auxiliary glass in place of the sample with its marked face pointing down. Comparing the reference marks with the image of the design, image focusing can be done. First, without moving the platform where glass and microscope are located, the height of the objective is adjusted in order to focus the image over the marks. Then, if our reference marks are rules, we can adjust the proper size of the image as wished by changing the object distance.This is done by moving vertically the entire system objective-platform.

Although lens diaphragm must be open for a better focusing, it is better to close it during exposition for two reasons. The first reason is to reduce vignetting, allowing for a uniform radiation dose in a big region. The second one is to optimize resolution, balancing diffraction and aberrations. In our case, we employed f-numbers between 4.75 and 5.6. They allow for an uniform radiation of more than 80% in a region of 5 cm and full field respectively.

This photo-reduction is done in glasses with 75×50 that will work as an intermediary photo-mask to implement a second photo-reduction. This first lithography was adjusted



(a) (b) (c) (d)

Figure 4.2.12: Experimental setup to implement the first reduction (a). (b) Microscope and platform for the sample. (c) Objective *Schneider Xenon-Sapphire* 4.5/95 mm (-0.07×). (d) Illumination system

to obtain a reduction of -1/14.11 within the optimized magnification range. In this way, the pixel printer pitch corresponds to 1.5 μm in the mask.

4.2.3.4.3 Second photo-reduction

To finally developing our wished IQPs, it was necessary to mount a secondary optical system to implement another different photo-reduction. This system was mount around the acquisition of an objective **Zeiss S-Planar 1.1 68mm**, with a f-number of 1.1 and a focal distance of 68 mm designed for monochromatic light of 435.8 nm. The numerical aperture for the optimized magnification of $-1/5$ is 0.35, while it has a MTF of 50-76% of contrast for a spatial frequency of 500 lp/mm with partially coherent illumination. This kind of objectives were originally designed for being employed in micro-lithography for the industrial fabrication of microelectronic integrated circuits [Glatzel, 1980, Ittner, 1977].

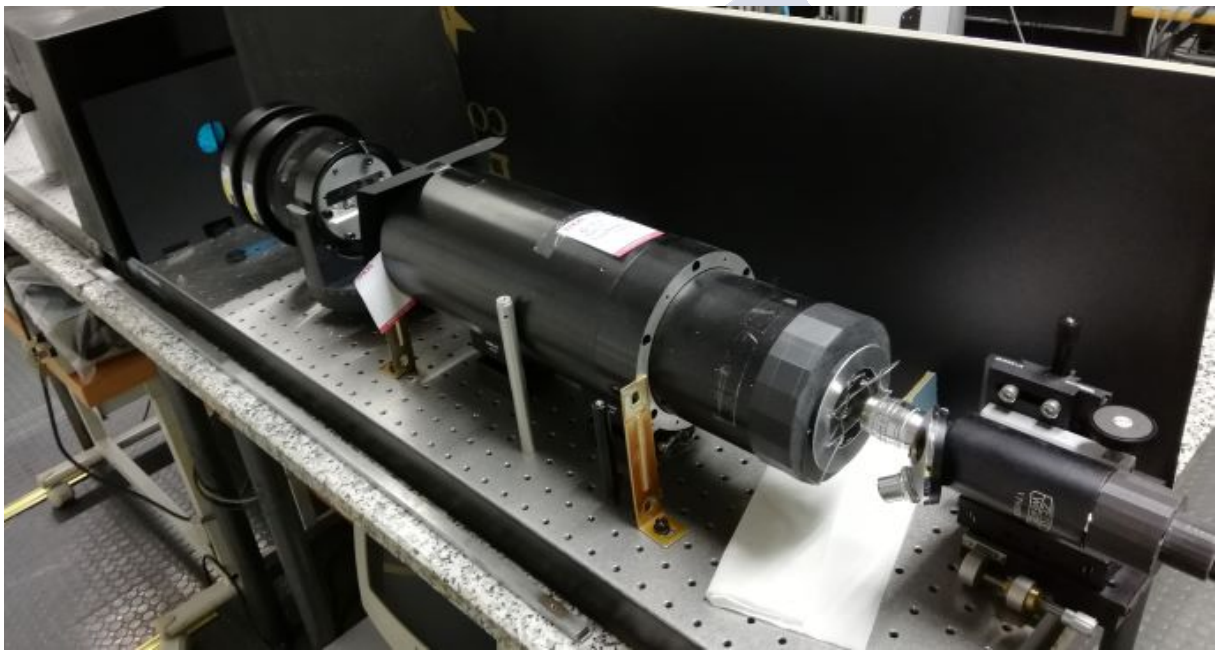


Figure 4.2.13: Experimental setup to implement the second photo-reduction.

In this new system, the object needs to be illuminated by transmission. This way of illuminating is far more effective that illumination by diffuse reflection, greatly reducing the exposition time needed from hours to minutes, thanks to the bigger radiation dose applied. To illuminate the object, monochromatic coherent light is used. The reason for using coherent light is that, despite the fact that maximum transmitted spatial frequency is reduced in comparison with incoherent light, the transmitted frequencies have a bigger modulation than in incoherent light. Monochromatic light from the glass of a *Hg* lamp is mandatory due to the objective design.

To achieve our wished illumination, a 50 W *Hg* commercial lamp was used. The lamp was encased in a box with a small opening to prevent light contamination. Attached to

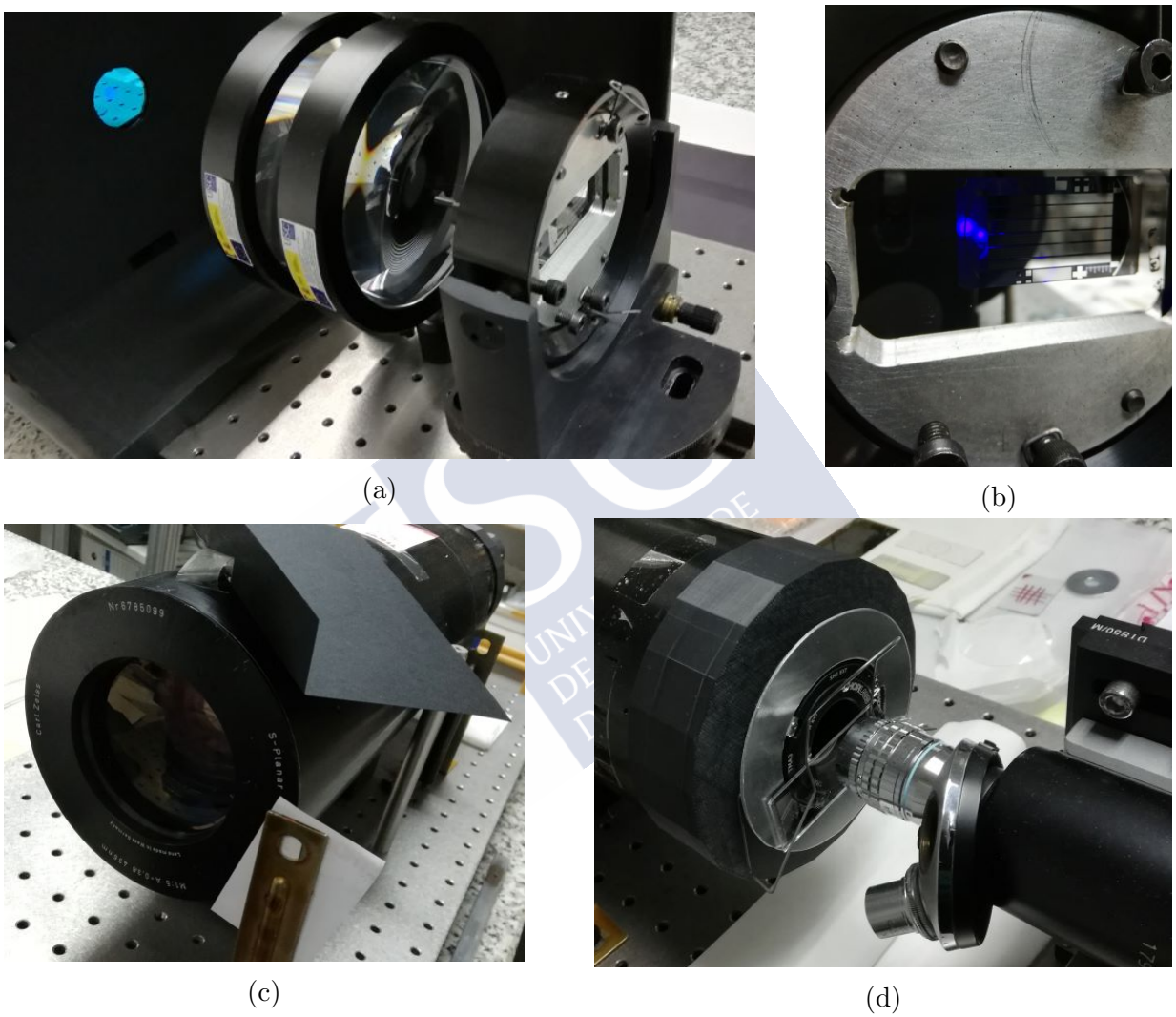


Figure 4.2.14: Different elements of the second photo-reduction system. (a) Illumination system. (b) Object holder. (c) Objective *Zeiss* of the system. (d) Holder for the sample and microscope to focus.

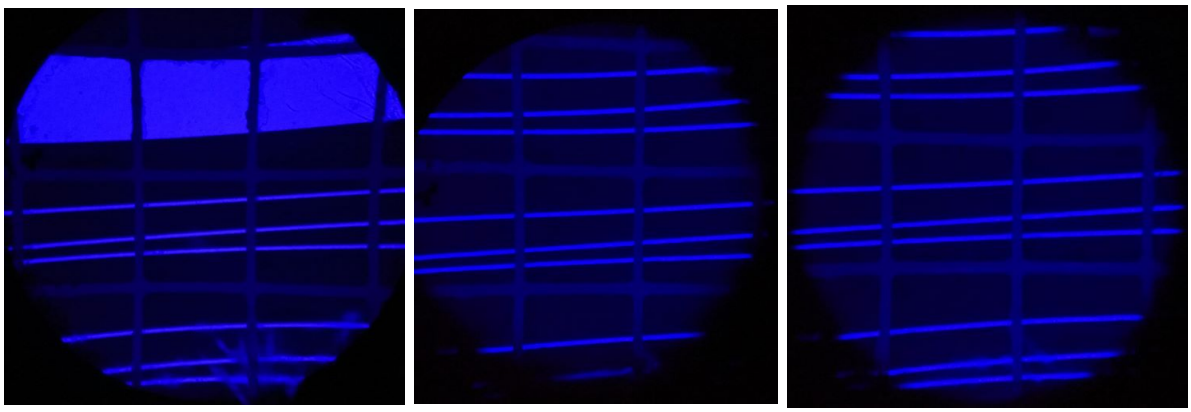
the opening, a diaphragm was placed, to control the amount of light introduced in the system, followed by a filter. The filter transmits a spectral band of 50 nm centred around 450 nm, which means that it transmits approximately 70% of the G-line from mercury. Moreover, we checked that the H-line emission (404.7 mm) was fully removed. The easy filtering is a great advantage of using coherent light instead of incoherent one.

A system of two lenses is situated afterwards in order to generate an image of the diaphragm over the entrance pupil of the objective, as well as correct the possible spherical aberration of said image. In this way, the lens must guaranteed that a ray crossing the border of the photomask, crosses through the center of the entrance pupil, to ensure that positive and negative diffraction orders are equally transmitted maintaining the contrast of the different corresponding spatial frequencies. To achieve this the lens system is composed of two flat-convex lenses of 125 mm diameter, located with the convex faces towards the inside of the system and separated approximately 50 mm. The first lens has a focal distance of 250 mm, while the second one is 375 mm. The distance between the lens and the diaphragm was a bit smaller than its focal distance so that the beam was slightly diverging between both lenses. The system is arranged in order that the image of the diaphragm is formed 190 mm inside the objective, where its input pupil is located.

As the objective has no internal focal adjustment, the distance between the object, our intermediary photo-mask, and the objective must remain constant. This distance must be of 15 cm, in order to have a reduction of $-1/5\times$. A fine tuning of this magnification is achieved with an axial translation stage under the object holder. It was made by a circular mount having tip-tilt adjustment, where we introduce a specially made circular piece of metal with an opening larger than the reduced motif of the mask. At the borders of the piece, wire tweezers were made to fix the mask against the piece.

Finally, a holder for the sample with photoresist was made. As the objective generates an image of our object at about 11 mm, it is required that this holder can move the sample position in order to correctly focus the image over it. This piece was made by different components. First, a 3D printer was used to generate a cylindrical cover, with an internal diameter equal to that of the exit of the objective mount to being introduced in it by pressure. The surface parallel to the lens of this cover has an opening, bigger than the outgoing beam of light. A set of four commercial thread adapter rings with some modifications were attached to the cylinder to make a thin and economical sample holder (see figure 4.2.14(d)) The rings opening allows light to pass and the sample can be fixed in it thanks to wire tweezer added to the ring. Just like in the first photo-reduction, a microscope is placed at the end of the system. Using a marked glass one can correctly focus the reduced image over the glass surface, and so of the sample, by changing the position of the glass screwing or unscrewing one of the rings.

To sum up, the combination of the first and second photo-reduction processes allow us to obtain a total reduction factor of 1/70.55, and the entire process as a resolution enough to resolve waveguides of few micrometers width (< 3 μm).



(a) (b) (c)

Figure 4.2.15: Image of the IQPs provided by the second photo-reduction objective seen through the microscope and a phone camera. The last two are responsible for the appreciable distortion.

4.2.3.5 Metallic layer etching

Finally, after the photoresist development, the metal layer corresponding to the developed motif in the resin must be removed. This is done by means of a etching acid for the respective metal, which does not interact with the photoresist.

The acid employed for aluminium is made by orthophosphoric acid (H_3PO_4) and nitric acid (HNO_3) The first one is responsible for dissolving the aluminium oxide layer (Al_2O_3) formed naturally when exposed to air, while the second one oxidizes the rest of the aluminium layer. The required time for the etching to be complete is between 5 and 10 minutes depending on the film thickness[4]. The process is complete when the metal layer suddenly turns from opaque to transparent[5], although waiting between 30 and 60 additional seconds is preferable in order to correctly remove all the punctual remains of metal not visible to the naked eye. It is not good to wait much more time to avoid the acid to etch the aluminium covered by photoresist by the side. Moreover, this lateral etching is faster than the frontal one due to a local temperature rise. It is generated by the exothermic etching reaction in absence of connection.

Once the motif is imprinted into the metal, photoresist is no longer needed and can be removed through dilution in acetone or scrubbing with a soft sponge to not scratch the metal. Finally, after the ion exchange is made on the glass, all the remaining metal can be etched and removed. It is important to note that the design of our IQPs includes some references to help during following steps. Thus, these references must be protected from etching by a few drops of photoresist placed manually on them or by means of a

[4]In the case of chrome, the etching acid is faster and transparency times oscillate around 3 to 5 minutes.

[5]This transition lasts around 15 to 30 seconds.

specific marker for the manufacture of printed circuits, whose ink withstands the acid.

4.2.4 Cutting and polishing of the IQPs

We are going to introduce light into our IQPs through end-fire coupling, which consists of directly illuminate the extremity of the waveguide. Consequently, the waveguide must end in a flat and smooth face of the glass, perpendicular to its propagation axis. This final fabrication process consists of three steps: stacking of ion exchanged glasses, cutting of the glasses and lapping and polishing of the IQPs. As our waveguides are situated into a small central region of the glass, it is necessary to cut and polish the edge of our desired element in a way that the waveguides end in it. As the final waveguides are not easily visible, it is useful to leave some aluminium marks as a reference as it has been explained before.

4.2.4.1 Stack

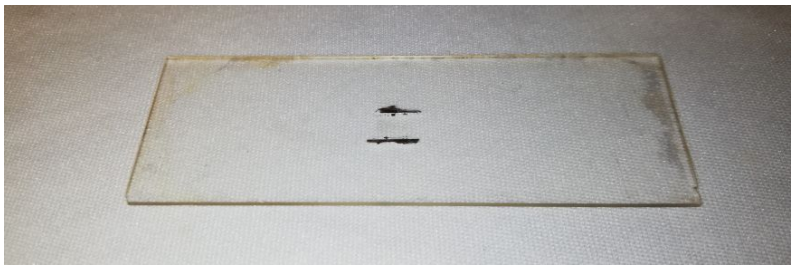
If we tried to directly cut or polish one of the exchanged glasses, small fractures can be produced in its edges. This fractures can affect the waveguides hindering coupling of light. To prevent this, it is necessary to stick to the sample several identical glasses to form an stack, as shown in Figure 4.2.16(c). The purpose is to protect the sample with the additional glasses which are the ones exposed to break during cutting or being fractured during polishing. Once the polish is finished, these glasses must be removed, so they were sticked with hot wax. On the other hand, polish process is very time consuming so several exchanged glasses can be stacked as well in order to be cut and polished together.

In our case, the stacks were made by three ion exchanged samples, each of them stick to two additional protective glasses. Additionally, two more protective glasses were add to each side of the stack. The protective glasses are stick to the samples wax. The three glasses are aligned and put into a hot surface with small wax particles between them. Once the wax is molten the pack is pressed by a press (Fig. 4.2.16(a)) to correctly spread the wax over the glasses preventing the appearance of bubbles. To avoid the glasses to slide between each other, they are put between tops once aligned.

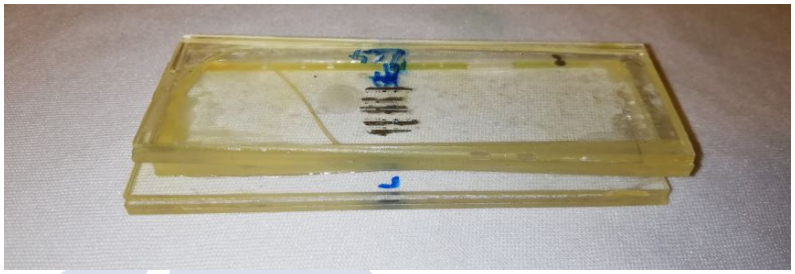
Having three packs of sample with protective glasses, two packs can be adhered to each other with epoxy glue (*Araldit*). Using glue not only avoids the problem of heating again the glasses adhered with wax, but epoxy has also a high transparency which is important when aligning samples. The alignment is done while the glue is soft by using the references of the samples with the help of a microscope, which allows us to align with greater precision than a tenth of a millimeter. Once the glue is hard, the third pack is added in the same way Finally, an additional glass is stick at each side of the stack. The advantage of the glue over the wax is the fact that is more transparent, but has the disadvantage that it can not be detached once hardened, while wax can be molten again.



(a)



(b)



(c)

Figure 4.2.16: Figure (a) shows the device used to create an stack of ion exchanged samples and protective glasses with wax and epoxy through pressure. In Figure (b) an ion exchanged sample is shown. The final stack of samples can be seen in Figure (c).

4.2.4.2 Cutting of the glass

A single glass can be cut by scratching it with a sharp stone and flex it until it breaks. But doing this can damage our sample. To cut the stack of glasses is necessary to employ a saw. In our case we employed a saw *Struers Accutom-2*, whose circular cutting blade is made of metal with embedded diamond particles and it has a thickness of 1 mm. The blade is water cooled and has a maximum speed of 3000 rpm. The sample is mounted in a holder situated in a wagon which moves at slow speed towards the blade by means of a spring, as shown in Figure 4.2.17. A micrometer is used to measure the forward speed, that must be slower than the cutting speed to not break the stack or the blade.

4.2.4.3 Lapping and polishing

The final step to have our IQPs ready consists of the lapping and polishing of the cut stack. This was done with a *Logitech Precision & Lapping Machine PM2A*. The objective of both process is to obtain flat and chipless sides of our stack. This is achieved by making the sample rub against a rotating wet disk. The disk is different for each process, just like the liquid used to moisten it.

For both processes, the sample is mounted in a holder called *jig* (Fig. 4.2.18(a)). The base of the *jig* is a ring with inner and outer diameters of 8.5 cm and 12.7 cm respectively,



(a) (b)

Figure 4.2.17: Struers Accutom-2 saw.



(a) (b) (c)

Figure 4.2.18: (a) *Jig* where the stack is mounted in the top. (b) Lapping process. (c) Polishing process.

inside of which the sample is mounted and pressed inside an auxiliary piece. This element descends due to gravity until it touches the disk surface. The *jig* has a micrometer to measure the fall of the sample and it also has a spring that acts against gravity to regulate the pressure of the sample against the disk.

The waveguides must be perpendicular to the ring of the *jig* in order to obtain a flat glass surface perpendicular to the guides. This alignment in two axes is done with the help of a laser using three scrubs in the *jig* to control the orientation of the sample. Levelling the laser beam and the *jig*, the surface parallel to the waveguides can be easily aligned by illuminating it with the laser and orient the reflection towards the laser. This guaranties that the surface to be polished will be perpendicular to waveguides. The second angle can be adjusted by measuring the distance of the surface to be polished to the non etched aluminium rules of the IQP with the help of a microscope.

4.2.4.3.1 Lapping

The purpose of the lapping is to obtain a flat and scratchless glass surface, although it leaves a roughness of around a micrometer, and can reduce around a millimetre of the sample. The lapping disk is made of iron 30 cm in diameter. During lapping, an abrasive liquid is used to moisten the disk, which is made of suspension of aluminium oxide particles of about 10μm in water. The machine also rotates the liquid tank which slowly drops liquid over the disk to keep it moisten. The lapping system is shown in Figure 4.2.18(b).

Once the sample is correctly oriented, the *jig* is put over the lapping disk and it is held by a mechanical arm. When the disk starts to rotate, the arm retains the *jig* over the disk but it allows it to rotate. The sample presses against the disc surface and, due to the rotation of both disk and *jig*, is polished by friction.

It is important to note that, at the beginning, the pressure of the sample against the surface must be regulated low with the spring. This is because, due to the sample alignment, only a fraction of the sample is actually touching the surface, so the pressure is higher there. Once the lapping advances and all of the sample is touching the disk surface, pressure can be deregulated leaving gravity act free. During this step, the orientation of the lapping can be checked with the help of a microscope and the reference and corrected.

This step finishes when the sample surface is flat but diffuse. Then, a deep cleaning must be done to remove all possible remains of abrasive over the sample and *jig* that can scratch the glass during polishing. It is also important to wash and dry the iron disk to prevent its oxidation.

4.2.4.3.2 Polishing

The polishing purpose is to reduce the roughness of the glass surface until it becomes transparent. Moreover, special attention must be paid to remove any chips in the sample edges. The surface of the polishing disk is made by polyurethane and it has a lot of pores of less than a millimeter in it. The abrasive liquid employed in this stage is also

made of a suspension of aluminium oxide particles in water, but of a lower size, around 1μm. Again, the sample pressure is progressively increased. When the polished surface becomes transparent, we must inspect the edge of each sample of the stack with help of a microscope (10×10).

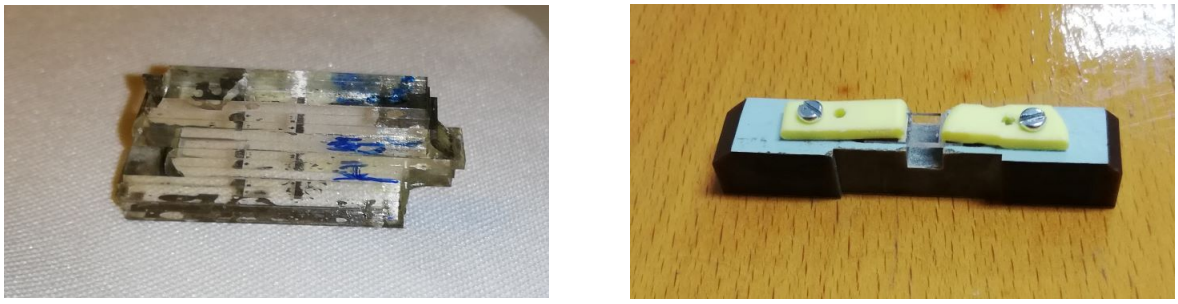
The process finishes when no chips remain, which usually requires fairly more polishing time that to achieve transparency. Once the it is over, the sample, the *jig* and the disk must be correctly washed, specially to prevent particles of aluminium oxide to close the pores of polyurethane.

The polishing process barely reduces a few tens of microns of the sample width. Thus, if the lapped surface is not correctly aligned, it will not be polished in its totality. Therefore, the polishing of each side of the sample must be done just after its lapping, without any change in its alignment.

4.2.4.4 Sample holder

Finally, after our stack is cut and polished as seen in Figure 4.2.19(a), we must separate our IQPs samples form the others and the protection glasses. This is done by putting it again over a hot surface to melt the wash. With the help of tweezers, we extract our samples with extreme delicacy trying to not cause new chips. The samples must be then thoroughly washed with acetone, alcohol and detergent to remove any remaining traces of wash and other dirt that can cause light dispersion during the characterization.

To protect and work comfortably with the IQPS, we manufactured sample holders, as shown in Figure 4.2.19(b). These are made of a piece of wood with a recessed surface to place the sample, which is held by two plastic pieces attached to the mount by screws. The edges of the holder have been lowered to nearly the sample size through a wood-milling cutter and they are removed in the center, leaving open the borders of the IQP where the waveguide inputs are located. Finally, the sample holder has two screw threads at its sides to mount it in the characterization system. Once mounted, our IQPs are ready for characterization.



(a) (b)

Figure 4.2.19: (a) Stack after being polished. We can see the aluminium reference marks of the three samples through the just polished surface. (b) Final IQP sample mounted on its protective holder. It measures 7 mm between the input and output polished surfaces.

4.3 IQPs characterization

4.3.1 Characterization of the IQPs through a four-step phase shifting algorithm

Once our IQPs are fabricated, we are interested in characterise their actual achieved parameters, like the size and depth of the waveguides or the distance between them in couplers. With this purpose, a phase shifting method can be applied on the ion exchanged glass to recover the modulating phase introduced by the waveguides when illuminating perpendicularly to the sample surfaces. This will be done through differential interference contrast (DIC) microscopy that, despite being primarily a qualitative phase-imaging technique, it can be used to implement a phase-shifting algorithm (PSA). The first of this kind of methods was originally introduced by Carré [Carré, 1966], but we are going to employ the four-step algorithm [Wyant, 1982, Creath, 1988, Wyant, 2015]. This non-linear algorithm is one of the first and best known PSA, and allows one to recover the modulating phase introduced by a sample from a set of 4 phase-shifted interferograms.

4.3.1.1 Description of the polarizing interference microscopy

DIC microscopy is based on the use of a polarizing prism (Nomarski prism, similar to a Wollaston prism) after the sample, being both placed between two aligned polarizers whose axis are rotated 45° respect the main axis of the prism [Prieto-Blanco, 2006, Pluta, 1988, Pluta, 1994,Sochacka et al., 1994]. This system works as an interferometer, as it duplicates the image laterally along the axis of the polarizing prism (lateral shearing). This is, the Nomarsky prism superposes two perpendicularly polarised rays coming from two slightly separated points along the prism main axis (axis y) generating two sheared images with orthogonal polarizations. If illumination is spatially coherent, both images interfere with each other once their polarizations superpose in the last polariser, known as analyser. Thus, the intensity at each point of the final image depends on the phase difference at two points of the object. The name of the DIC technique (differential interference contrast) comes from the fact that the shearing is so small (lower than the image resolution) that this difference can be approximated by a phase derivative and the double image is not appreciated [Pluta, 1988]. DIC microscopy can be configured to introduce phase shifts between both images to implement a PSA.

Often, DIC systems phase shifts between both images are introduced with a transversal displacement of the Nomarsky prism. However, our microscope has a fixed Nomarsky prismand the phase is shifted by a Sénarmont compensator instead. This compensator substitutes the first fixed polariser with a combination of a freely rotatable one along with a fixed QWP, whose axis are aligned with the analyser (axis y'). Each orientation of the polariser leads to the QWP introducing a different phase shift between the polarization components x and y without changing the amplitudes of the Nomarsky reference system. Specifically, a rotation of α respect the parallel direction of the analyser (axis x') leads

to a phase shift of 2α in the interferogram. In this way, if the polariser and analyser are aligned, the retarded (also aligned) does not affect polarization So maximum constructive interference is observed in those regions of the field with constant phase, while lesser intensity occurs where the object has a phase gradient along the shearing direction, with no phase shift between both generated images. On the other hand, if, for example, the polariser is rotated 45° respect the analyser, the QWP will introduce a $\pi/2$ phase shift between both images. The phase gradient regions are brighter or darker (depending on the sign of the gradient) than uniform phase regions.

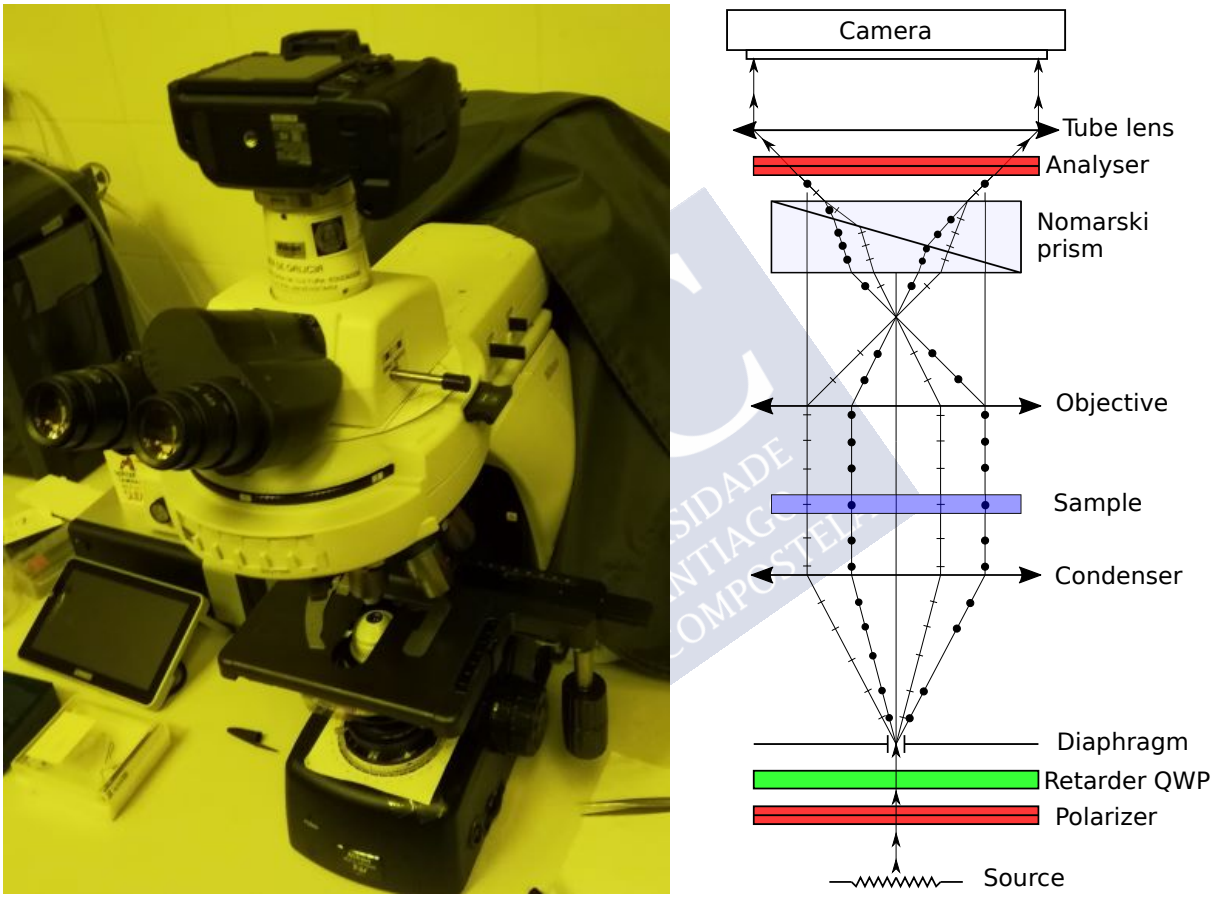
In figure 4.3.20(b), the diagram of our used DIC microscopy system is shown. First, light emitted by the source crosses the polariser and QWP of the Sénarmont configuration, to generate the phase shift between polarizations as explained. The light is collimated by closing the aperture stop of the illumination system, in order to increase the spatial coherence of the source. Then, the light illuminates the sample and is focused by the microscope objective. Simultaneously, it forms an image of the sample at infinity. Finally, the Nomarsky prism and the analyser generate the interference which is registered by a camera located at the image focus of the tube lens.

4.3.1.2 Experimental setup and image acquisition

The microscope used, shown in figure 4.3.20(a), is a Nikon microscope Eclipse Ni-U with with CFI TU Plan Fluor Objectives in a DIC transmission configuration working with only one Nomarski prism, Nikon LV-DIC-A, mounted on a slider that is introduced just after the objective. This model is typically used for biological applications and it is not designed to make quantitative DIC measurements, as it does not allow to shift the Nomarski prism. However, by modifying it by taking advantage of a rotatable polarizer and a retarder, the microscope can be used to implement a PSA obtaining images with different rotations of the polarizer, as was previously explained in subsection 4.3.1.1. Images were captured with a Nikon D750 camera. This camera has a 35.9 x 24 mm RGB CMOS sensor with a pixel size of 5.95 μm.

A four-step algorithm [Wyant, 1982,Wyant, 2015] requires four images with a constant phase step between them. However, in our case, a total of 12 images are needed, three batches of four images each one. One batch must be done over a region of the glass sample without structures to work as a reference from where we can obtain a background phase introduced by the optical system. The other two set of four images must be done in the same region of interest of the IQPs, but with the sample rotated 90° around the optical axis (centered in the region). The objective of this additional rotated batch of four images is recovering the partial derivative of the phase along the perpendicular direction, which allos to integrate the phase without the appearance of errors, as will be explained later.

Once all the images of the wished regions are obtained, they are processed with the MATLAB software, implementing the algorithm explained in the next section.



(a) (b)

Figure 4.3.20: (a) Experimental microscope for applying DIC microscopy. (b) Diagram of the configuration for DIC microscopy.

4.3.1.3 Four-step phase shifting algorithm

As previously said, we are going to employ a four-step phase shifting algorithm [Creath, 1988] for characterising our IQPs. This algorithm requires the obtention of four different interferograms with phase steps of $\pi/2$ between them. Let us explain briefly how it works for our system.

Let α be the angle between the first polariser and x'-axis, which is perpendicular to the main y'-axis of the analyser. By applying wave optics it can be calculated that the interference irradiance between the two images produced in the Nomarski prism once they cross the analyser is given by

$$I_{2\alpha}(x,y) = I_1(x,y) + I_2(x,y) - 2\sqrt{I_1(x,y)I_2(x,y)}\cos\left[\phi''(x,y) + 2\alpha\right], \tag{4.3.41}$$

where I_1 and I_2 are the irradiations of both images, $\phi''(x,y)$ is the phase difference between beams introduced by the IQPs and a phase bias due to the Nomarski prism itself; and 2α is the phase shift introduced by rotating the polariser an angle α. Trivially, by choosing our phase step as $\pi/2$, that is, phase shifts of $2\alpha = 0$, $\pi/2$, π and $3\pi/2$, the intensities of the four interferograms are

$$\begin{aligned}
I_0(x,y) &= I_1(x,y) + I_2(x,y) - 2\sqrt{I_1(x,y)I_2(x,y)}\cos\phi''(x,y),\\
I_{\pi/2}(x,y) &= I_1(x,y) + I_2(x,y) - 2\sqrt{I_1(x,y)I_2(x,y)}\sin\phi''(x,y),\\
I_{\pi}(x,y) &= I_1(x,y) + I_2(x,y) + 2\sqrt{I_1(x,y)I_2(x,y)}\cos\phi''(x,y),\\
I_{3\pi/2}(x,y) &= I_1(x,y) + I_2(x,y) + 2\sqrt{I_1(x,y)I_2(x,y)}\sin\phi''(x,y).
\end{aligned} \tag{4.3.42}$$

Therefore, performing an image acquisition process with a monochromatic green spectral filter ($\lambda = 532$ nm) for polariser rotations of $\alpha = 0$, $\pi/4$, $\pi/4$ and $3\pi/4$, we can obtain the phase through

$$\tan\phi'_y(x,y) = \frac{I_{3\pi/2}(x,y) - I_{\pi/2}(x,y)}{I_{\pi}(x,y) - I_0(x,y)}. \tag{4.3.43}$$

As said above, the Nomarski prism introduces a small phase $\phi''_0(x,y)$ between both beams that depends on the image point. This phase can be obtained by acquiring four additional images without any object with the same rotations α and employing (4.3.43). Thus, the corrected phase difference between beams is given by

$$\phi_y(x,y) = \text{unwrap}\left(\phi''(x,y) - \phi''_0(x,y)\right), \tag{4.3.44}$$

where the Matlab's unwrap function is used to eliminate the phase steps introduced by the arctan function.

Now, we are not interested in $\phi_y(x,y)$, which is the phase difference between rays, but in the phase $\phi(x,y)$ introduced by the object in a single ray. By choosing the y-axis parallel to the shearing direction, both phases are trivially related by

$$\phi_y(x,y) = \phi(x, y + s/2) - \phi(x, y - s/2), \tag{4.3.45}$$

where s is the shear introduced by the Nomarski prism, that is, the distance between both beams. As s is small enough to be considered differential, $\phi_y(x,y)/s$ can be considered the gradient of the wavefront phase $\phi(x,y)$ in the y direction.

$$\frac{\partial\phi(x,y)}{\partial y} \simeq \frac{\phi(x,y+s/2)-\phi(x,y-s/2)}{s} = \frac{\phi_y(x,y)}{s}. \tag{4.3.46}$$

Therefore, to obtain the wished phase $\phi(x,y)$, it is necessary to integrate $\phi_y(x,y)$. However, this is not as trivial as it appears. If we make the integral in the y direction over the phase image with a program, for example by doing the accumulated sum on each column, there is also a sum of random noise phases that lead to different results in two contiguous columns; that is, a noise appears in the x-direction. We can analyse this noise clearly in the Fourier space. If we apply a Fourier transform to equation (4.3.45), we have

$$\begin{aligned}\Phi_y(w_x,w_y) &= F\left[\phi(x,y-s/2)-\phi(x,y+s/2)\right] \\ &= \Phi(w_x,w_y)e^{iw_y s/2} - \Phi(w_x,w_y)e^{-iw_y s/2} = 2i\sin(\frac{w_y s}{2})\Phi(w_x,w_y),\end{aligned} \tag{4.3.47}$$

where w_i is the conjugated variable of $i=x,y$, $\Phi'(w_x,w_y)$ and $\Phi(w_x,w_y)$ are the Fourier transforms of $\phi_y(x,y)$ and $\phi(x,y)$ respectively. We can not recover $\Phi(w_x,w_y)$ from the measured $\Phi_y(w_x,w_y)$, because any noise in low y spatial frequencies ($w_y <<$) will be amplified in the spectrum of $\Phi(w_x,w_y)$ due to the low values of $\sin(\frac{w_y s}{2})$. To solve this, it is required to acquire other four additional images with the interested analysed region rotated 90°, turning x-axis into the shear axis obtaining $\Phi_x(w_x,w_y) = 2i\sin\left(\frac{w_x s}{2}\right)\Phi(w_x,w_y)$, which also leads to Φ but having a different distribution of noisy regions. Thus, we can combine them by a weighted average to reduce errors [Shan, 2010]. In other words, the integration to obtain our wished phase $\phi(x,y)$ combining the gradients in both dimensions is given by[6]

$$\phi(x,y) = F^{-1}\left\{f_x(w_x,w_y)\cdot F\left[\phi'_x(x,y)\right] + f_y(w_x,w_y)\cdot F\left[\phi'_y(x,y)\right]\right\}, \tag{4.3.48}$$

where $\phi'_i(x,y)$, $i=x,y$, is the obtained phase gradient in directions x and y, and f_i is the integrating function

$$f_i = \frac{2i\sin(\frac{w_i s}{2})}{-4\sin^2(\frac{w_x s}{2}) - 4\sin^2(\frac{w_y s}{2})}. \tag{4.3.49}$$

[6]Except for an additive constant and a linear dependence in x and y cause we must set $f_x(0,0) = f_y(0,0) = 0$ to avoid numerical singularities. Note that the same problem is present at $\left\|\frac{w_x s}{2}\right\| = \left\|\frac{w_x s}{2}\right\| = 2\pi$. However, as s is lower than the microscope resolution, these spatial frequencies are not transmitted through the optics and can be also removed.

4.3.1.4 IQPs analysis

As explained, utilising DIC microscopy and a phase-step algorithm we can get the phase of propagation $\phi(x, y)$ (4.3.48), that is, the transmitted phase introduced by the IQPs in a wavefront propagating through them is expressed as

$$\phi(x, y) = \frac{2\pi}{\lambda} \int_0^\infty (n(x, y, z) - n_s)\, dz, \tag{4.3.50}$$

where $n(x, y, z)$ is the index distribution. For planar waveguides, $n = n(x)$ is given by equation (4.2.25), where x is the direction perpendicular to the sample surface. If we suppose a Gaussian profile, expression (4.3.50) can be written as

$$\phi = \frac{2\pi}{\lambda} \int_0^\infty \Delta n e^{-\frac{x^2}{d^2}}\, dx = \frac{2\pi}{\lambda} \Delta n \sqrt{\pi}\, \frac{d}{2}. \tag{4.3.51}$$

Therefore, by measuring the phase introduced by the waveguide, we can obtain the depth of said waveguide.

$$d = \frac{\lambda}{\pi^{3/2} \Delta n} \phi. \tag{4.3.52}$$

This expression can be used to obtain an estimation of the depth of our surface waveguides. However, this does not work for buried ones, as they do not have a Gaussian profile like (4.2.25). In this case, we can consider the profile in the x direction to be given by an HG function (2.2.52). In particular,

$$n(x) = \Delta n_b \sqrt{2e}\, \frac{x}{d} e^{-\frac{x^2}{d^2}}, , \tag{4.3.53}$$

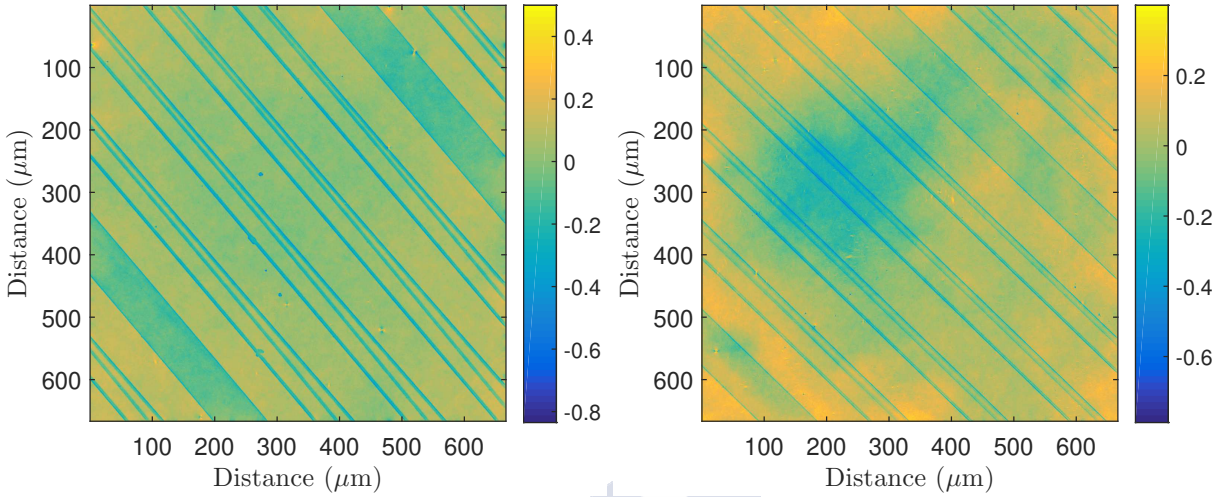
where $\sqrt{2e}$ is a normalizing constant to make the index change for buried waveguides Δn_b the maximum value. By introducing this profile in the integral (4.3.50), we have

$$\phi_b = \frac{2\pi}{\lambda} \Delta n_b \sqrt{2e} \frac{1}{d} \int_0^\infty x e^{-\frac{x^2}{d^2}}\, dx = \frac{2\pi}{\lambda} \Delta n_b \sqrt{2e} \frac{1}{2d^3}. \tag{4.3.54}$$

When waveguides are buried, their depth barely changes. Thus, using the depth of the surface waveguides calculated in (4.3.52), we can obtain the index change Δn_b of our buried waveguides as follows

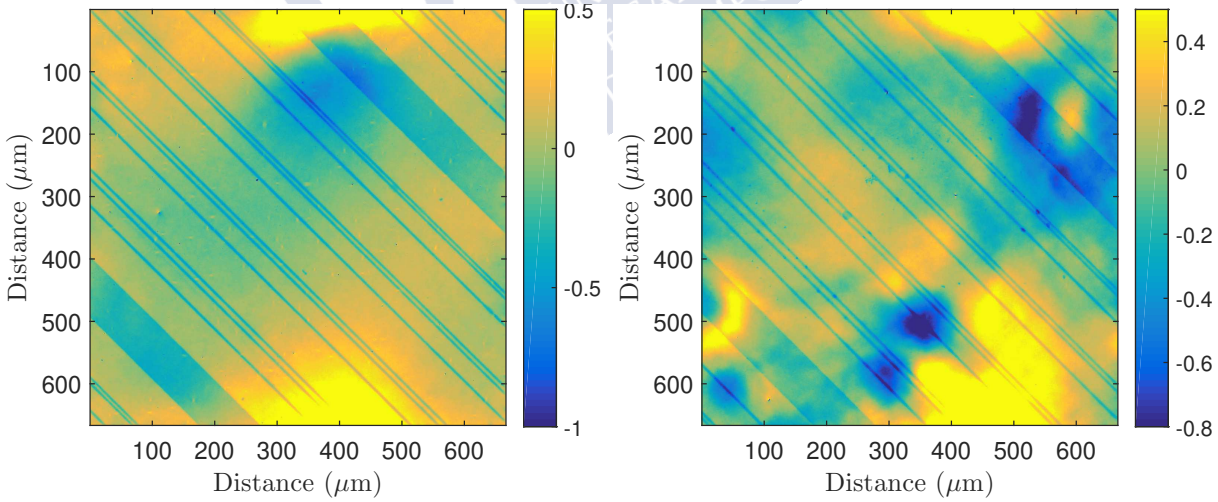
$$\Delta n_b = \frac{\lambda}{\pi \sqrt{2e} d} \phi_b. \tag{4.3.55}$$

Let us analyse our IQPs by obtaining the phase of propagation through the phase shifting algorithm. Specifically, we present an analysis of four different IQPs samples made by thermal diffusion employing two salts (silver and potassium) and with and without a burial process. In particular, in Figure 4.3.21 we show the analysis for the silver diffused samples AC2D0 (a) and AC2X1 (b), with the former corresponding to superficial waveguides and the later, to the buried ones. Meanwhile, Figure 4.3.22 shows the results



(a) (b)

Figure 4.3.21: Transmitted phase introduced by IQPs in false colour (with sign change for visualization) for silver waveguides. Image (a) corresponds to the superficial AC2D0 and image (b), to the buried AC2X1.



(a) (b)

Figure 4.3.22: Transmitted phase introduced by IQPs in false colour (with sign change for visualization) for potassium waveguides. Image (a) corresponds to the superficial AC2K4 and image (b), to the buried AC2K2.

for the potassium diffused IQPs AC2K4 (a) and AC2K2 (b), where the second once was subjected to a burial diffusion process unlike the first. All these figures were obtained by processing 12 DIC images taken with a 20× objective. Note that the axis of the image correspond to the system (x',y') of the analyser. The shear direction y is the diagonal $(x+y)/\sqrt{2}$, perpendicular to the waveguides.

In all these figures we can clearly see the presence of the ion exchanged waveguides in the glass. The phase sign is changed respect to (4.3.50) for aesthetic reasons. For comparison, a detail of the aluminium mask of this IQP before being removed for characterization is shown in figure 4.3.23. If we compare the silver and potassium diffused waveguides, we can see how the potassium ones (Fig. 4.3.22) present far more phase noise than the silver ones (Fig. 4.3.21). This is consequence of the anisotropic effects that potassium introduces in the waveguides, unlike silver. At the same time, by comparing the superficial (a) and buried (b) case in both figures, we observe that the burial process also increases phase noise. This is consequence of the expansion of the doping ion and the reintroduction of Na^+ ions in the glass.

Now, by means of a profile along a line perpendicular to the waveguides in these figures, we can obtain an estimation of the main experimental parameters of the IQPs: the size (s_w) of the waveguides and the separation (d_w) between them in the couplers. Besides, by using the gaussian index change of Table 4.3 it is possible to obtain the depth (d) of the superficial waveguides with equation (4.3.52), and with it, the index change (Δn_b) of the buried ones with equation (4.3.55). All the linear profiles shown later were made by making the mean of several ones.

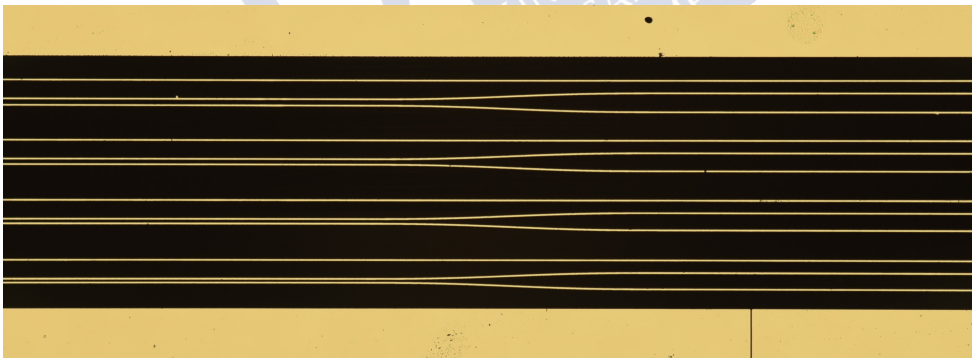


Figure 4.3.23: Aluminium mask of the IQP AC012 as view through an objective Nikon ×20 .

4.3.1.4.1 Silver exchanged waveguides

In Figure 4.3.24, we show the linear profiles of the silver diffused waveguides, being (a) the superficial AC2D0 and (b) the buried AC2X1. If we look at the profiles, we can see nine phase wells corresponding to the twelve waveguides seeing in Figure 4.3.21. From left to right, each group of three waveguides corresponds to the reference waveguide and the coupler, with the couplers going from the one with biggest waveguide separation to the one with the smallest. The phase reference level has a bit of noise and it is not constant along the distance, but rises and decreases along it. This is specially true in the buried case (b), where the phase disturbance is bigger as commented before. In any way, it does not affect our measurements, as we took mean values of the closest reference points of each waveguide to calculate its depth. The size and distance of waveguide are easily obtained through the middle points of the fall.

The experimental measures obtained are presented on Tables 4.8 and 4.9 respectively. In them, each row represents each group of three waveguides with waveguide 1 being the reference one, and waveguides 2 and 3 being the ones from the coupler. In the left column the designed waveguide separation is shown against the experimental one from the right column.

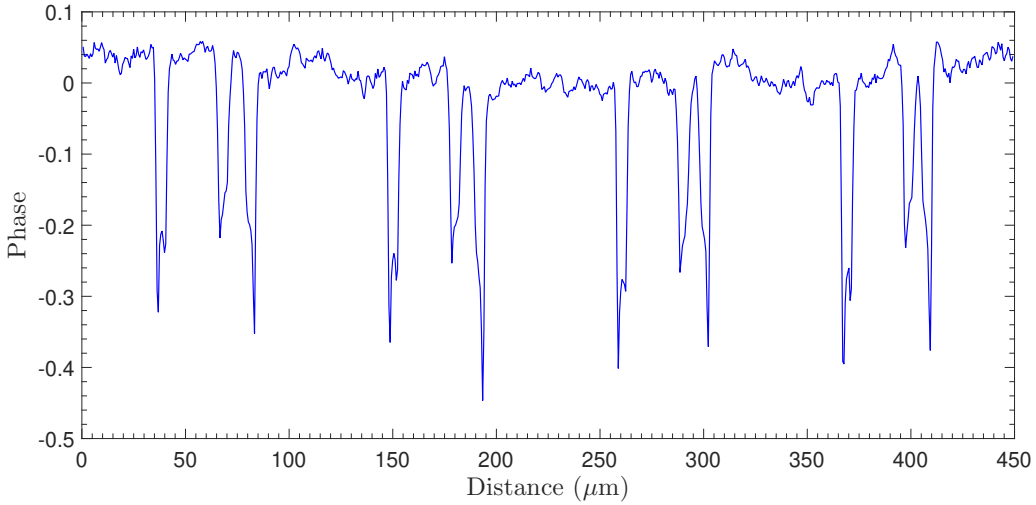
Table 4.8: Main parameters of the IQP AC2D0 with silver superficial waveguides.

AC2D0	Waveguide 1 (μm)		Waveguide 2 (μm)		Waveguide 3 (μm)		Waveguides
	size	depth	size	depth	size	depth	distance (μm)
3.0 μm	4.00	2.74	3.37	1.96	3.37	2.76	3.26
4.5 μm	3.77	2.85	3.46	2.45	3.63	2.69	5.17
6.0 μm	3.84	3.06	2.88	2.73	3.64	3.04	6.24
7.5 μm	4.19	2.99	3.67	2.49	3.80	2.63	7.60
mean	3.95	2.91	3.35	2.41	3.54	2.78	-

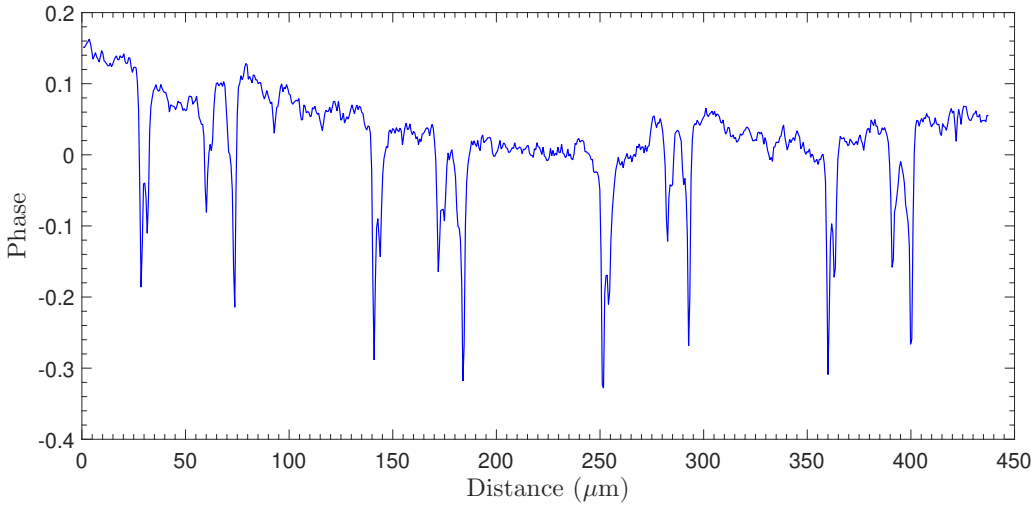
Table 4.9: Main parameters of the IQP AC2X1 with silver buried waveguides.

AC2X1	Waveguide 1 (μm)		Waveguide 2 (μm)		Waveguide 3 (μm)		Waveguides
	size	Δn_b (10^{-3})	size	Δn_b (10^{-3})	size	Δn_b (10^{-3})	distance (μm)
3.0 μm	4.27	3.24	3.53	5.46	3.84	5.39	2.97
4.5 μm	4.36	3.85	3.87	2.56	3.94	3.70	4.08
6.0 μm	4.43	2.59	4.31	2.25	4.20	4.29	5.35
7.5 μm	4.26	3.32	4.04	2.43	4.19	3.86	7.25
mean	4.33	3.26	3.94	3.18	4.04	4.33	-

As we can see in Tables 4.8 and 4.9 , the size of our ion exchanged waveguides tends to be around $s_w = 3 - 4$ μm for superficial waveguides and between $s_w = 3.9 - 4.3$ μm for buried ones. However, as can be observed in the figures 4.3.24 and checked on the



(a)



(b)

Figure 4.3.24: Linear mean profile of the transmitted phase perpendicular to the waveguides. Figure (a) shows the complete profile of all the waveguides of the analysed region for the superficial IQP AC2D0, while Figure (b) shows the buried waveguides of IQP AC2X1. The phase sign is changed for a aesthetic reasons.

respective tables, there is a slight difference in size between the reference waveguide and the waveguides in the coupler. The size of the first case are of about $s_w = 3.9$ μm for superficial waveguides and of $s_w = 4.3$ μm for buried ones. In comparison, the size of the waveguides that form the coupler are $s_w = 3.4$ μm and and $s_w = 4.0$ μm, for superficial and burial cases respectively. This might be consequence of a slight interaction between close waveguides during diffusion that slows the ion exchange process.

We also observe in the tables, the depths and index changes of the superficial and buried waveguides respectively. The measured depths are around $d = 2.4 - 3$ μm, a bit bigger than the estimations obtained in Table 4.4. Meanwhile, the depths of the buried guides are about $\delta n_b = 3.2 - 4 \cdot 10^{-3}$ which is about half of the superficial $\delta n = 7.7 \cdot 10^{-3}$ obtained in Table 4.3. This is consistent with the percentage of cations that remain in the glass after the burial, which can be estimated dividing the measured phases $p_c = \phi_s/\phi_c$, obtaining values around 50-60%.

We can compare the results shown in these table with the photo-masks designing parameters of Table 4.6. The design values of our photomasks were a size of $s_m = 3$ μm and distances between waveguides in the couplers of d_m =3.0, 4.5, 6.0 and 7.5 μm. In Table 4.8, we observe that for superficial waveguides there is a small amount of lateral diffusion, lower than 1 μm. This means that ion exchange was also occurring in the sides under the mask, resulting in bigger sizes than the ones designed for. Meanwhile, the waveguide separation is practically the same. By the contrary, as shown on Table 4.9, lateral diffusion is greater than a μm as a consequence of the expansion, while the waveguide separations are now lower than the designed values.

Finally, in figure 4.3.24, a curious phenomenon can be observed. There is a pronounced phase peak in each side of the waveguides. Moreover, in the close waveguides that constitute the coupler, this peak is only pronounced in the external sides of the coupler, being barely appreciated at the internal ones. We consider this to be a result of some silver reduction ($Ag^+ + e^- \rightarrow Ag^0$) and accumulation through some side diffusion effect, since it depends on the distance to the nearest waveguide. However, the reason is not really clear. An integrative effect can also be the origin. When calculating the depth, these peaks are not taken into account.

4.3.1.4.2 Potassium exchanged waveguides

Profiles of the phase of potassium diffused waveguides along a line are shown in Figure 4.3.25, with (a) being the superficial sample AC2K4 and (b), the buried one AC2K2. These profiles correspond to Figure 4.3.22. Just like before, the couplers are ordered, from left to right, from the biggest waveguide separation to the lowest. In these profiles, we can observe a higher phase noise than the one in Figure 4.3.24, specially in the buried case (b) where the phase level rises and falls markedly. As was commented before, this is attributed to the anisotropy that potassium ions in the glass produce. The first notable difference with silver exchanged waveguides is that the pronounced peaks at both sides of the waveguides observed for silver does not appear for potassium. Instead, these

waveguides present a simple phase peak. This shows that those peaks were not artefacts the image processing.

Despite noise, measure estimations can still be taken. They are presented on Tables 4.10 and 4.11 respectively. Again, waveguide 1 is the reference one and waveguides 2 and 3 form the coupler. In the left column the designed waveguide separation is shown against the experimental one from the right column.

Table 4.10: Main parameters of the IQP AC2K4 with potassium superficial waveguides.

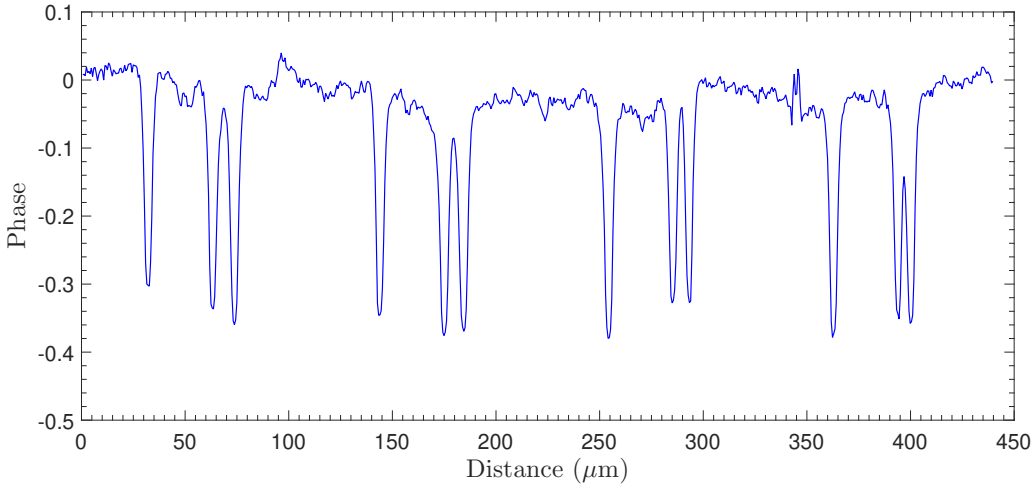
AC2K4	Waveguide 1 (μm)		Waveguide 2 (μm)		Waveguide 3 (μm)		Waveguides
	size	depth	size	depth	size	depth	distance (μm)
3.0 μm	2.98	3.50	3.27	3.41	3.41	3.46	3.41
4.5 μm	3.82	3.45	3.34	3.07	3.50	3.03	4.93
6.0 μm	3.93	3.29	3.28	3.11	3.14	3.03	6.03
7.5 μm	3.67	3.33	3.23	3.45	3.52	3.66	7.63
mean	3.60	3.39	3.28	3.26	3.40	3.30	-

Table 4.11: Main parameters of the IQP AC2K2 with potassium buried waveguides.

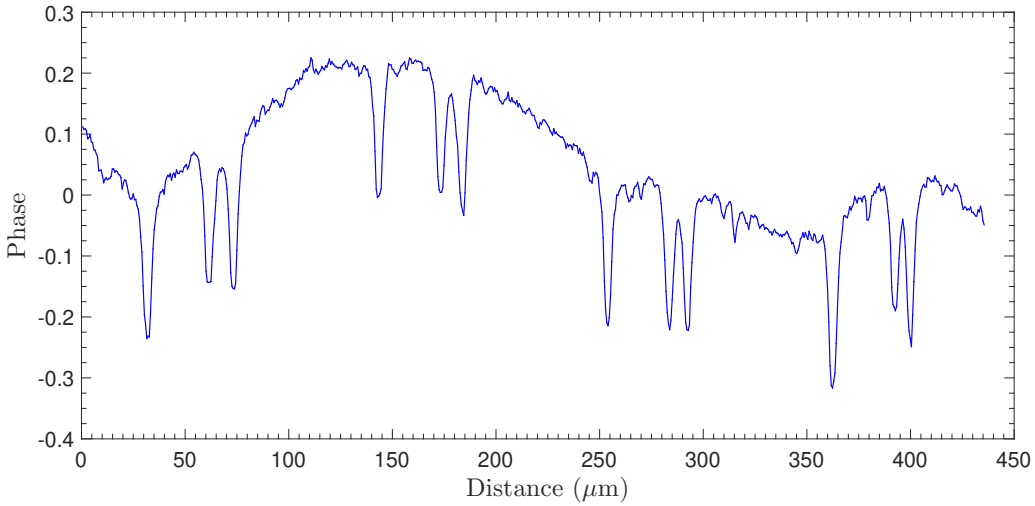
AC2K2	Waveguide 1 (μm)		Waveguide 2 (μm)		Waveguide 3 (μm)		Waveguides
	size	Δn_b (10^{-3})	size	Δn_b (10^{-3})	size	Δn_b (10^{-3})	distance (μm)
3.0 μm	4.44	5.20	3.57	4.21	3.36	5.38	3.79
4.5 μm	4.06	4.92	4.19	4.95	3.93	5.14	4.72
6.0 μm	3.69	4.37	3.80	4.28	4.68	5.19	6.42
7.5 μm	4.47	4.96	4.82	4.28	4.47	4.20	6.83
mean	4.16	4.86	4.10	4.41	4.10	4.98	-

Unlike with silver waveguides, there is not much variation between the different parameters of the waveguides. The size of our potassium waveguides is of about $s_w = 3.2{-}3.6$ μm when superficial and it grows to $s_w = 4.1$ μm when buried, as observed in Tables 4.10 and 4.11. Regarding the depth of the superficial guides we got values around $d = 3.3$ μm Meanwhile, The index change for the buried potassium waveguides vary between $\Delta n_b = 4.4 - 4.9 \cdot 10^{-3}$. Once again, this is half of $\Delta n_b = 8.9 \cdot 10^{-3}$ from Table 4.3

Considering the designing parameters of Table 4.6, we see that lateral diffusion still generates a bigger size than the one from the mask. Meanwhile, the separation between waveguides has some variations, due to the low precision of the measure, but still stays in the wished range. Curiously, unlike with silver waveguides, we do not see a reduction of the separation when buried, which reinforces the idea that lateral diffusion and phase peaks in silver are related. However, as the first diffusion time (t_{dif}) used was different for superficial and buried samples (Table 4.5), comparison is not easy.



(a)



(b)

Figure 4.3.25: Profile of the transmitted phase along a line perpendicular to the potassium exchanged waveguides. Figure (a) shows the complete profile of all the waveguides of the analysed region for the superficial IQP AC2K4, while Figure (b) shows the buried waveguides of IQP AC2K3. The phase sign is changed for a aesthetic reasons.

4.3.2 Semi-classical characterization of the IQPs through coherent light

4.3.2.1 Experimental setup

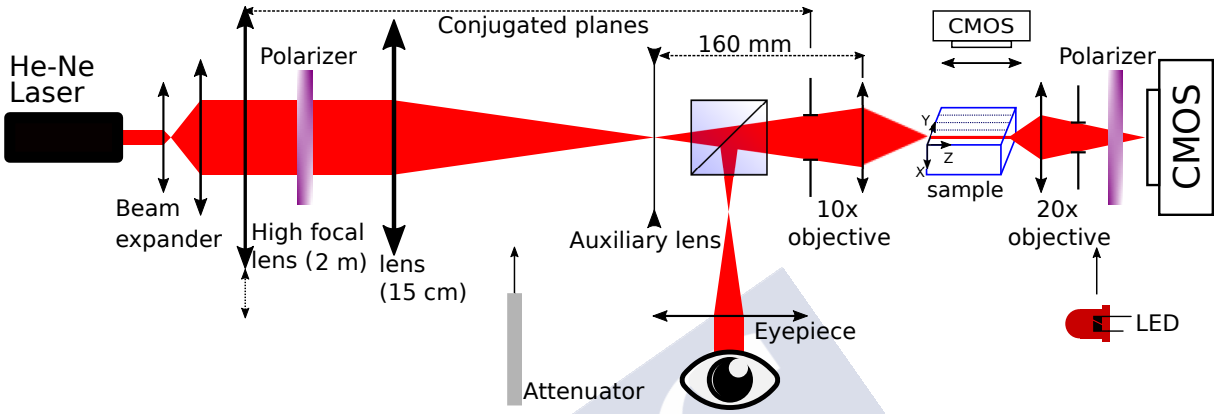


Figure 4.3.26: Simplified diagram of the optical setup.

In this section we are going to characterize how the integrated elements work when guided light is coupled in them. To introduce light into our waveguides through the end-fire coupling technique, an optical setup is prepared to directly illuminate one of the polished faces of the sample with a light beam focused into the transversal section of the waveguides.

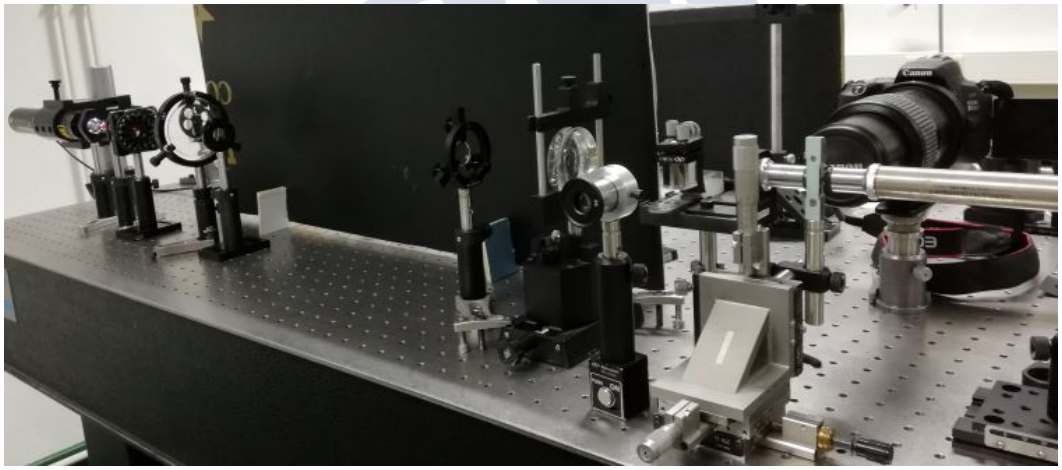
In figure 4.3.26, a simplified diagram of our optical setup is shown. First, a high-power positive lens (10 diopter) is used to focus a previously expanded He-Ne laser beam. An auxiliary negative lens is placed in the focus to help with the beam alignment. Next, the beam is focused again by means of a finite-conjugated (DIN standard) 10x microscope objective, situated at 160 mm of the auxiliary lens. Thus, a high-quality focused beam with a waist of few micrometers wide falls on the input face of our sample to excite the fundamental mode of the waveguide, which is usually monomode. As the required waist is wider than the objective resolution, only a portion of the objective aperture must be illuminated by the Gaussian beam. To ensure this, a beam expander was used, as shown in 4.3.26.

In order to correctly introduce the light beam into the waveguides, a cube beam splitter is placed before the input objective leading the back-reflected beam from the face of the sample to an eyepiece lens. By illuminating the output face of the sample with a retractable white LED, both the laser back-reflection (suitably attenuated just after the laser) and the input face are simultaneously seen through the 10x microscope objective in the eyepiece. The sample is mounted over micrometric precision translation stages in directions x, y and z, allowing for a precise control of its position. First, the sample is axially displaced to focus its input face. Then, the laser beam is accurately focused on this surface by axially moving the 10 dp lens. Now, we can easily make the beam to fall

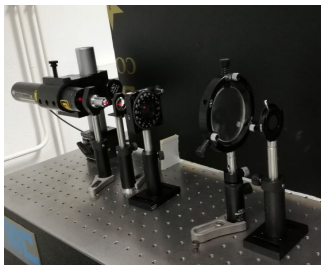
on the waveguide with a fine tuning of the sample position. Originally, a high focal lens (2 m) with adjustable height was placed in the conjugated plane of pupil of the objective, thanks to the high-power positive lens and the negative lens, with the purpose of fine tuning the beam position in the sample. Although the resolution of the translation stage was enough, the lens was kept in order to compensate beam misalignments.

Finally, in the output face, another standard 40x microscope objective creates an image of the end surface on to an CMOS Thorlabs DCC1545M camera. Therefore, we can take images of the transmitted irradiance by the waveguides at the output face. Additionally, a commercial camera Canon EOS 200D, equipped with an Canon Macro MP-E 65 mm objective, was placed perpendicular to the optical axis of the sample to take pictures of the dispersed light during its transmission in the waveguides.

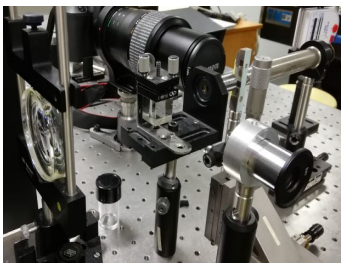
To sum up, the illumination system is configured for generating a high-quality beam focused over the input face with an appropriate waist to excite the fundamental mode of the waveguides. Moreover, an additional observation system allows to finely focus and move the sample within its support along the perpendicular directions to the beam, in order to couple this to the desired waveguide.



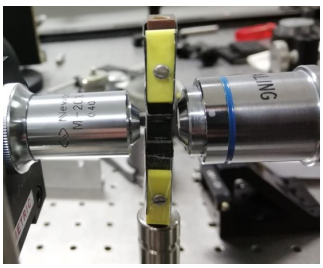
(a)



(b)



(c)



(d)

Figure 4.3.27: Experimental optical setup for the IQPs characterization. (a) Optical system. (b) Illumination system.(c) Focusing and observation system. (d) Sample mounted in its holder.

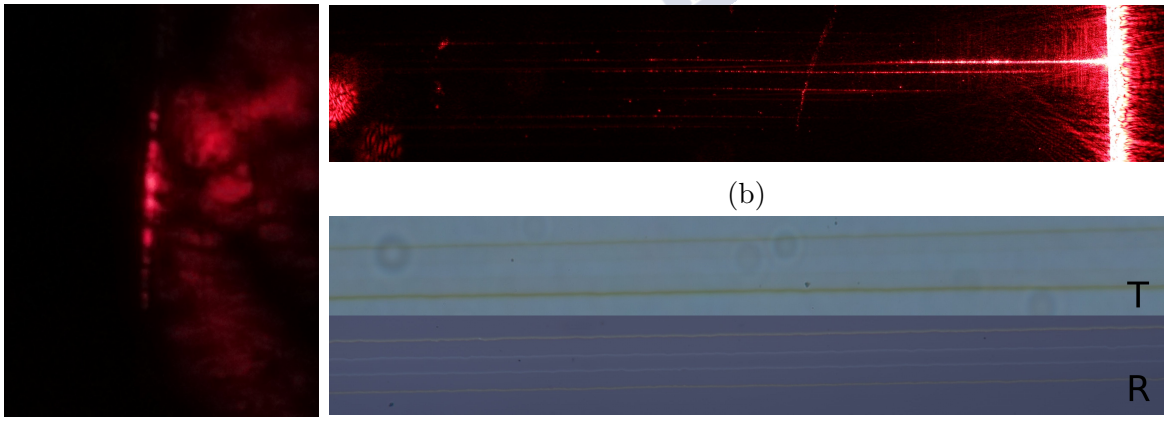
4.3.2.2 Coupling analysis

4.3.2.2.1 Silver exchanged samples

The first samples we fabricated were the silver ones. The reason for this was that silver does not present anisotropy and so, coupling between polarization transverse electric (TE) and transverse magnetic (TM) modes, that could disturb the coupling between waveguides, does not exist. However, it turns out that other problems arisen with it.

As explained before, silver waveguides presented high phase peaks at both sides. This was attributed to an accumulation of silver right under the aluminium mask due to some repulsive chemical effect during diffusion. These peaks can be observed under transmitted or reflected illumination as seen in Figure 4.3.28(c). The problem is that these peaks guide light as well and present high losses due to both, absorption and coupling to radiation modes. Thus, light transmitted through the waveguide is coupled in such peaks and gets lost. Superficial waveguides are already subjected to high losses, so barely any light came out of such waveguides for superficial samples and, definitely, not more than background dispersed light. Hence, it was not possible to take intensity measurements to characterize the coupling with superficial silver diffused samples.

It was expected that buried waveguides presented lesser scattering. However, its losses were still high. Moreover, it was observed that a slight planar waveguide was produced during the second diffusion to bury the waveguides. This is mos likely consequence of a slight contamination of silver ions in the salt. Therefore, light that gets lost in the peaks is transmitted through this planar waveguides until it collides with other buried waveguides and it is dispersed. Again, although it was possible to observe light modes coming out of the buried sample, these were too many, originated from the peaks and



(a) (b) (c)

Figure 4.3.28: Images of light losses in buried silver waveguides. (a) Light output on a screen. (b) Losses in light propagation. It can be observed how dispersion affects other waveguides and how the output is full of noise. (c) Silver peaks observed through transmitted (T) and reflected (R) light.

other waveguides that were dispersing light. Background dispersed light was too bright as well, hindering the possibility of measuring intensities. Even more, the impossibility of distinguish if light, or what amount of it, was coming from possible coupling or due to dispersion invalidated this samples. All this is observed in Figure 4.3.28.

In consequence, using silver exchanged waveguides requires dielectric masks.

4.3.2.2.2 Potassium exchanged samples

As said, the problem with potassium is anisotropy. This not only force us to work with a particular polarization, but the problem of coupling between different polarizations appear as well. To work with an specific polarization two polarisers were added, as shown in Figure 4.3.26. The first was added at the illumination system in order to couple a singular polarization into the waveguides, while the second one was added before the camera to take measures of the wished polarization, either the introduced one or its orthogonal. Employing potassium resulted in success, as we obtained bright light modes coming out of the IQP unit where we introduced light and barely any background light. Therefore, it was possible to characterize the coupling.

During characterization, it was observed that couplers behaved in the same way independently of the incident polarization (TE or TM). Nonetheless, as we expected, inner coupling between the introduced mode and the orthogonal one occurred inside the waveguides. When light in TE mode is introduced in input 1 from the IQP unit (Fig. 4.2.7), a significant TM mode was observed in output 2, while barely any light in such mode comes out of the other outputs. This suggest that the proximity of the waveguides induces in them a rotation of their optical axis. In this way, light inside the more separated reference waveguide (output 1) essentially retains the input polarization, whether it is TE or TM, being transferred very lightly to the other polarization mode. Basically, an isolated waveguide behaves like a waveplate with its main axis parallel and perpendicular to the surface. Meanwhile, in the second waveguide, light enters the coupler and finds some kind of rotated optical axis due to the asymmetry induced by the nearby presence of the companion waveguide of the directional coupler. Thus, part of the light gets transferred to the other polarization mode, while other part is being coupled into waveguide 3. Due to the length of the couplers, the new TM mode in waveguide 2 seems to not have enough length to be fully coupled into the other waveguide, while in this one, the TE mode is also unable to transfer to TM in time. Thus, barely any light in TM mode was observed in output 3, although it was observed in some couplers. As previously told, if we introduced TM mode instead in the IQP, the behaviour was symmetrically identical.

This polarization coupling was far greater in superficial waveguides than in buried ones. In superficial waveguides there was a lot of variation in the amount of light transferred to the orthogonal mode, reaching maximum values close to 50% and minimum around 15%. On average, the amount of light transferred between polarization modes in superficial waveguides is 26%. On the other hand, in buried waveguides polarization coupling had maximums of 11% and minimums of 2%, with an average of 6%. Once

buried, waveguides gain symmetry in both orthogonal axis, as they acquire an oval shape. Moreover, there is a smoothing of anisotropic effects due to a reduction of potassium concentration. Consequently, for manufacturing IQPs with potassium is important to bury the waveguides, as high polarization coupling means a big loss of efficiency.

In order to characterize coupling, we introduced light in the waveguide with the Y-junction of each IQP unit (Figure 4.2.7). Light is divided in the junction, with half of it going through a singular waveguide that acts as a reference, and the other half going through a waveguide that is part of a coupler. So, three light modes are observed on camera. By taking pictures and processing them with a MATLAB software, we can reassume the quantity of light that comes of each of the three waveguides, as well as the relative percentage of light that comes out in each of the waveguides of the coupler. The results are then compared by measuring as well the relative light intensity of the two outputs when light is coupled into input 2 (Fig. 4.2.7). This was done for the sixteen different IQP units of photomask 4.2.9, grouped in four blocks of four units. As explained in subsubsection 4.2.2.2, each block is characterized by a different coupler length (l_c) with each unit in it having a different waveguide separation (d_w).

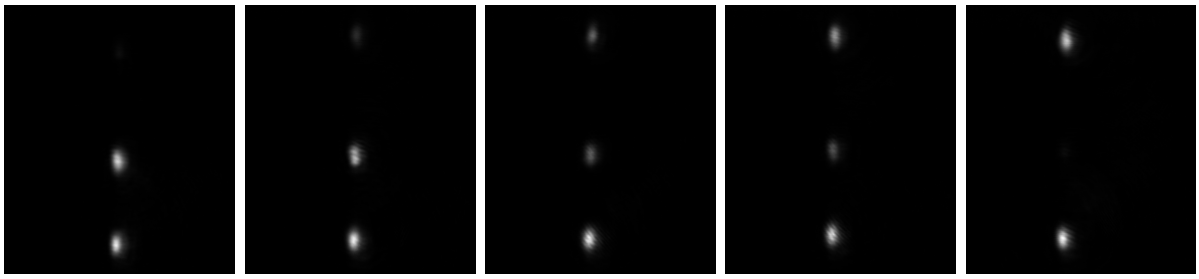
Figure 4.3.29 collects examples of the images taken in characterization for different couplers. The measurements obtained for the superficial and buried samples, AC2K4 and AC2K2, are shown in Tables 4.12 and 4.13 respectively. In these tables, relative intensities that come out of outputs 2 and 3 are presented. The given values are the mean of different batch of measurements taking into account both inputs and polarizations.

Table 4.12: Coupling measures for superficial potassium IQP AC2K4. Relative light intensity (i_i) in percentage that exits by the outputs 2|3 after enter by input 1(2).

AC2K4		l_c (mm)			
		0.5	1.0	1.5	2.0
d_m (μm)	3.0	9.1||90.9	39.5||60.5	86.7||13.3	81.2||18.8
	4.5	61.7||38.3	31.2||68.8	8.4||91.6	11.9||88.1
	6.0	85.9||14.1	80.4||19.6	63.1||36.9	48.8||51.2
	7.5	90.9|| 9.7	89.3||10.7	87.9||12.1	84.1||15.9

Table 4.13: Coupling measures for buried potassium IQP AC2K2. Relative light intensity (i_i) in percentage that exits by the outputs 2|3 after enter by input 1(2).

AC2K2		l_c (mm)			
		0.5	1.0	1.5	2.0
d_m (μm)	3.0	17.8||82.2	93.6|| 6.4	54.9||45.1	2.5 ||97.5
	4.5	35.9||64.1	5.9||94.1	7.4||92.6	40.9||59.1
	6.0	80.7||19.3	63.8||36.2	49.3||50.7	26.8||73.2
	7.5	92.6|| 7.4	88.4||11.6	86.3||13.7	79.8||20.2



(a) (b) (c) (d) (e)

Figure 4.3.29: Light modes obtained on the CMOS after introducing TE light into input 1 (Y union) in different IQPs. The lower point corresponds to the output of the reference waveguide (1), while the two upper points are the outputs of the coupler waveguides (2 and 3). From (a) to (e) light goes from output 2 ($\kappa z = 2n\pi$) to output 3 ($\kappa z = (2n+1)\pi/2$) crossing by a $\kappa z = (2n+1)\pi/4$ coupler (c).

According to equation (4.1.1), these values correspond to $\cos^2 \kappa z || \sin^2 \kappa z$. In particular, for the buried AC2K2, we can see at Table 4.11 that we have two couplers that works more or less as a $C_{\kappa z=\frac{\pi}{4}}$ (eq. (4.1.3)) and three working as a $C_{\kappa z=\frac{\pi}{2}}$ (eq. (4.1.2)), which are the most interesting couplers used in this thesis. These cases, in (d_m, l_c) notation, belong to couplers $(3.0, 1.5)$ and $(6.0, 1.5)$ for $C_{\frac{\pi}{4}}$, and couplers $(4.5, 1.0)$, $(4.5, 1.5)$ and $(3.0, 2.0)$ for $C_{\frac{\pi}{2}}$. For the superficial AC2K4 (tab. 4.12), we have one $C_{\frac{\pi}{4}}$ $(3.0, 1.5)$ and $(6.0, 2.0)$ and another $C_{\kappa z=\frac{\pi}{2}}$ $(7.5, 0.5)$ and $(6.0, 1.5)$.

Now, we can calculate the phase $\kappa(z - z_0) = \arccos\sqrt{i_2}$, where i_2 is the relative intensity of output 2. It is important to note that we take into account z_0, which represents the part where waveguides interact before and after the defined l_c. Thus, $z - z_0 > z$ represents the effective coupler length. Additionally, the $\kappa(z - z_0)$ values obtained belong to the first quadrant, but must be ordered to their right one. In Tables 4.14 and 4.15, we show the phases obtained for the superficial and buried samples respectively.

Table 4.14: Coupling measures for buried AC2K4 in terms of phase with unity π.

AC2K4		l_c (mm)			
		0.5	1.0	1.5	2.0
d_w (μm)	3.0	0.4024(14)	0.7164(04)	0.8814(06)	1.1428(23)
	4.5	0.2125(17)	0.3114(52)	0.4061(11)	0.6122(13)
	6.0	0.1227(10)	0.1458(24)	0.2077(23)	0.2538(08)
	7.5	0.0974(01)	0.1061(06)	0.1129(06)	0.1305(04)

These phases can be represented in function of both, coupler length (l_c) and waveguide separation (d_w). In the first case, as the phase itself means, the relation between coupling phase and l_c is trivially linear. In the second one, we know that the coupling comes from the evanescent exponential terms of the light modes outside the waveguides due to the

Table 4.15: Coupling measures for buried AC2K2 in terms of phase with unity π.

AC2K2		l_c (mm)			
		0.5	1.0	1.5	2.0
d_w (μm)	3.0	0.6387(16)	0.9187(06)	1.2343(11)	1.5505(19)
	4.5	0.2957(14)	0.4219(02)	0.5877(22)	0.7208(22)
	6.0	0.1449(11)	0.2053(03)	0.2523(07)	0.3268(10)
	7.5	0.0874(06)	0.1105(04)	0.1208(05)	0.1485(09)

mode tails. Thus, it is expected that the relation between the coupling phase and the waveguide separation be exponential as well. Therefore, it should be possible to fit our measures to the following curves:

$$\kappa\left(z - z_0\right) = m \cdot l_c + n, \tag{4.3.56a}$$

$$\kappa\left(z - z_0\right) = a \cdot \exp\left[-b \cdot d_w\right], \tag{4.3.56b}$$

Coupling phase in function of the coupler length is represented in Figure 4.3.30 for the different waveguide separations and for a superficial and buried sample, with the fitting parameters of the curves (4.3.56a) being shown on Table 4.16. On the other hand, Figure 4.3.31 represents the curves (4.3.56b) of the coupling phase in function of the waveguide separation for different coupler lengths, with its fitting parameters presented in Table 4.17.

Table 4.16: Fitting parameters of the coupling curves from Figure 4.3.30.

d_w (μm)	AC2K4		AC2K2	
	κ (π/mm)	$-z_0$ (mm)	κ (π/mm)	$-z_0$ (mm)
3.0	0.4872	0.3469	0.6088	0.5391
4.5	0.2592	0.2288	0.2847	0.5441
6.0	0.0949	0.6457	0.1196	0.6969
7.5	0.0239	3.3326	0.0397	1.7003

Table 4.17: Fitting parameters of the coupling curves from Figure 4.3.31.

l_c (mm)	AC2K4		AC2K2	
	a (π)	b (1/μm)	a (π)	b (1/μm)
0.5	1.380	0.4119	2.832	0.4973
1.0	3.473	0.5328	4.045	0.4947
1.5	3.767	0.4869	5.616	0.5042
2.0	4.469	0.4532	7.319	0.5170

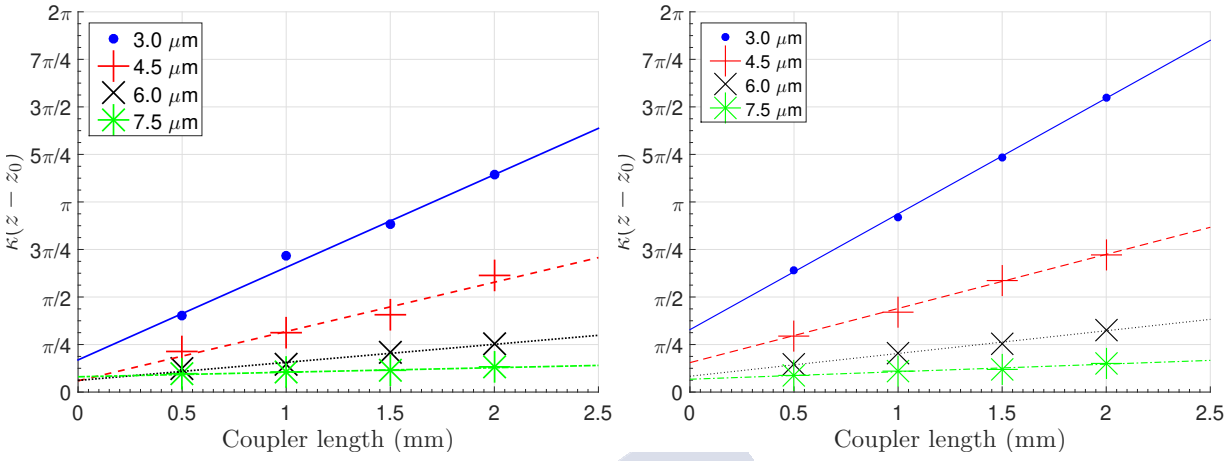


Figure 4.3.30: Coupling propagation phase in function of the coupler length for different waveguides separation. Coupling characterization for potassium diffused IQPs: (a) superficial sample AC2K4, (b) buried sample AC2K2.

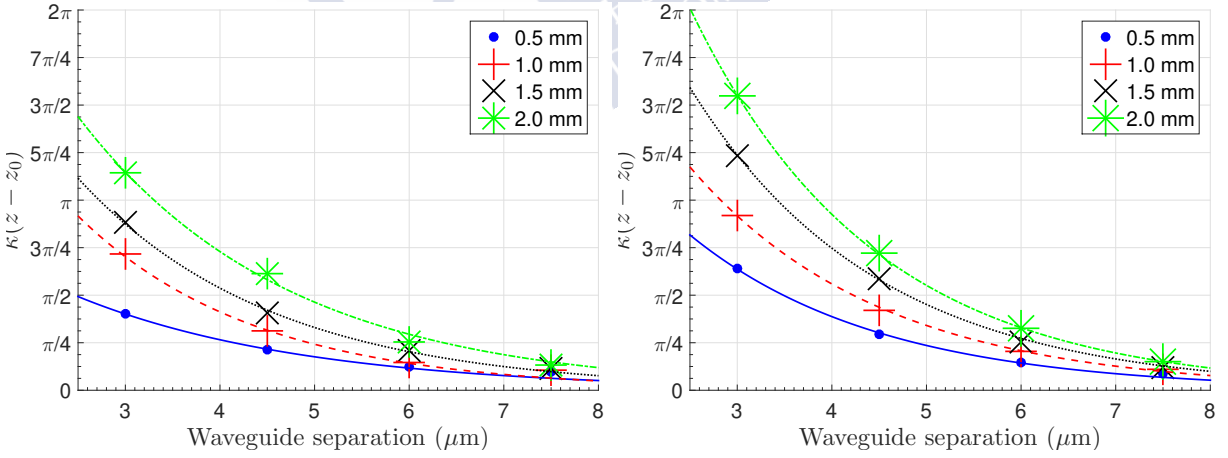


Figure 4.3.31: Coupling propagation phase in function of the waveguide separation for different coupler lengths. Coupling characterization for potassium diffused IQPs: (a) superficial sample AC2K4, (b) buried sample AC2K2.

In Figure 4.3.30 and Table 4.16, we can clearly see how the coupling phase grows linearly with the coupler length. Besides, in the different curves we see that, the closest the waveguides are, the faster it grows, as the coupling is stronger. Regarding the differences between superficial and buried couplers, we can see how the latter has a slightly stronger coupling than the former. This can be a consequence of the expansion of the waveguide during the burial process, which facilitates coupling. In Figure 4.3.31 and Table 4.17, an exponential decrease with the waveguide separation is clearly observed. This decrease is more pronounced for longer coupler lengths. Or alternatively, as the waveguides tend to be closer, the coupling exponentially grows in faster way for longer the couplers. Just like before, a slight stronger coupler is observed for buried IQPs.

These figures constitute fabrication curves that allow us to manufacture any kind of coupler with potassium for waveguides of $s_w = 3$ μm. In this way, in Table 4.16 we have obtained the values of κ and of z_0 for the different waveguides separation. z_0 inform us of the effective coupler length for our coupler that depends of the used curvature in our waveguides. It is observed that the values tend to be similar, specially in the buried one, with the exception of the case $d_w = 7.5$ μm. For this case, coupling is very weak in the initial points, which means that such points are not reliable as there may not be any coupling at all. For the more stable buried sample, we see that the values of $-z_0$ stand between 0.5-0.7. On the other, the coupling constant κ depends on the size of the waveguides, of the salt employed and of the waveguide separation. We observe in Table 4.17 that the exponential coupling b, which should be dependent on the effective index of the mode which determines the rate of the decrease, is basically the same (around 0.5 μm^{-1} for buried couplers) regardless of the coupler length, and it seems to be slightly smaller for superficial waveguides, possibly due their small size difference. Parameter a is smaller for the superficial sample, due to their weaker coupling. Finally, assuming always sizes of 3 μm for potassium, the dependence of the coupling phase κ with the waveguide separation can be fitted as equation (4.3.56b), obtaining the curves

$$\begin{aligned} \textit{Superficial: } \kappa &= 2.282\pi \cdot \exp\left[-0.509 \cdot d_w\right] \, mm^{-1}, \\ \textit{Buried: } \kappa &= 3.065\pi \cdot \exp\left[-0.537 \cdot d_w\right] \, mm^{-1}, \end{aligned} \tag{4.3.57}$$

which are shown in Figure 4.3.32. With these curves and the z_0 values in Table 4.17, we can fabricate any kind of coupler for potassium with a waveguide size of $s_w = 3$ μm and the same diffusion process with the parameters described in Table 4.5

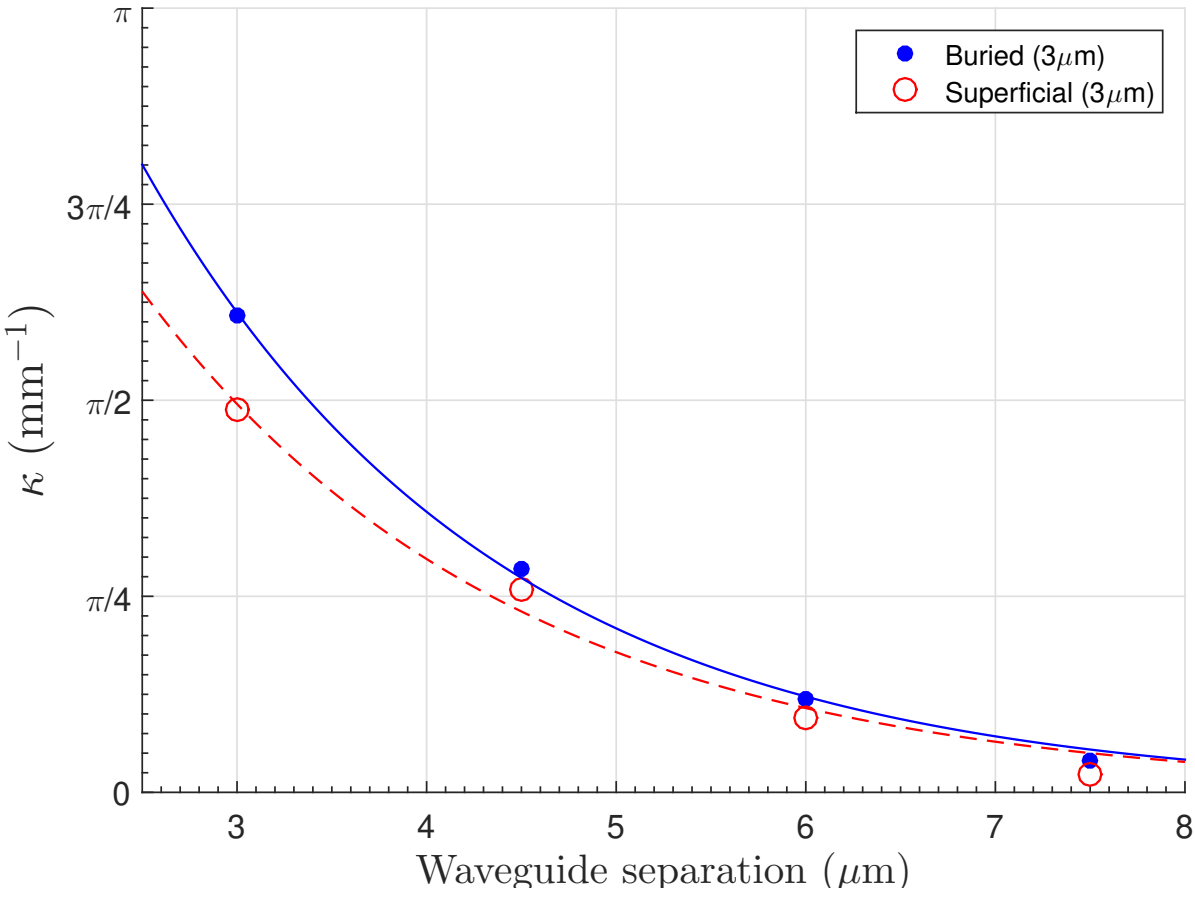
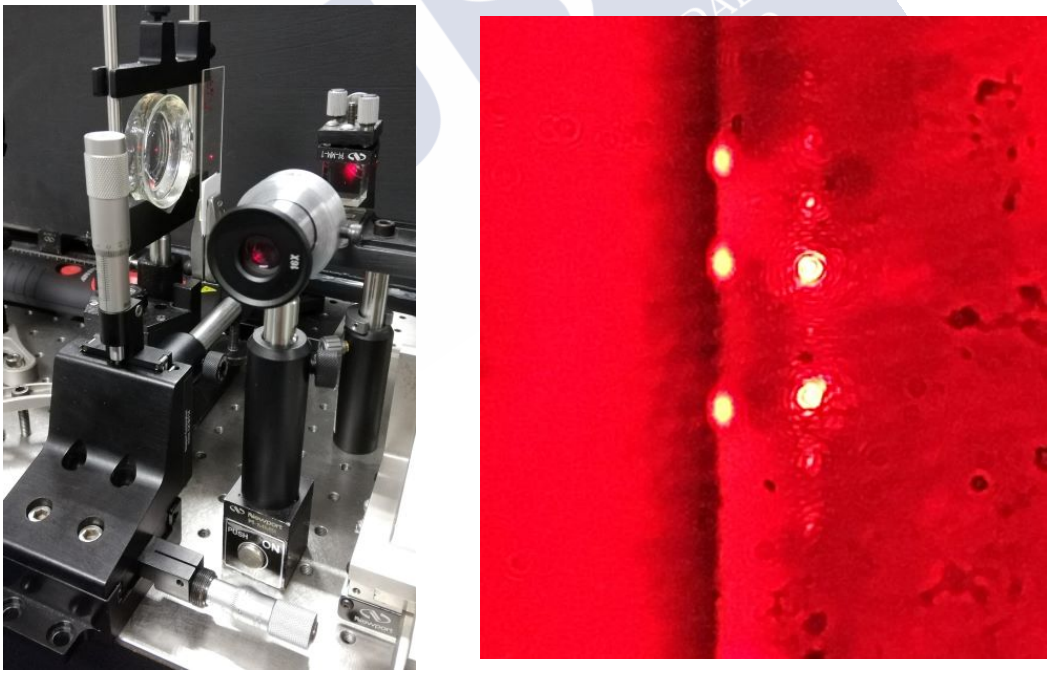


Figure 4.3.32: Coupling constant of AC2K2 (potassium diffused buried waveguides) in function of the waveguide separation.

4.3.2.3 Projection experiment

Finally, we wanted to probe that our IQPs can realize a projection transformation for two dimensions. In order to test this, we introduced a diffraction grating between the auxiliary lens and the BS from Figure 4.3.26. This grating had a period of 60 μm and was designed to not generate a order zero. Instead light is mainly distributed symmetrically between diffraction orders +1 and -1, allowing us to obtain two light beams with the same intensity. This grating was obtained through ion exchange using silver and fabricated following the method described in [Montero-Orille et al., 2020].

As shown in Figure 4.3.33(a), the grating is mounted in a support with two micrometric screws, which allow us to move it in two directions: the propagation one and the same direction of the diffraction (Z and Y axis from Figure 4.3.26). The two beams generated by it cross the BS and are focused in the sample by the objective. Like before, through the ocular lens we can observe these beams to couple them into the waveguides, as seen in Figure 4.3.33(b). By moving the grating closer or farther to the BS, we can control the separation between focused beams to correctly couple each of them into the waveguides of the couplers. Moreover, by displacing vertically the grating, a phase shift is added between the beams. Particularly, a displacement of half a period (30 μm) corresponds to a phase shift of 2π between them.



(a) (b)

Figure 4.3.33: Projection system. Figure (a) shows the diffraction grating and its support. Figure (b) shows the three waveguides of the IQP and the two diffracted beams at their side, as observed through the ocular lens.

Taking into account the operator transformations of a coupler (eq. (4.1.4)), the probability of a photon coming out from any of both outputs from the coupler, which corresponds to the classical intensity

$$I_{1|2} = \langle 1_1|1_2\rangle \frac{1}{2}\left[1 \pm \sin\left(2\kappa z\right)\sin\theta\right], \tag{4.3.58}$$

where $\theta = \delta_i$ is the relative phase between the beams introduced by the grating. Now, to do the projection test, we are interested in the couplers with $\kappa z = \pi/4$ as they are the ones that implement a full projection when the incoming light beams are identical, as shows equation (4.3.58). In particular, we used the couplers from the buried IQP AC2K2. This sample is preferred because, as previously explained, superficial samples have a strong inner polarization coupling. Besides, its coupler $(6.0\,\mu m, 1.5\,mm)$ from Table 4.13 is the closest one to a perfect 50-50 coupler, and so, is the one in which we focused. To avoid losses in the reference waveguide, the sample was turned around. In this way, former outputs 2 and 3 are used now as the inputs where we couple the two beams, while the two original inputs 1 and 2 are now used as outputs (Fig. 4.2.7). Nonetheless, some losses in output 1 due to the Y-junction were still observed. In this way, when light came out entirely from output 1, its intensity was lower than when it came exclusively from output 2.

By displacing the grating few micrometers and taking measures of light intensities in both outputs, we can characterize the coupling. In particular, we took measures each two micrometers. Moreover, the measurements of intensity in output 1 had to be corrected due to the losses in the Y-junction, by taking into account that these losses are given by $1 - I_1^{(max)}/I_2^{(max)}$, where $I_i^{(max)}$ is the maximum measured intensity when light comes out from output $i = 1, 2$.

The characterization of the coupler is represented in Figure 4.3.34 comparing it to theoretical curves (4.3.58). In the figure, we can perfectly observe the sinusoidal behaviour of the light outputs in function of the grating movement. Maximum and minimum experimental values do not reach 1 and 0 due to background light and the coupler not being actually a perfect $\pi/4$-coupler. We also observe that a full cycle is completed for a displacement of 30 μm, which corresponds to a phase 2π.

The most important cases for us are those that correspond to phases $\theta = 0$, $\pi/2$, π and $3\pi/2$, as these are the cases which simulate the quantum states used in the BB84 protocol. As we can see in the figure, for phase shifts 0 and π, light comes out with the same intensity in both outputs. On the contrary, when the phase shift applied is $\pi/2$ or $3\pi/2$, we have maximums and minimums of light, which means that light comes out either in the upper or lower output respectively. Figure 4.3.35 shows the light coming out of both outputs for such cases.

In conclusion, this coupler works as a measure device for two dimensional quantum vortex states $\left(|1_1\rangle \pm i\,|1_2\rangle\right)/\sqrt{2}$. Whenever such single-photon state hits the system, the photon exits it by one of the outputs depending on the state. Meanwhile, if the states hitting the IQP are the ones belonging to the other MUB $\left(|1_1\rangle \pm |1_2\rangle\right)/\sqrt{2}$, the photon gets out randomly by one of the outputs with a 50% of probability.

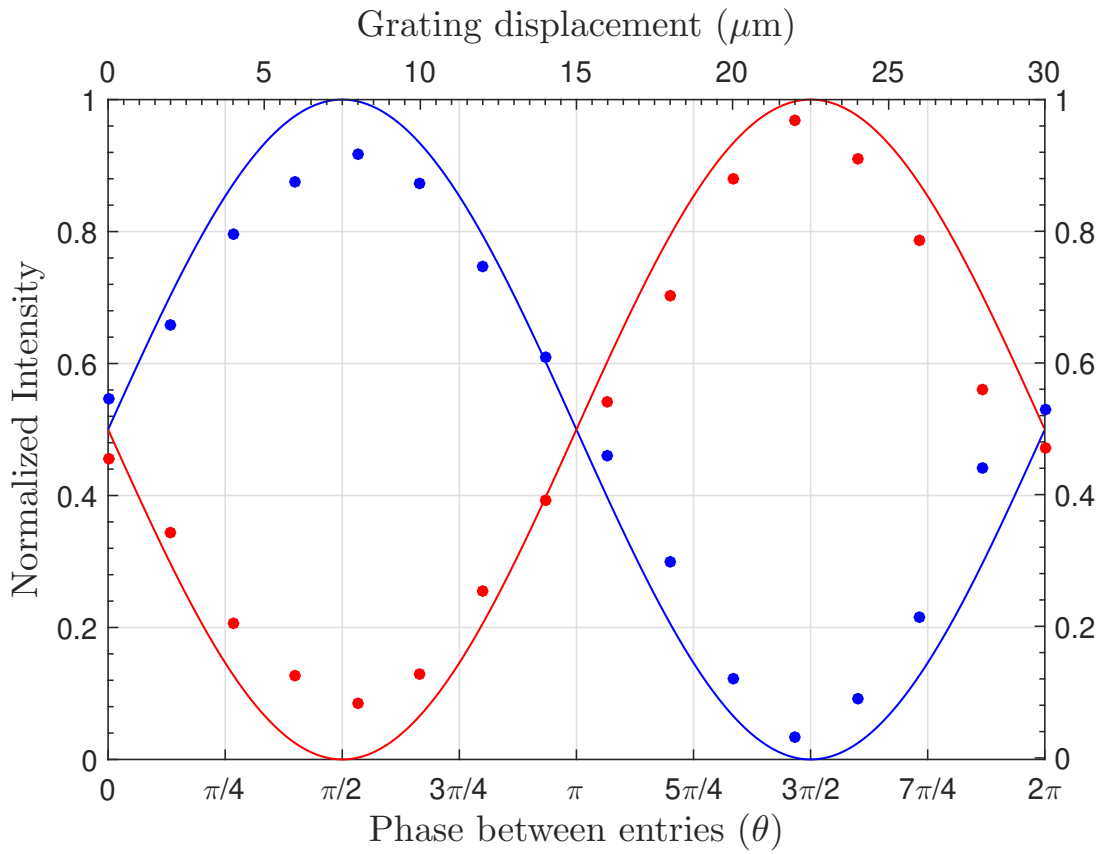
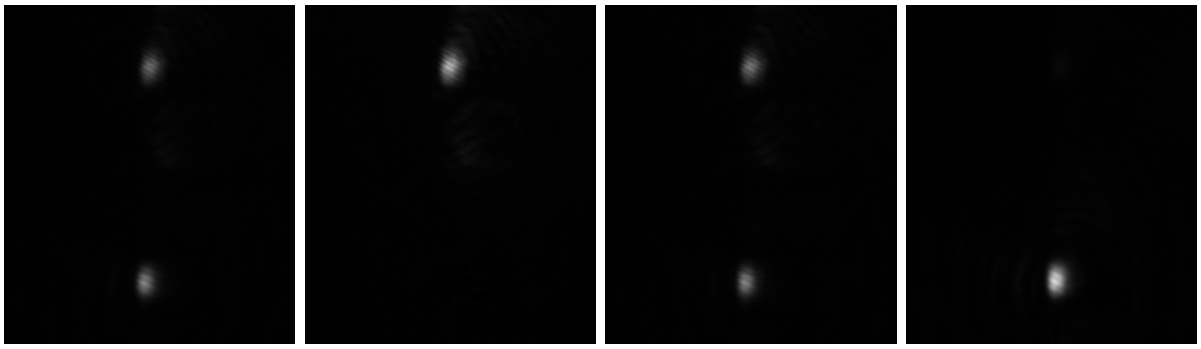


Figure 4.3.34: Light intensities in both outputs in function of the displacement of the grating (upper x-axis) and the introduced phase between beams (lower x-axis). The line represents the theoretical curve of a $\pi/4$-coupler. Blue line represents output 1 and the red line, ouptut 2.



(a) $\frac{1}{\sqrt{2}}(1,1)$ (b) $\frac{1}{\sqrt{2}}(1,i)$ (c) $\frac{1}{\sqrt{2}}(1,-1)$ (d) $\frac{1}{\sqrt{2}}(1,-i)$

Figure 4.3.35: Light output after introducing two identical light beams from both inputs changing the phase ϕ between them: (a) $\phi = 0$, (b) $\phi = \pi/2$, (c) $\phi = \pi$, (d) $\phi = 3\pi/2$.

5

Autocompensating Quantum Cryptography in Multicore Fibers

Apart from FMFs, multicore fibers (MCF) have a high potential in optical communications, as they allow to increase the data bandwidth through space division multiplexing. Naturally, the possibility of using MCFs to implement quantum cryptography has started to be explored. In particular, the utilization of the different modes from the different cores in a MCF (different path modes) constitutes a natural way to perform spatial high-dimensional cryptography [Dynes et al., 2016, Cañas et al., 2017]. Moreover, the use of MCFs with integrated devices like the IQPs explored in the previous chapter is absolutely natural. Just like with FMFs, MCFs are also subjected to modal crosstalk and random intermodal phases. MCFs great advantage over FMFs manifest in the lower, although existing, modal crosstalk between the different cores, which can be minimized with the separation between them. Nonetheless, different cores suffer from different propagation phases, time delays and phase fluctuations, which are also randomized during transmission as a consequence of the environment changes. A high dimensional autocompensating system is thus required in order to compensate all these fluctuations.

In this chapter we present two different methods to implement autocompensating HD-QKD through MCFs. The first method consists of a variation of the multi-loop autocompensating system already introduced in chapter 3, but using path modes instead of collinear spatial ones. The second method proposed by us is a new original one that makes use of the non-linear effect known as phase conjugation to implement an autocompensating system. This chapter is structured in the following way. First, sections 5.1 and 5.2 are an introduction to both proposed methods. Then, we annexe two works where such methods are explained in detail: paper P4 [Balado et al., 2019] is about the multi-loop autocompensation system, while paper P5 [Liñares et al., 2020] presents the autocompensation system based in phase conjugation.

5.1 Autocompensation by multi-loop propagation

In chapter 3 we presented an general scheme to implement autocompensating HD-QKD in FMFs by establishing a multi-loop propagation system. Section 3.2 introduced the general protocol and a simple particularization to implement the regular two dimensional BB84 protocol with spatial modes. Afterwards, in our work P3 [Balado Souto et al., 2019], we detailed the autocompensating system needed for four dimensions. The biggest drawback of our system is that it makes use of bulk optics with discrete photonic devices, which means that for bigger dimensions the required devices will be bigger and more complex.

Integrated devices are a far more preferable approach for quantum information processing, either in cryptography or other technologies as quantum computing. In the previous chapter 4, we demonstrated the feasibility of manufacturing DCs in glass with ion exchange and characterized them in order to be able to manufacture any kind of device, such as generators or IQPs needed in QKD. Integrated devices naturally work with path modes and so, they can be used along MCFs. In this section, we present a brief explanation of how to build an autocompensating HD-QKD system by multi-loop propagation with integrated devices and MCFs, that is later expanded in our work [Balado et al., 2019] in section P4.

5.1.1 Multi-loop system with MCFs and integrated devices

Integrated devices can be easily combined with MCFs to implement QKD of dimension D by using path modes. In this way, we can make use of the fundamental modes of N different waveguides, each one connected to a different core of a MCF, to generate a single-photon state excited in any of such spatial path modes as

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} e^{i\theta_i} |1_i\rangle = \frac{1}{\sqrt{N}} \left(e^{i\theta_1} |1_1\rangle + e^{i\theta_2} |1_2\rangle + \cdots + e^{i\theta_N} |1_N\rangle \right), \tag{5.1.1}$$

where $i = 1, 2, ..., N$ represents each of the N different paths (waveguides/cores) and θ_i are the different phases introduced at each mode in order to generate all the possible states of the MUBs of dimension $D = N$.

In Figure 5.1.1 we present the basic scheme needed to implement autocompensation by multi-loop propagation in MCFs. The biggest difference with respect to sketch for autocompensation with spatial modes in FMFs, shown in Figure 3.2.4, is that no M/DM is required. This is because with path modes there is no need to delay modes, and multiplex and demultiplex them, in order to be able to introduce phase shifts between them. Now, implementing an EFM and a RTC is still fundamental to establish a multi-loop system. As we are using spatial modes, the former can be implemented through a system of integrated optical circulators, as shown in Figure 5.1.2, obtaining the wished transformation (3.2.17). Regarding the latter, instead of complex interferometric systems required for collinear

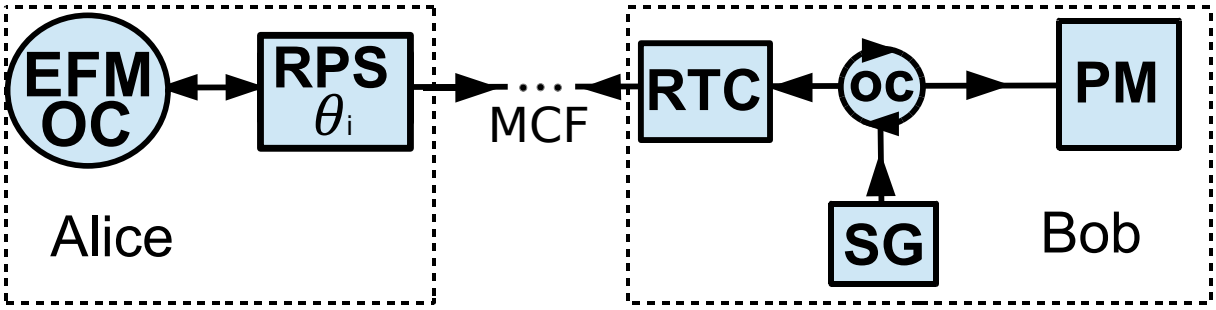


Figure 5.1.1: Basic setup of autocompensating high-dimensional cryptography by multi-loop propagation in MCFs. Bob's system: SG, quantum state generator; OC, optical circulators; RTC, round trip controller; PM, projective measurement device. Alice's system: RPS, relative phase shifter; EFM-OC, effective Faraday mirror (optical circulators).

spatial mode, like the one explained in subsection P3.3.2 (Fig. P3.3(a)), the RTC needed to selectively keep and extract the states from the loop can easily be implemented with reconfigurable directional couplers (RDC) and mirrors or optical circulators. Moreover, an EFM can be used after the RDC leading to a reduction in half of the necessary loops.

With respect to the state generator (SG) and the projective measurement device (PM), integrated devices must be designed. As a SG, for example, our proposed device in [Barral et al., 2016] (section P2) generalized for more dimensions (subsection 2.4.3) could be used. However, the SG only needs to generate the base state (5.1.1) with $\theta_i = 0$ for $i = 1, \cdots, N$, as Alice will introduce the phase shifts θ_i with her RPS. Thus, a simpler device may be used, as proposed in [Balado et al., 2019]. In the case of PMs, we can use the IQPs explained in section 4.1 from chapter 4, following, for example, de Guise factorization [de Guise et al., 2018] in order to design them. In said chapter, we were able to obtain a simple IQP of dimension $D = 2$ in glass. Now, we have also proposed a better factorization for designing IQPs for dimension $D = N = 2^m$ in [Balado et al., 2019].

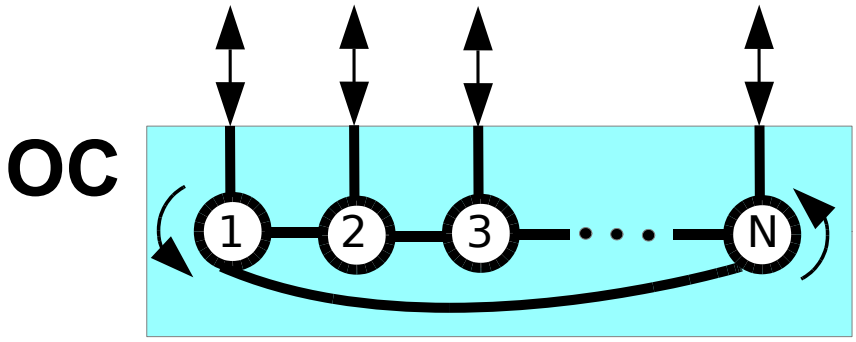


Figure 5.1.2: Effective Faraday mirror implemented with integrated optical circulators.

5.1.2 Proposed autocompensation system

In our work *Phase and polarization autocompensating N-dimensional quantum cryptography in multicore optical fibers* published on *Journal of the Optical Society of America B* **36** (10) in 2019, [Balado et al., 2019], we proposed an autocompensating system for a general dimension $D = N$, based in multi-loop propagation to be implemented with MCFs an integrated devices. Our work is included as section P4 and it is structured and summarized as follows.

First, subsection P4.1 is the introduction to our work, where the problem is presented. Next, in subsection P4.2 we present the N-dimensional autocompensating method based in multi-loop propagation. Particularly, we start by presenting the primary quantum state generator in P4.2.1 and explain the autocompensating process in P4.2.2. The idea of our system, shown in Figure P4.2, is that Bob generates a coherent state and sends it to Alice. Alice's subsystem has a closed circuit with an OC and a HWP that resends the state back to Bob correcting polarization fluctuations in each core. Through reconfigurable directional couplers (RDC), Bob sends the state to a set of OCs that exchange the modes between of the waveguides, as (3.2.14), and send them back to Alice. In the Nth loop, Alice attenuates the coherent state to a single photon state and, when reaching Bob, the RDC sends it to the measurement system. Additionally, a brief analysis about the maximum transmission distance allowed by our system, as well as the transmission rate of the same, is made in P4.2.3.

Afterwards, subsection P4.3 explains how the qudits are obtained by attenuating the original coherent state through a proposed electro-optical attenuator (EOA) and phase shifting the different waveguides. MUBs for the particular case of $D = N = 2^m$ are shown (already showed in subsubsection 2.4.1 from chapter 2). It is worth noting that the use of a coherent state during the autocompensation process has several advantages. First, losses during transmission help to attenuate the state and don't result in losses of single-photon states. Also, this allows to make good use of the decoy states protocol explained in subsection 3.3.1 of chapter 3.

Moreover, in subsection P4.4 IQPs for our qudits measurement are presented. Particularly, we show devices for dimensions $N = 4$, $N = 8$ and a generalization for the case $N = 2^m$. This generalization constitutes our own factorization of a SU(2^m) projection transformation into a combination of SU(2) DC transformation. Our factorization only works for dimension $D = N = 2^m$, unlike factorizations explained in subsection 4.1 from chapter 4. Nonetheless, for this particular case, it has several advantages respect to de Guise's factorization [de Guise et al., 2018]. To begin with, it requires a less number of couplers and phase shifters. For example, for dimension 4, our IQP (shown in Figure P4.4) requires five couplers compared to the six from the other factorization (Figure 4.1.3). Dimension 8 needs twenty couplers for our case (Figure P4.5), while it would require twenty eight with de Guise factorization. At the same time, we only make use of $\kappa z = \pi/2$ and $\kappa z = \pi/4$ couplers, as seen in equations (P4.30), (P4.31) and (P4.35), while it is not the same in the other way, as shown in (4.1.17) and (4.1.18). In this way, finding the

right couplers for a given dimension N is not trivial, while in our case (Figure P4.6) the couplers are known (P4.35). Subsection P4.4 also presents a general integrated passive splitter (P4.40), shown in Figure P4.8, in order to randomly select the measurement basis.

Finally, a security analysis of our system under the phase-remapping attack is made in subsection P4.5. The analysis of the PR attack for a general multi-loop autocompensating system of dimension $N = 2^m$, employing the presented MUBs, was already explained in detail in subsection 3.3.3 of chapter 3. Then, conclusions are presented in subsection P4.6.

5.2 Autocompensation by phase conjugation

In this section we are going to introduce a new autocompensation method based in the non-linear phenomenon of phase conjugation. We have first proposed this method in a contribution to the conference *European Optical Society Annual Meeting (EOSAM) 2020* [Liñares-Beiras et al., 2020] and it has been expanded in the work *Fully autocompensating high-dimensional quantum cryptography by optical phase conjugation*, still to be published [Liñares et al., 2020], which is annexed as section P5.

5.2.1 Phase conjugation of coherent states

5.2.1.1 Degenerate four-wave mixing

Degenerate four-wave mixing (FWM) is a non-linear process that consists of the mutual interaction in a non linear medium between four different waves of the same frequency [Mandel and Wolf, 1995]. The scheme of the process is shown in Figure 5.2.3. Two of the waves (1 and 2) act as classic counter-propagating pumps that are introduced to the non-linear crystal and interact with the perpendicularly incident signal (s) and idler (i) waves, which are also counter propagating between them. As a result of this

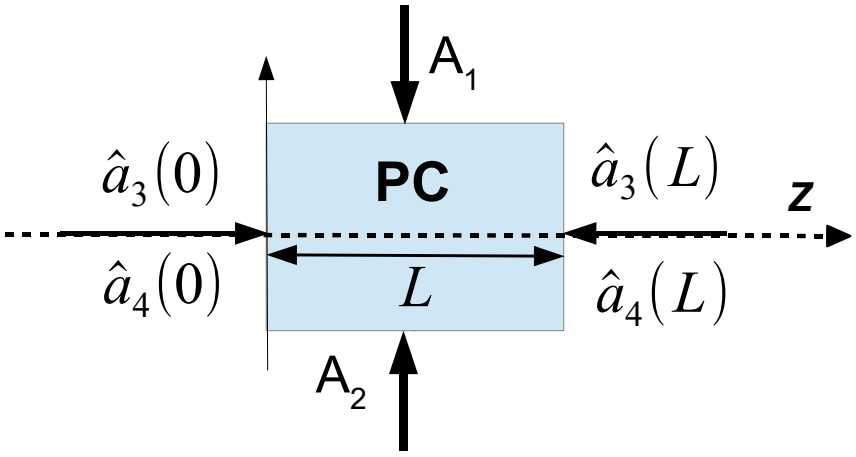


Figure 5.2.3: Four-wave mixing with two pump waves.

interaction, two photons are absorbed from the pump beams and are created in the signal and idler beams. FWM is differentiated from SPDC, explained in section 2.1.3, in the fact that four propagating waves are involved in the former, as opposed to the three of the latter.

The interaction Hamiltonian of this process can be written as an integral of the four waves over the volume V of the non-linear medium, as follows

$$\hat{H}_I = \int_V \chi^{(3)}_{ijlm} \mathbf{E}^{(1)}_i(\mathbf{r},t)\mathbf{E}^{(2)}_j(\mathbf{r},t)\mathbf{E}^{(s)}_l(\mathbf{r},t)\mathbf{E}^{(i)}_m(\mathbf{r},t), \tag{5.2.2}$$

where $\mathbf{E}^{(1)}_l$ and $\mathbf{E}^{(2)}_l$ are the classical pump waves and $\mathbf{E}^{(s)}_l$ and $\mathbf{E}^{(i)}_l$ are the quantized signal and idler waves. These waves can be expressed as

$$\mathbf{E}^{(1)}(\mathbf{r},t) = \mathcal{E}_1 \mathbf{u}_1 e^{i\omega(x/c_m - t)} + \mathcal{E}_1^* \mathbf{u}_1 e^{-i\omega(x/c_m - t)}, \tag{5.2.3a}$$

$$\mathbf{E}^{(2)}(\mathbf{r},t) = \mathcal{E}_2 \mathbf{u}_2 e^{i\omega(-x/c_m - t)} + \mathcal{E}_2^* \mathbf{u}_2 e^{-i\omega(-x/c_m - t)}, \tag{5.2.3b}$$

$$\hat{\mathbf{E}}^{(s)}(\mathbf{r},t) = \hat{a}_3(z/c_m - t)\mathbf{u}_3 e^{i\omega(z/c_m - t)} + \hat{a}_3^\dagger(z/c_m - t)\mathbf{u}_3 e^{-i\omega(z/c_m - t)}, \tag{5.2.3c}$$

$$\hat{\mathbf{E}}^{(i)}(\mathbf{r},t) = \hat{a}_4(z/c_m + t)\mathbf{u}_4 e^{i\omega(-z/c_m - t)} + \hat{a}_4^\dagger(z/c_m - t)\mathbf{u}_4 e^{-i\omega(-z/c_m - t)}, \tag{5.2.3d}$$

where c_m is the phase velocity of the waves in the medium and $\mathbf{u}_j$ $(j = 1, 2, 3, 4)$ are unit polarization vectors. $\mathcal{E}_{1|2}$ and $\hat{a}_{3|4}$ are the pumps complex amplitudes and the signal and idler complex operators respectively, and in both cases are function of $(z/c_m \pm t)$.

Considering that the dimensions of the medium V are far larger than the beams wavelength $\lambda = 2\pi c_m/\omega$, once expressions (5.2.3) are substituted into equation (5.2.2), all crossed therms with in which the oscillatory exponential factors cancel become the main contribution. In this way, equation (5.2.2) becomes

$$\begin{aligned}\hat{H}_I = V\chi^{(3)}_{ijlm}\left(\mathcal{E}_1\mathcal{E}_2\hat{a}_3^\dagger\hat{a}_4^\dagger\mathbf{u}_{1i}\mathbf{u}_{2j}\mathbf{u}^*_{3l}\mathbf{u}^*_{4m} + \mathcal{E}_1^*\mathcal{E}_2^*\hat{a}_3\hat{a}_4\mathbf{u}^*_{1i}\mathbf{u}^*_{2j}\mathbf{u}_{3l}\mathbf{u}_{4m}\right)& \\ = \hbar f\left(\mathcal{E}_1\mathcal{E}_2\hat{a}_3^\dagger\hat{a}_4^\dagger + \mathcal{E}_1^*\mathcal{E}_2^*\hat{a}_3\hat{a}_4\right),&\end{aligned} \tag{5.2.4}$$

where f is a real frequency.

5.2.1.2 Operator propagation equations

Applying the Hamiltonian (5.2.4), we can obtain the temporal Heisenberg equations of FWM [Mandel and Wolf, 1995] using (2.1.12)

$$\begin{aligned}\frac{\partial \hat{a}_3}{\partial t} &= -if\mathcal{E}_1\mathcal{E}_2\hat{a}_4^\dagger, \\ \frac{\partial \hat{a}_4}{\partial t} &= -if\mathcal{E}_1\mathcal{E}_2\hat{a}_3^\dagger.\end{aligned} \tag{5.2.5}$$

Taking into account that operators $\hat{a}_3$ and $\hat{a}_4$ are function of $(z/c_m + t)$ and $(z/c_m - t)$ respectively, the spatial and time derivates are related as

$$\begin{aligned} \frac{\partial \hat{a}_3}{\partial t} &= -V\frac{\partial \hat{a}_3}{\partial z}, \\ \frac{\partial \hat{a}_4}{\partial t} &= V\frac{\partial \hat{a}_4}{\partial z}\hat{a}_3^\dagger. \end{aligned} \tag{5.2.6}$$

Thus, the time Heisenberg equations (5.2.5) can be transformed into spatial equations as

$$\begin{aligned} \frac{\partial \hat{a}_3}{\partial z} &= \frac{if}{V}\mathcal{E}_1\mathcal{E}_2\hat{a}_4^\dagger, \\ \frac{\partial \hat{a}_4}{\partial z} &= -\frac{if}{V}\mathcal{E}_1\mathcal{E}_2\hat{a}_3^\dagger. \end{aligned} \tag{5.2.7}$$

This system can be uncoupled by differentiating once, obtaining the following oscillator equations

$$\begin{aligned} \frac{\partial^2 \hat{a}_3}{\partial z^2} &= -\frac{f}{V}\left\|\mathcal{E}_1\mathcal{E}_2\right\|\hat{a}_3^\dagger, \\ \frac{\partial^2 \hat{a}_4}{\partial z^2} &= -\frac{f}{V}\left\|\mathcal{E}_1\mathcal{E}_2\right\|\hat{a}_4^\dagger, \end{aligned} \tag{5.2.8}$$

whose solutions are given by

$$\begin{aligned} \hat{a}_3(z) &= \hat{a}_3(0)\cos(Kz) + i\hat{a}_4^\dagger(0)e^{i(\epsilon_1+\epsilon_2)}\sin(Kz), \\ \hat{a}_4(z) &= \hat{a}_4(0)\cos(Kz) - i\hat{a}_3^\dagger(0)e^{i(\epsilon_1+\epsilon_2)}\sin(Kz), \end{aligned} \tag{5.2.9}$$

where we have defined $K = \frac{f}{V}\left\|\mathcal{E}_1\mathcal{E}_2\right\|$ and $\mathcal{E}_j = \|\mathcal{E}_1\|e^{i\epsilon_j}$ $(j = 1, 2)$.

As shown in Figure 5.2.3, let us considerate L to be the non-linear medium length. We can consider as well, that wave 3 is incident from the right while wave 4 incises from the left. In this way we can define the input and output operators of both waves as

$$\begin{aligned} \hat{a}_3(0) \equiv \hat{a}_{3out}, \quad \hat{a}_3(L) \equiv \hat{a}_{3in}, \\ \hat{a}_4(0) \equiv \hat{a}_{4in}, \quad \hat{a}_4(L) \equiv \hat{a}_{4out}. \end{aligned} \tag{5.2.10}$$

Therefore, if we put $z = L$, we can obtain the input/output operator transformations from equations (5.2.9)

$$\begin{aligned} \hat{a}_{3out} &= \hat{a}_{3in}\sec(KL) - i\,\hat{a}_{4in}^\dagger e^{i(\epsilon_1+\epsilon_2)}\tan(KL) \\ \hat{a}_{4out} &= \hat{a}_{4in}\sec(KL) - i\,\hat{a}_{3in}^\dagger e^{i(\epsilon_1+\epsilon_2)}\tan(KL) \end{aligned} \tag{5.2.11}$$

or, in the inverse form,

$$\begin{aligned} \hat{a}_{3in} &= \hat{a}_{3out}\sec(KL) + i\,\hat{a}_{4out}^\dagger e^{i(\epsilon_1+\epsilon_2)}\tan(KL) \\ \hat{a}_{4in} &= \hat{a}_{4out}\sec(KL) + i\,\hat{a}_{3out}^\dagger e^{i(\epsilon_1+\epsilon_2)}\tan(KL) \end{aligned} \tag{5.2.12}$$

5.2.1.3 Application to the coherent state

Let us consider two coherent states incident in each input of the non linear medium $|\alpha_3\rangle\,|\alpha_4\rangle$, where $\alpha_j = \|\alpha_j\|e^{i\epsilon_j}$. Taking into account the definition of a coherent state (2.1.15)

$$|L_{in}\rangle = e^{\alpha_3\hat{a}^\dagger_{3in}-\alpha_3^*\hat{a}_{3in}}e^{\alpha_4\hat{a}^\dagger_{4in}-\alpha_4^*\hat{a}_{4in}}\,|0_30_4\rangle = |\alpha_{3in}\rangle\,|\alpha_{4in}\rangle \tag{5.2.13}$$

applying expressions (5.2.12) in it we obtain

$$\begin{gathered}|L_{out}\rangle = e^{\alpha_3\left(s\hat{a}^\dagger_{3out}-i\,t\hat{a}_{4out}\right)-\alpha_3^*\left(s\hat{a}_{3out}+i\,t\hat{a}^\dagger_{4out}\right)}e^{\alpha_4\left(s\hat{a}^\dagger_{4out}-i\,t\hat{a}_{3out}\right)-\alpha_4^*\left(s\hat{a}_{4out}+i\,t\hat{a}^\dagger_{3out}\right)}\,|0_30_4\rangle = \\ e^{\left(s\alpha_3-it\alpha_4^*\right)\hat{a}^\dagger_{3out}-\left(s\alpha_3^*+it\alpha_4\right)\hat{a}_{3out}}e^{\left(s\alpha_4-it\alpha_3^*\right)\hat{a}^\dagger_{4out}-\left(s\alpha_4^*+it\alpha_3\right)\hat{a}_{4out}},\,|0_30_4\rangle = \\ |s\alpha_3 - it\alpha_4^*\rangle\,|s\alpha_4 - it\alpha_3^*\rangle\,,\end{gathered}$$

where we have defined $s = \sec(KL)$ and $t = \tan(KL)$. Thus, the output state of the FWM is

$$|L_{out}\rangle = |s\alpha_3 - it\alpha_4^*\rangle\,|s\alpha_4 - it\alpha_3^*\rangle\,. \tag{5.2.14}$$

From (5.2.14), or equations (5.2.11), it is easy to obtain the expectation values of output operators $\hat{a}_{3out}$ and $\hat{a}_{4out}$, recalling that $\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$, which will be

$$\begin{aligned}\langle\hat{a}_{3out}\rangle_{|L_{out}\rangle} &= \alpha_3\sec(KL) - i\alpha_4^*e^{i(\epsilon_1+\epsilon_2)}\tan(KL),\\ \langle\hat{a}_{4out}\rangle_{|L_{out}\rangle} &= \alpha_4\sec(KL) - i\alpha_3^*e^{i(\epsilon_1+\epsilon_2)}\tan(KL).\end{aligned} \tag{5.2.15}$$

These represent the intensities of output states and we can see how they are an interaction of the input intensities augmented by spontaneous emission within the medium.

Now, it is also interesting to calculate the mean photon number of the output states. Employing again equations (5.2.11)

$$\begin{gathered}\langle\hat{n}_{4out}\rangle = \langle\hat{n}_{4in}\rangle\sec^2(KL) + (\langle\hat{n}_{3in}\rangle + 1)\tan^2(KL) \\ + \left[ie^{-i(\epsilon_1+\epsilon_2)}\langle\hat{n}_{3in}\hat{n}_{4in}\rangle + ie^{-i(\epsilon_1+\epsilon_2)}\langle\hat{n}^\dagger_{3in}\hat{n}^\dagger_{4in}\rangle\right]\sec^2(KL)\tan^2(KL) = \\ \|\alpha_4\|^2\sec^2 KL + \left(\|\alpha_3\|^2+1\right)\tan^2 KL + \left[i\alpha_3\alpha_4e^{-i(\epsilon_1+\epsilon_2)} - i\alpha_3^*\alpha_4^*e^{i(\epsilon_1+\epsilon_2)}\right]\sec^2 KL\tan^2 KL\end{gathered} \tag{5.2.16}$$

We can see that even when α_3 and α_4 are zero, $\langle\hat{n}_{3out}\rangle$ grows with $\tan^2(KL)$ because of spontaneous emission.

5.2.1.4 Phase conjugation

Let us suppose now that we have no idler wave incident from the left ($\alpha_4 = 0$), this is, we only have a signal coherent state incising into the non-linear medium pumped by the classical beams. In this way, we have state

$$|L_0\rangle = e^{\alpha\hat{a}^\dagger_{3in}-\alpha^*\hat{a}_{3in}}\,|0_30_4\rangle = |\alpha_30_4\rangle\,. \tag{5.2.17}$$

Trivially, the output state will be given by equation (5.2.14) making $\alpha_4 = 0$, so we get

$$|L_c\rangle = |s\alpha\rangle_3 \, |-it\alpha^*\rangle_4 \, . \tag{5.2.18}$$

Therefore, when a coherent state $|\alpha\rangle$ incises over a non-linear medium stimulated by two counter-propagated pumps we obtain two coherent states, one transmitted (3) and one reflected (4).

The interesting output is the reflected wave. By looking at the expectation value of its operator 5.2.15

$$\langle \hat{a}_{4out} \rangle_{|L_c\rangle} = -i\alpha^* e^{i(\epsilon_1+\epsilon_2)} \tan(KL), \tag{5.2.19}$$

we can see how it is proportional to $\alpha^* = \|\alpha\| e^{-i\epsilon}$ instead of $\alpha = \|\alpha\| e^{i\epsilon}$ like in a regular reflection. Thus, while the incident state carries a phase ϵ, the reflected state carries a phase $-\epsilon$. This phenomenon is known as *phase conjugation* (PC) and it is said that FWM work as a phase conjugator mirror.

If a coherent state suffers a phase shift $|e^{i\phi}\alpha\rangle$, this is conjugated as well by the PC as $|e^{-i\phi}\alpha^*\rangle$. This ability is useful to compensate for phase shifts suffered by an incident wave and it has been widely use for different applications like, for example, compensating for wave front distortion in scattering or for phase aberrations of an image forming system [Giuliano, 1981, Agarwal et al., 1982, Agarwal et al., 1983, Wolf et al., 1984].

At the same time, from equation (5.2.16) we can easily evaluate the mean number of photons for this case, which is

$$\langle \hat{n}_{4out} \rangle = \left(\|\alpha\|^2 + 1 \right) \tan^2(KL). \tag{5.2.20}$$

We can see how the mean photon number is given by the intensity of the reflected state $|-it\alpha|^2$ with an aditional photon number given by $\tan^2(KL)$, which takes account for the photons produced by stimulated spontaneous emission. Using expression 5.2.20, it is simple to determine the attenuation needed to reduce the pulse α to have an average of one photon $\hat{n}_{4out}$.

5.2.2 Phase conjugation for HD-QKD

Let us consider a MCF with N different cores in order to support N modes, with operators $\hat{a}_i$, $i = 1, ..., d$, to implement HD-QKD with 1-qudit states. A problem that can arise during transmission is, not only the presence of unpredictable relative phases between the different modes, but the modal coupling that can arise between said modes. As a consequence, a 1-qudit state sent by Alice will reach Bob's system as an unpredictable 1-qudit state. We have previously analysed the relative phase and polarization coupling in MCFs in section P4. However, we are going to study how we can make use of phase conjugation to solve the modal coupling drawback, which includes as well the presence of relative phases.

5.2.2.1 Modal coupling between cores

In a general system, the coupling of N different modes is going to be mathematically described by the Heisenberg equation (2.1.11) for the operators $\hat{a}_i$, as given by (2.1.12), so we have

$$\left\{ -i\hbar \frac{\partial \hat{a}_i}{\partial z} = \hbar \left(\beta_i \sum_j^N \delta_{ij} \hat{a}_j + \sum_j^N \kappa_{ij} \hat{a}_j \right) \equiv \sum_j^N C_{ij} \hat{a}_j, \right\}_i^N \tag{5.2.21}$$

where β_i are propagation constants and κ_{ij} are modal coupling coefficients. These coefficients C_{ij} constitute a symmetric matrix

$$C = \begin{pmatrix} \beta_1 & \cdots & \kappa_{1j} & \cdots & \kappa_{1N} \\ \vdots & \ddots & & & \vdots \\ \kappa_{i1} & & \beta_i & & \kappa_{iN} \\ \vdots & & & \ddots & \vdots \\ \kappa_{N1} & \cdots & \kappa_{Nj} & \cdots & \beta_N \end{pmatrix}. \tag{5.2.22}$$

Solving the differential equation system (5.2.21), we get the matrix

$$S_{ij} = \exp\{iC_{ij}z\}, \tag{5.2.23}$$

which is a complex symmetric matrix, that is, $S_{ij} = S_{ji}$. On the other hand, modal coupling is an unitary transformation, therefore

$$S_{ij}^{-1} = S_{ij}^{\star}. \tag{5.2.24}$$

Next, let us consider q different modal couplings along z direction from Alice to Bob and vice versa, with total transmission matrices

$$T_{A\to B} = S_1 \cdots S_q, \qquad T_{B\to A} = S_q \cdots S_1. \tag{5.2.25}$$

Therefore, after applying phase conjugation to an incident state coming from Bob to Alice, the actual transformation of the state will be

$$T_c = T_{B\to A}^{\star} = S_q^{\star} \cdots S_1^{\star} = S_q^{-1} \cdots S_1^{-1}. \tag{5.2.26}$$

Finally, once the light travels back to Bob, and so, it is subjected to the coupling transformation (5.2.25), the final coupling matrix of the back and forth trip will be given by

$$T_{total} = T_{A\to B} \cdot T_c = \mathbb{I}. \tag{5.2.27}$$

Consequently, the unpredictable modal coupling has successfully been removed.

5.2.2.2 Modal and polarization coupling

Phase conjugation also allows to compensate between polarization modes, either transmitted by the same or by different cores. Considering a MCF of N different cores and taking into account the polarization mode of each spatial one, the Heisenberg equation (5.2.21) can be rewritten as

$$\left\{ -i\hbar \frac{\partial \hat{a}_{ig}}{\partial z} = \hbar \left(\beta_{ig} \sum_{j}^{N} \sum_{p=H,V} \delta_{ig,jp} \hat{a}_{jp} + \sum_{j}^{N} \sum_{p=H,V} \kappa_{ig,jp} \hat{a}_{jp} \right) \equiv \sum_{j}^{N} \sum_{p=H,V} C_{igjp} \hat{a}_{jp} \right\}_{\substack{i=1,\cdots,N \\ g=H,V}} \tag{5.2.28}$$

The solution to this system is given again by equation (5.2.23) where now, each term C_{ij} corresponds to the coupling coefficient κ_{ij} with $i, j = 1H, 1V, \cdots, NH, NV$. However, because of reflection the polarization coordinate system experiments a sign change $x \to -x$ and $z \to -z$ [Yariv, 1987]. Therefore, coupling coefficients between different polarization modes also experiment a sign change as $\kappa_{ig,jp} \to (-1)^{\delta_{g,p}+1} \kappa_{ig,jp}$. As a consequence, the back-propagation coupling matrix can be written as

$$C^{(R)} = D \cdot C \cdot D; \tag{5.2.29}$$

where

$$D = \mathbb{I} \otimes \mathrm{diag}\,(1, -1), \tag{5.2.30}$$

and so, the formal solution to the equation system (5.2.28) is

$$S^{(R)} = \exp\{iC^{(R)} z\} = D \cdot S \cdot D, \tag{5.2.31}$$

The transmission matrix from Bob to Alice (5.2.26) taking polarization into account, once the phase conjugation has been made will be

$$T_c^{(P)} = T_{B\to A}^{(P)\star} = S_q^{(R)\star} \cdots S_1^{(R)\star} = D \cdot S_q^{\star} \cdot D \cdots D \cdot S_1^{\star} \cdot D = D \cdot S_q^{-1} \cdots S_1^{-1} \cdot D. \tag{5.2.32}$$

Now, as explained by Yariv [Yariv, 1987], the polarization operator transformation introduced by a PC mirror (which reflects back the state by the incident way) is represented by

$$\begin{pmatrix} \hat{a}_H \\ \hat{a}_V \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \hat{a}_{H0}^{\star} \\ \hat{a}_V^{\star} \end{pmatrix}. \tag{5.2.33}$$

Consequently, matrix D needs to be taken into account when calculating the full propagating transformation, which will be given by

$$T_{A\to B} \cdot D \cdot T_c^{(P)} = D \cdot S_q^{-1} \cdots S_1^{-1} \cdot D \cdot D \cdot S_1 \cdots S_q = D. \tag{5.2.34}$$

We can see that all the spatial and polarization couplings have been compensated except for a π phase shift between H and V modes in each core, which can be easily corrected in BOS before making a projective measurement.

5.2.3 BB84 autocompensating system

We have shown in subsection 5.2.2 that it is possible to employ PC to design an autocompensating optical system to implement HD-QKD. In Figure 5.2.4 we present the basic scheme of a autocompensating system implementing BB84 protocol. Let us describe this setup.

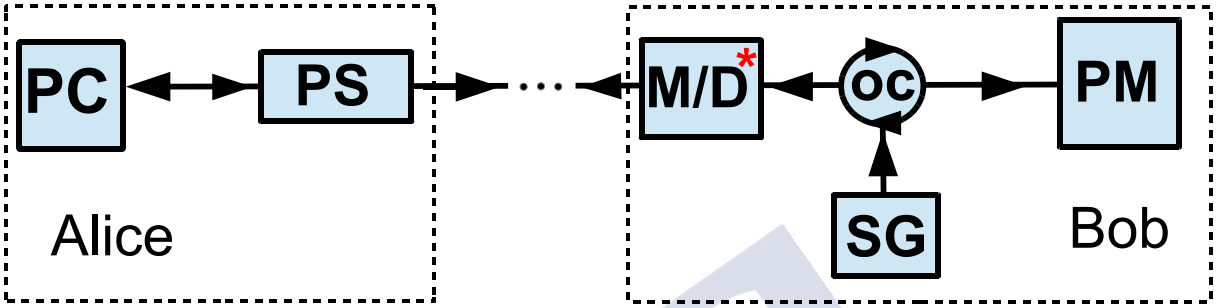


Figure 5.2.4: Basic setup of autocompensating high-dimensional cryptography by phase conjugation. PC, phase conjugation mirror; PS, phase shifter; M/D, multiplexer/demultiplexer; OC, optical circulators; SG, state generator; PM, projective measurement device.

The first device of the system is a state generator (SG) located in Bob system. The SG can consists of a coherent source emitting $|2^{N/2}\alpha\rangle$ followed by a series of concatenated $\pi/4$ DCs, as proposed in [Balado et al., 2019] (subsection P4.2.1) and shown in Figure P4.1. By correcting phases, the SG emits the multimode coherent state

$$|L\rangle = |\alpha_1 \cdots \alpha_N\rangle_3 \,, \tag{5.2.35}$$

excited in the N optical states of a FMF or a MCF. Next, one (for FMFs) or several (for MCFs) optical circulators launch the state towards Alice. A Demultiplexer-Multiplexer (D-M) device is needed to produce delays τ between modes if a FMF is used in order to being able to individually modify each of them, while introducing them for the same optical path of the FMF. In case we use a MCF, then, the M/D device is not required, as each integrated waveguide, carrying an spatial mode each, acts as the input of each core of the MCF.

Once the quantum state (5.2.35) reaches AOS, it crosses a phase shifter system (PS) in off-position and reaches the PC device. As seen in subsubsection 5.2.1.4, taking into account equations (5.2.17) and (5.2.18), it is trivially that, in the PC, state (5.2.35) is going to become the following state

$$|L_c\rangle = (|s\alpha_1\rangle_3 \, |-it\alpha_1^*\rangle_4) \cdots (|s\alpha_N\rangle_3 \, |-it\alpha_N^*\rangle_4) \,, \tag{5.2.36}$$

where $s = \sec KL$, $t = \tan KL$ and subindex $3, 4$ refer to te propagating and back-propagating directions respectively. We can see how the portion of multimode coherent

state returning to Bob is conjugated

$$|L_c\rangle_4 = |-it\alpha_1^*, \cdots, -it\alpha_N^*\rangle_4 \,. \tag{5.2.37}$$

We must stress that each single mode coherent state (a core in a MCF) becomes a multimode coherent state due to modal coupling. Then, the reflected state in the PC device goes through the PS system and an attenuator system. The PS system introduces phase shifts θ_i in each of the incoming modes; if a FMF is used a single PS can introduce phases in each delayed state, while if a MCF is used, N PSs can be simultaneously used for each core. At the same time, the attenuator attenuates the multimodal coherent state to the single-photon level. In consequence, Alice sends to Bob the following 1-qudit encrypted state

$$|L_c\rangle = \sum_i \frac{1}{\sqrt{N}} \{e^{i\theta_1} |1_1\rangle + ... + e^{i\theta_N} |1_N\rangle\}. \tag{5.2.38}$$

These states must be encrypted in N-dimensional MUBs. For example, the MUBs for $N = 2^m$ from subsubsection 2.4.1 of chapter 2 can be used.

Finally, state (5.2.38) reaches BOS and finds the D-M device, which cancels the delays τ between states $|1_j\rangle$. Afterwards, the circulator system sends the encrypted state to the PM device to be measured. If the basis $N = 2^m$ (2.4.1) are used, the PM devices can be build by the factorization scheme that we presented in [Balado et al., 2019] (subsection P4.4).

Regarding the security of this autocompensating system, like any other round trip system it is subjected to the phase-remapping attack. Trivially, our security analysis presented in [Balado et al., 2019] (subsection P4.5) and explained in subsection 3.3.3 of chapter 3 is also valid for this system. Additionally, this system has the advantage with respect to the other ones presented in [Balado Souto et al., 2019, Balado et al., 2019] of only need one round trip, although it has the disadvantage of the difficulty of working with a PC system.

As previously told, in the preprint work *Fully autocompensating high-dimensional quantum cryptography by optical phase conjugation* [Liñares-Beiras et al., 2020] we have proposed an autocompensating system to implement HD-QKD based in phase conjugation. Although still unpublished, the work has been annexed as section P5.

This work summarizes and develops what has been already explained in this section and it is structured as follows. First, subsection P5.1 introduces the problem of modal coupling and phase fluctuations. Then, in subsection P5.2, we present the optical phase conjugator (OPC), which acts as the phase conjugation mirror of our system and works with spatial and polarization modes. The following subsections explain the autocompensation process when using codirectional modes from a MCF (subsection P5.3) and when polarization modal coupling is also taken into account (subsection P5.4). This autocompensation is generalized for non symmetric SU($2N$) coupling transformation in subsection P5.5. Next, in subsection P5.6, our proposed autocompensation system is shown. Finally, after a brief comment about free space optical communication in subsection P5.7, our summary is presented in subsection P5.8.

USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

P4 Phase and polarization autocompensating N-dimensional quantum cryptography in multicore optical fibers

JOURNAL OF THE OPTICAL SOCIETY OF AMERICA B
VOL. 36 NO. 10 PAGE 2793-2803
ISSN: 0740-3224 (PRINT), 1520-8540 (ONLINE)
doi: https://doi.org/10.1364/JOSAB.36.002793

PUBLISHED 1 OCTOBER 2019

BY DANIEL BALADO[1], JESÚS LIÑARES[1], XESÚS PRIETO-BLANCO[1] & DAVID BARRAL[2]

[1] OPTICS AREA, DEPARTMENT OF APPLIED PHYSICS, FACULTY OF PHYSICS AND FACULTY OF OPTICS AND OPTOMETRY, UNIVERSITY OF SANTIAGO DE COMPOSTELA, CAMPUS VIDA S/N (CAMPUS UNIVERSITARIO SUR), E-15782 SANTIAGO DE COMPOSTELA, GALICIA, SPAIN

[2] CENTRE DE NANOSCIENCES ET DE NANOTECHNOLOGIES C2N, CNRS, UNIVERSITÉ PARIS-SACLAY, 10 BOULEVARD THOMAS GOBERT, 91120 PALAISEAU, FRANCE

Abstract: *Space division multiplexing based on multicore optical fibers (MCFs) is an optimum candidate to further increase the data bandwidth in optical communications and its interest for spatial high-dimensional quantum cryptography has increased in the last few years. However, the main shortcoming lies in the appearance of phases and polarization acquired independently in each spatial mode after a long propagation, which prevents to implement efficient quantum key distribution (QKD) protocols with spatial optical modes. In this work we propose a method for achieving phase, polarization and time delays autocompensating for N-dimensional QKD in MCFs by using strong coherent states coming from Bob system. These coherent states make N trips between Alice and Bob and undergo N suitable optical transformations before Alice attenuates such states for producing 1-qudit states. Likewise, passive random-projective-measurement integrated devices are presented, as well, in order to measure 1-qudit states. Finally, we analyze the behaviour of the system under a cryptographic attack, like for example the phase-remapping attack, in order to assess the strength of our system.*

Daniel Balado Souto

P4.1 Introduction

Over the last years, space division multiplexing has been proposed to further increase the data bandwidth in optical communications, thus a high interest has arisen about new optical fibers such as few-mode fibers (FMF) and multicore fibers (MCF) [Bai et al., 2012]. Consequently, the interest on the implementation of quantum cryptography in these new optical fibers has remarkably increased in the last few years, particularly if we take into account that spatial high-dimensional cryptography [Mafu et al., 2013, Cozzolino et al., 2019] can be implemented in MCFs in a very natural way [Dynes et al., 2016, Cañas et al., 2017]. It is well-known that a higher degree of security is achieved by increasing the Hilbert space dimension [Leach et al., 2012, Sit et al., 2017, Sheridan and Scarani, 2010]. However, several drawbacks appear, which are related to modal cross-talk and random intermodal phases (and time delays) acquired by spatial modes after long propagation distances. Cross-talk can be notably minimized by using MCFs with well-separated cores. However, it is well known in optical communications that phase together with time delays and polarization are randomized after a long optical fiber transmission. This effect is mainly due to the environment changes during transmission, that is, the phase and polarization of photons drift independently in each core. An obvious solution for mitigating this effect is using a short link distance, nonetheless in a real QKD system random drifts must be considered unavoidably [Ding et al., 2017, Bacco et al., 2016]. These random changes of intermodal phases (and time delays) and polarization can not be eliminated, however they can be autocompensated. Autocompensating techniques have been proposed for polarization modes some years ago and thus restricted to a bidimensional Hilbert space [Muller et al., 1997, Bethune and Risk, 2002]. However, if several spatial modes are considered in high-dimensional QKD protocols, phase drifting and polarization changes can occur in each mode independently. Then, a new autocompensating method, together with the corresponding projective measurement devices, are required.

In this work we propose a phase (and time delay) and polarization autocompensating N-dimensional QKD method to be used in MCFs by launching strong coherent states from Bob system (preliminary results have been recently presented for $N = 4$, that is, a MCF with four cores [Balado et al., 2018]). The mentioned strong coherent states make N trips between Alice and Bob and undergo N suitable circulations between the cores of the MCF in order to get an efficient autocompensation of phase and polarization. Once achieved such compensation Alice attenuates the strong coherent states and generates signal states for implementing a particular QKD protocol, for instance the BB84 one, together with decoy states to detect eavesdropping attacks by any method based on the seminal work proposed by Hwang [Hwang, 2003] with decoy states. We must also stress that our method can also be applied to MDI-QKD protocol [Lo et al., 2012, Xu et al., 2014], that is, by biphoton states such as will be shown in a next work. On the other hand, optical transformations (circulations, phase shifts, etc.) and quantum projective measurements are performed with optical fiber components (mainly optical fiber circulators) and integrated photonic devices, which are fully compatible with MFCs.

Results are explicitly presented for two particular dimensions (N=4, 8), although we will show that the same procedure can be followed for an arbitrary number of N single-mode cores, and in particular, for sake of expositional convenience and without loss of generality, for $N = 2^n$ with n any integer $n \in \mathbb{N}$. We outline that taking into account polarization modes, $2N$ modes are indeed involved. In this work we only focus on spatial modes, but polarization modes could be used because the optical system also achieves autocompensating polarization. Finally, we must indicate that a similar method of phase autocompensation employing spatial LP modes of a few-mode elliptical core fiber has recently been proposed [Balado Souto et al., 2019].

The plan of the work is as follows: in section 2 the N-dimensional autocompensating method is presented together with the corresponding optical system. In section 3 an integrated optical device to generate quantum states is presented for an arbitrary dimension of the Hilbert space, in particular, states belonging to Mutually Unbiased Bases (MUBs) are obtained. In section 4 random projective measurements based on integrated optical devices are presented and analyzed for dimensions N=4, N=8 and arbitrary dimension N. In section 5, we perform a security analysis of our system, by studying how it behaves under some specific attacks our system allows. In section 6 conclusions are presented.

P4.2 N-dimensional autocompensating method

P4.2.1 Primary quantum state generator

We show in Fig. P4.1 (a) an example of optical integrated circuit formed by $N-1$ bimodal directional couplers with arguments $\tilde{\kappa} = \kappa L = \pm\pi/4$, where L is the interaction length in each coupler, that is,

$$M_{\tilde{\kappa}} = \begin{pmatrix} \cos\tilde{\kappa} & i\sin\tilde{\kappa} \\ i\sin\tilde{\kappa} & \cos\tilde{\kappa} \end{pmatrix}; \quad M_{\pm\pi/4} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \pm i \\ \pm i & 1 \end{pmatrix}. \tag{P4.1}$$

These particular directional couplers are denoted as $M_{\pi/4}$ and $M_{-\pi/4}$. This integrated circuit can generate quantum states in a N-dimensional Hilbert space with $N=2^n, n \in \mathbb{N}$, although, other couplers and/or topologies can be used. For instance, by using trimodal directional couplers states of dimension $N = 3^m, m \in \mathbb{N}$ can be obtained. Let us consider a coherent state $|\alpha\rangle$ launched into the first coupler as shown in Fig. P4.1 (a). We assume, for instance, that it is a linearly polarized coherent state. Hence, the optical integrated circuit, shown in Fig. P4.1, generates the following primary multimode coherent quantum state

$$|L_e\rangle = |2^{-\frac{n}{2}} e^{i\epsilon_1}\alpha\rangle\, |2^{-\frac{n}{2}} e^{i\epsilon_2}\alpha\rangle \,....\, |2^{-\frac{n}{2}} e^{i\epsilon_{N-1}}\alpha\rangle |2^{-\frac{n}{2}} e^{i\epsilon_N}\alpha\rangle, \tag{P4.2}$$

with $N=2^n$, ϵ_j integer multiples of phase $\pi/2$ and $j = 1, \ldots N$. We assume that these phases are cancelled by using phase shifters at the end of the integrated device. We outline that such phase cancellation is not necessary to obtain the QKD, and thus we obtain a simpler description of the whole system.

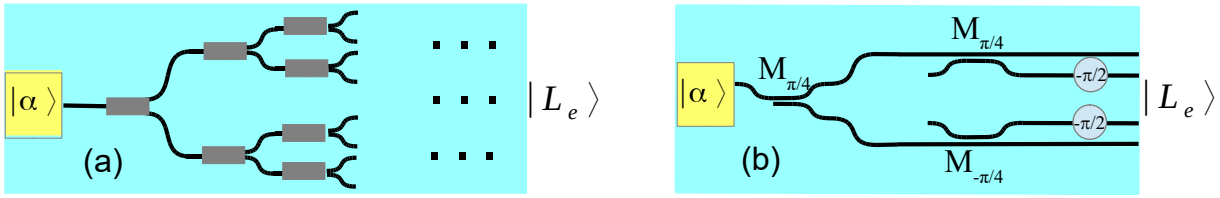


Figure P4.1: Primary quantum state generator from a coherent source (a). The case $N = 4$ with phase cancellation is shown in (b).

In Fig. P4.1.b an example for N=4 is shown. The emerging state is given by the expression $|L_e\rangle = |2^{-1}\alpha\rangle\,|2^{-1}e^{i\pi/2}\alpha\rangle|2^{-1}e^{-i\pi/2}\alpha\rangle|2^{-1}\alpha\rangle$ with phases $\epsilon_1 = \epsilon_4 = 0$, $\epsilon_2{=}\pi/2$ and $\epsilon_3{=}-\pi/2$. Note that, as commented before, phases $\pm\pi/2$ can easily be cancelled by using $-\pi/2$-shifters as shown in Fig. P4.1.b.

The state generator (SG) device is located in the Bob optical system (BOS) as shown in Fig. P4.2. After the SG device, N single mode optical fibers (SMF) are used and connected to optical circulators (OC_1) as shown in Fig. P4.2.

P4.2.2 Autocompensating process

The set of circulators OC_1 carries the quantum state (P4.2) from the SG up to Alice optical system (AOS) through SMFs. The coupling from the SMFs to the MCFs, connecting AOS with BOS, is performed by using reconfigurable directional couplers (RDCs). For instance, an electro-optical coupler taking values $\kappa L = \pi/2, \pi$, that is, couplers $M_{\pi/2}$ and M_π, or respectively, switching (on-position) and non-switching (off-position). From expression (P4.1) the transformations corresponding to these couplers are

$$M_{\pm\pi/2} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}; \quad M_{\pm\pi} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{P4.3}$$

When the RDCs take the on-position, light is coupled directly to the photonic lantern (PL) and then to the MCF, as shown in Fig. P4.2. Once the pulses are coupled into the MCF then the RDCs take the off-position, which prevents light returning from AOS to go to circulators OC_1, but allows light to reach the set of circulators OC_2.

The light pulses arrive at AOS coming from N SMFs emerging from a second PL (left), as shown in Fig. P4.2. The autocompensating process for polarization and spatial modes is obtained by loop devices, located at the end of these SMFs in AOS. These loops allow to send back the pulses to BOS. Moreover, Alice is able to generate the different quantum states by a phase modulation within these loop devices. Each loop device consists of a circulator (OC_3) and a half wave plate (HWP), working similarly to a Faraday mirror in free space [Bethune and Risk, 2002].Likewise, inside the loops there are electro-optical phase shifters for generating the quantum states such as will be shown in the next section. Finally, optical fiber delays could be included in the loop devices if necessary.

It is easy to check that the polarization state reaching the BOS is restored after one round-trip. The perturbations that the polarization undergoes across the MCF are

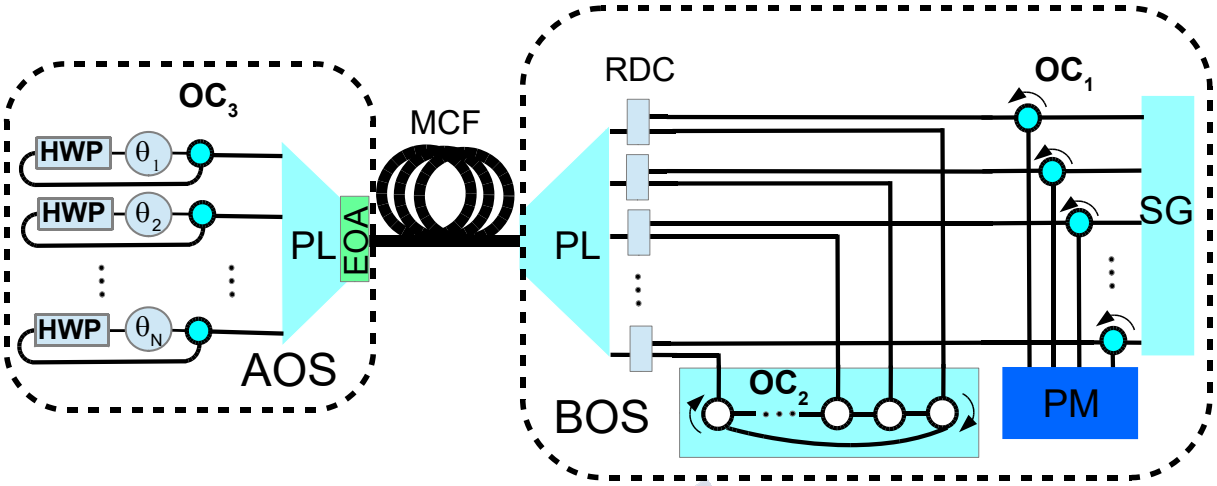


Figure P4.2: Sketch of the optical system. AOS, Alice optical system; BOS, Bob optical system; SG, state generator; OC, optical circulators; PM, projective measurement device; RDC, reconfigurable directional couplers; PL, photon lantern; MCF, multicore fiber; EOA, electro-optical attenuator; HWP, half wave plate, θ_i, electro-optical phase-shifters.

respectively phase shifts between components of the (local) fiber principal axis ($P_s(\beta)$) and the corresponding rotations ($R(\alpha)$) respect to Alice's laboratory reference system. Therefore the polarization is transformed according to the following matrix

$$T_{MCF_{\leftarrow}} = R(\alpha)^{-1} P_s(\beta) R(\alpha) = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \cdot e^{i\sigma_1} \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \quad \text{(P4.4)}$$

where σ_1 is the global phase acquired in the first core of the optical fiber. If we consider that the laboratory reference system used in AOS is determined by the principal axis of the HWP plate, then the only difference between going from Bob to Alice and from Alice to Bob is that the principal axis are inverted, that is, $\alpha \to -\alpha$. Thus, by using a HWP rotated $\pi/4$ within AOS, that is, $H(\pi/4)$, the polarization change in a round-trip is given by the following transformation

$$T_{MCF_{\leftarrow}} \cdot T_{MCF_{\rightarrow}} = R(-\alpha)^{-1} P_s(\beta) R(-\alpha) \cdot H(\pi/4) \cdot R(\alpha)^{-1} P_s(\beta) R(\alpha) = e^{i2\sigma_1} X, \quad \text{(P4.5)}$$

where X is the first Pauli matrix. Therefore, the unpredictable relative phase shift is compensated and we recover, up to a global phase $e^{i\sigma_1}$, the original polarization state, although the polarization modes are permuted (X matrix). Note that in our case no Faraday mirror is used.

When the state returns to BOS, the RDCs are in the off position as mentioned above, and thus light propagates to the set of circulators OC_2 that implement a circulation transformation C_{ij} to autocompensate the phase, i. e., it implements the following circulation optical transformation

$$C_{ij} = \delta_{i+1,j} + \delta_{i+1-N,j} = \begin{pmatrix} 0 & 1 & 0 & 0 & ... & 0 \\ 0 & 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & ... & 1 \\ 1 & 0 & 0 & 0 & ... & 0 \end{pmatrix}, \tag{P4.6}$$

where $i = 1, \dots N; j = 1, \dots, N$ and $\delta_{i,j}$ is the Kronecker delta. Consequently, light starts to circulate between the sets of circulators OC_2 and OC_3 with each mode travelling by different cores in each trip. After N circulations the RDCs take the on-position and light goes to the projective measurement device (PM) through the set of circulators OC_1. Therefore, after N trips the quantum state is given by

$$|L_e\rangle = |2^{-\frac{n}{2}} e^{i\sigma}\alpha\rangle\, |2^{-\frac{n}{2}} e^{i\sigma}\alpha\rangle \,....\, |2^{-\frac{n}{2}} e^{i\sigma}\alpha\rangle |2^{-\frac{n}{2}} e^{i\sigma}\alpha\rangle, \tag{P4.7}$$

where $\sigma = \sum_{i=0}^{N} 2\sigma_i$, with σ_i the phase acquired in each core. Likewise, it is easy to check that the time delays are also compensated, that is, all coherent states are delayed a time $\tau = \sum_{i=0}^{N} \tau_i$, with τ_i the time delay in each core.

P4.2.3 Maximum distance and light circulation analysis

The separation distance between Alice and Bob (D) is a fundamental requirement in QKD. In our system light travels $2N$ times this distance. As a consequence, our system can be affected by phase noise due to environmental changes while light travels [Minář et al., 2008]. This limits the maximum distance between Alice and Bob with respect to a one-way system. However, the use of MCFs allows to minimise this drawback. Environmental variations should affect the different cores in an uniform way, and so, phase noise within cores in a MCF should be far more stable than between single-core fibers. Indeed in [Ramirez et al., 2015] phase noise between two cores in a MCF is 70 times less than between separate fibers, with lower frequencies being the main contributor to the noise. Smaller and slower phase fluctuations allow for higher distances of propagation and could also be more easily corrected. If t_{pf} is the time while phase noise is assumable and c_f is the speed of light in the fiber, then the maximum distance is given by

$$D = \frac{c_f\, t_{pf}}{2\, N}. \tag{P4.8}$$

This means that D will decrease at high dimensions still, becoming not assumable at some point. If we consider $t_{pf} \approx 1ms$ for a two fiber path [Minář et al., 2008] and

apply a linear assumption, taking into account [Ramirez et al., 2015], $t_{pf} \approx 70ms$; with $c_f \approx 200000\, km/s$ then

$$D \approx 7000/N\, km. \tag{P4.9}$$

Regarding the light circulation inside our system, different approaches can be taken into account. One simple possibility would be to sent a group of light pulses followed by blank spaces to allow the group an enough time to make the round trips needed. The final key-rate is determined by the pulse rate and the electro-optical phase shifters operation time, however blank spaces decrease the transmitted information. If T is the time between pulses it is straightforward to check that, in a N dimension system, we have an effective transmission rate of

$$f_{ef} = \frac{1}{N\,T}. \tag{P4.10}$$

Another possible approach is to send interleaved pulses. In this case, the final key-rate is limited by the switching speed of the RDCs τ_{RDC}, as it is the device which separates the states to be measured from those that continue in the loop. So, pulses in different round trips must not overlap between them. Let's call $n_p = \lfloor L/c_f T \rfloor$ the total number of pulses in a round-trip $L = 2D$, where c_f is the speed of light in the fiber and D is the distance between Alice and Bob, and be $t_L = L/c_f$ the time it takes a pulse to complete a round trip; then, the time differences between pulse 1 and pulses n_p and $n_p + 1$ when they reach RDC are

$$\Delta t_{1,\,n_p} = \|t_L - (n_p - 1)T\|, \tag{P4.11a}$$

$$\Delta t_{1,\,n_p+1} = \|t_L - n_p\, T\|\,. \tag{P4.11b}$$

So, the time difference between light pulses in consecutive round-trips is $\Delta t = \min\left(\Delta t_{1,n_p}, \Delta t_{1,n_p+1}\right)$ and it is needed that $\tau_{RDC} \leq \Delta t$, so T must be controlled. An optimal case would be

$$\tau_{RDC} \leq \Delta t = \frac{T}{N}. \tag{P4.12}$$

In consequence, the transmission rate would be limited by

$$f = \frac{1}{T} \leq \frac{1}{N\,\tau_{RDC}}. \tag{P4.13}$$

We can see in (P4.10) and (P4.13) that we have the same rate, but different limiter times. However, another hybrid method is possible. We can send interleaved groups of pulses in order to use the full performance of our devices. If Δt_g is the separation between different groups in different round-trips, limited by τ_{RDC}, and n_p/N is the number of groups in a same round-trip, then the transmission rate will be given by

$$f = \frac{1}{N\,\Delta t_g}\frac{n_p}{N} \leq \frac{L}{c_f}\frac{1}{N^2\,T\,\tau_{RDC}}, \tag{P4.14}$$

which allows higher rates than the previous methods. It must be noted that, although the transmission rate decreases with the dimension, bit information per state increases as well.

It is important to analyze what happens if decoy states are used. In this case, the speed would also depend on the operational time of the EOA (τ_{EOA}), as it is responsible of applying different levels of attenuation to the different pulses to implement the decoy states protocol. This way, in the first two methods, the rate will be

$$f = \frac{1}{N\, t_{lim}}, \tag{P4.15}$$

where t_{lim} is the limiter operational time between τ_{EOA} and $T//\tau_{RDC}$. In the last method (P4.14), if we want to attenuate between pulses, τ_{EOA} can limit T; however, we can also create decoy groups without affecting the protocol, and so, τ_{EOA} would limit τ_{RDC}. Regarding the times, electro-optical switches with time responses in the order of ns [Van Campenhout et al., 2009] and even reaching few ps [Zheng et al., 2008] have been implemented. Meanwhile, high-repetition-rate pulse lasers have also been developed [Mao et al., 2013].

P4.3 Generation of signal quantum states (Alice System)

As commented, just before the last half-trip from Alice to Bob systems, Alice introduces the θ_i phases in order to obtain the signal quantum state. We must stress that Alice previously needs to attenuate the multimode coherent state to obtain the mentioned signal quantum state. Therefore, we obtain the following signal 1-qudit state

$$|L_e\rangle \approx 2^{-\frac{n}{2}} e^{i\sigma}\{e^{-i\sigma_1}e^{i\theta_1}|1_1\rangle + e^{-i\sigma_2}e^{i\theta_2}|1_2\rangle + ... + e^{-i\sigma_N}e^{i\theta_N}|1_N\rangle\} + ..., \tag{P4.16}$$

where we have disregarded the contribution of the vacuum $|0\rangle$. Obviously, the phases $e^{-i\sigma_i}$ are cancelled in the last half-trip. Moreover, the above N-dimensional qudit state is in turn superposed with number states of two or more photons ($|n\rangle, n = 2, 3, ...$), however, they will not be considered because it is assumed that possible attacks are counteracted by some decoy states method [Hwang, 2003]. For getting an effective attenuation we consider an electro-optical attenuator (EOA) based, for instance, on polarization. It can be placed just before the second PL, as shown in Fig. P4.2 (left). An example of such a EOA is presented in figure P4.3. It is composed by two polarization beam splitters (PBS), a HWP rotated $\pi/4$ and two electro-optical rotators (EOR). We start from an arbitrary polarization state which is divided by a first PBS. Next, on the horizontal direction a HWP rotates $\pi/2$ the linear polarization. Finally, one EOR rotates the state an angle α with respect to the incidence plane, and the other one an angle $\pi/2-\alpha$, therefore the output state is attenuated an amount $\cos\alpha$ in one arm and an amount $\sin\alpha$ in the other arm.

As mentioned above, the purpose of the EOA is not only to attenuate in order to produce the state (P4.16), but also to increase the security of the system, that is, the

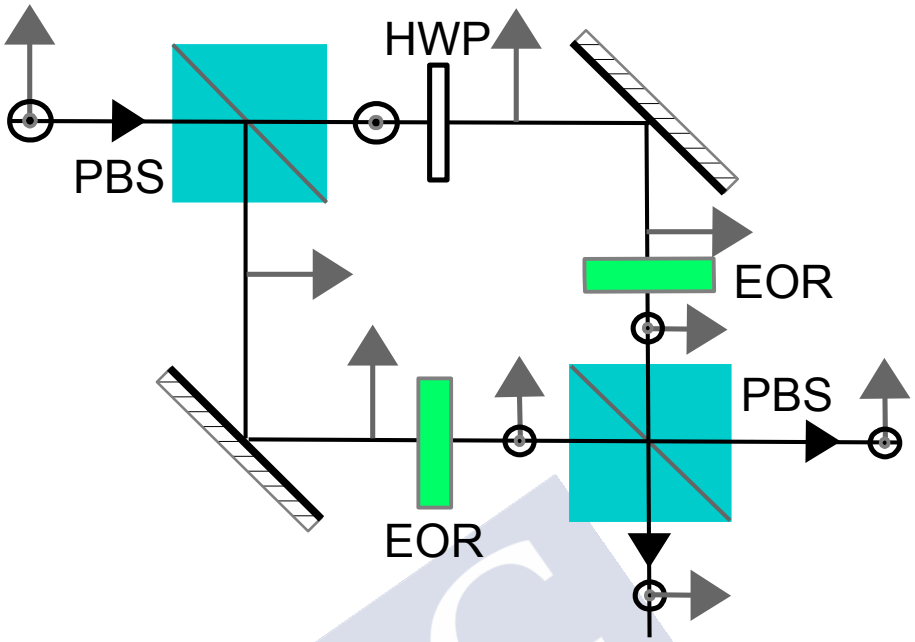


Figure P4.3: Sketch of an Electro-Optical Attenuator (EOA).

attenuation of the EOA can be controlled, allowing us to produce different attenuated pulses (signal and decoy states) in order to implement a decoy states protocol to protect against different attacks of an eavesdropper Eve, like the Photon-number-splitting attack [Hwang, 2003]. Likewise, this EOA can be used to shut down communication between AOS and the MCF, opening it only when a light pulse is expected to arrive to or to leave AOS. Optical buffers can be used by Alice in order to control the arrival and departure of pulses. This makes more difficult for an eavesdropper Eve to implement trojan horse attacks [Gisin et al., 2006].

It should also be taken into account that pulses are attenuated along the optical fiber during the different trips. The OC_2-OC_3 circulation system assures that the final attenuations of the different modes are the same, as long as we consider that the environment conditions (temperature, pressure, etc.) of the fiber do not change significantly during the transmission of each qudit. We can take advantage of this natural attenuation in order to reduce the attenuation required by our EOA. It has been shown that losses around 0.15 dB/km at 1550 nm of SMF can be theoretically achieved for pure-silica-core few-mode fibers (FMF) [Liu et al., 2018], so an optical fiber of 50 km in a system of 4 dimensions means around 60 dB losses.

Finally, we must define the MUBs which will be used in the QKD system. The projective measurement in each base will be made in the next section, that is, in the

BOS. Let us consider, for example, a MUB for dimension 2, that is,

$$\mathcal{B}_1^{(2)} = \left\{ \frac{1}{\sqrt{2}}(1,1);\ \frac{1}{2}(1,-1) \right\}, \tag{P4.17a}$$

$$\mathcal{B}_2^{(2)} = \left\{ \frac{1}{\sqrt{2}}(1,i);\ \frac{1}{2}(1,-i) \right\}. \tag{P4.17b}$$

It has been shown that starting from these basis it is possible to obtain MUBs of higher dimensions. In particular, MUBs for dimension $N = 2^n$ can be obtained by using tensorial products and rotation matrix [Tselniker et al., 2009]. For the case $N = 4$ we have the following MUB set

$$\mathcal{B}_1^{(4)} = \left\{ \frac{1}{2}(1,1,1,1);\ \frac{1}{2}(1,-1,1,-1);\ \frac{1}{2}(1,1,-1,-1);\ \frac{1}{2}(1,-1,-1,1) \right\}, \tag{P4.18a}$$

$$\mathcal{B}_2^{(4)} = \left\{ \frac{1}{2}(1,i,i,-1);\ \frac{1}{2}(1,-i,i,1),\ \frac{1}{2}(1,i,-i,1);\ \frac{1}{2}(1,-i,-i,-1) \right\}, \tag{P4.18b}$$

$$\mathcal{B}_3^{(4)} = \left\{ \frac{1}{2}(1,i,1,-i);\ \frac{1}{2}(1,-i,1,i);\ \frac{1}{2}(1,i,-1,i);\ \frac{1}{2}(1,-i,-1,-i) \right\}, \tag{P4.18c}$$

$$\mathcal{B}_4^{(4)} = \left\{ \frac{1}{2}(1,1,i,-i);\ \frac{1}{2}(1,-1,i,i);\ \frac{1}{2}(1,1,-i,i);\ \frac{1}{2}(1,-1,-i,-i) \right\}. \tag{P4.18d}$$

Therefore we have sixteen 1-ququart states and four bases ($N = 4$). Note that for these MUBs the detection probability of each 1-ququart is $\mathcal{P} = 1/4$ and only the relative phases 0, π, $\pm\pi/2$ are used to generate the sixteen single photon states. Such phases are obtained by implementing phase shifts θ_i, with $i = 1, ..., 4$, in each of the four spatial modes, as shown in Fig. P4.2.

As to higher dimension, for example $N = 8$ ($n = 3$), we present a MUB pair, that is, two basis and sixteen 1-qudits of dimension $N = 8$. In a matrix form we have the MUB pair

$$\mathcal{B}_1^{(8)} = \mathcal{B}_1^{(2)} \otimes \mathcal{B}_1^{(2)} \otimes \mathcal{B}_1^{(2)} = 2^{-3/2} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}, \tag{P4.19a}$$

$$\mathcal{B}_2^{(8)} = \mathcal{B}_2^{(2)} \otimes \mathcal{B}_2^{(2)} \otimes \mathcal{B}_2^{(2)} =$$

$$2^{-3/2} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ i & -i & i & -i & i & -i & i & -i \\ i & i & -i & -i & i & i & -i & -i \\ -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ i & i & i & i & -i & -i & -i & -i \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ -i & i & i & -i & i & -i & -i & i \end{pmatrix}, \quad \text{(P4.19b)}$$

where each column is a vector of the basis $\mathcal{B}_1^{(8)}$ and $\mathcal{B}_2^{(8)}$. Again, only the relative phases 0, π, $\pm\pi/2$ are used to generate the sixteen single photon states and the detection probability of each qudit is $\mathcal{P} = 1/8$. Such phases are again obtained by the phase shifts θ_i with $i = 1, ..., 8$.

Finally, basis $\mathcal{B}_1^{(2^n)}$ and $\mathcal{B}_2^{(2^n)}$ of dimension $N = 2^n$ can always be factorized as follows [Tselniker et al., 2009]

$$\mathcal{B}_1^{(2^n)} = \mathcal{B}_1^{(2)} \otimes \mathcal{B}_1^{(2)} \otimes ... \otimes \mathcal{B}_1^{(2)}, \quad \text{(P4.20a)}$$

$$\mathcal{B}_2^{(2^n)} = \mathcal{B}_2^{(2)} \otimes \mathcal{B}_2^{(2)} \otimes ... \otimes \mathcal{B}_2^{(2)}, \quad \text{(P4.20b)}$$

where $\mathcal{B}_i^{(2)}$ is the corresponding basis in two dimensions (P4.17). It is important to stress that encryption protocols do not require the use of all the MUBs to be secure, and, in fact, the use of several basis will only led to decreasing bit transmission rate.

P4.4 Random projective measurement integrated device (Bob System)

Once Alice has attenuated the pulse and encrypted the information with the θ_i phases, the state given by Eq. (P4.16) arrives to BOS. As N circulations have been completed, the RDCs take the on-position, and then the state goes through OC_1 and reaches the projective measurement device (PM). Next we present integrated PM devices for $N = 4$, $N = 8$ and $N = 2^n$ together with an integrated splitter device in order to make random projective measurements.

P4.4.1 Case $N = 4$

In Fig. P4.4, we show an example of an integrated optical PM for the case $N = 4$. The device consists of the following sequence of couplers: two $\tilde{\kappa} = \pi/4$ couplers connected by one $\tilde{\kappa} = \pi/2$ coupler, followed by a second pair of $\tilde{\kappa} = \pi/4$ couplers. Before the second pair

of couplers, $-\pi/2$-shifters are used in even guides. The general quantum transformation of the device is:

$$\hat{\mathcal{P}}_4 \left|\psi_{bs}\right\rangle = \hat{M}^{(4)}_{\pi/4} \cdot \hat{\mathcal{S}}^{(4)}_{-\pi/2} \cdot \hat{D}^{(4)}_{\pi/2} \cdot \hat{M}^{(4)}_{\pi/4} \cdot \hat{\mathcal{S}}^{(4)}(\phi_i) \ \left|\psi_{bs}\right\rangle , \tag{P4.21}$$

where $\hat{\mathcal{S}}^{(4)}$ represents phase shifts ϕ_i, with $i = 1, 2, 3, 4$, introduced in the different modes if required (first column of integrated devices shown in Fig. P4.4), $\hat{M}^{(4)}_{\pi/4}$ is the operator of $\tilde{\kappa} = \pi/4$ couplers (second column), $\hat{D}^{(4)}_{\pi/2}$ is the $\tilde{\kappa} = \pi/2$ coupler (third column), $\hat{\mathcal{S}}^{(4)}_{-\pi/2}$ is the transformation of the $-\pi/2$-shifters (fourth column) and finally another operator $\hat{M}^{(4)}_{\pi/4}$ (fifth column). The superindex (4) indicates the dimension of the Hilbert space. State $\left|\psi_{bs}\right\rangle$ corresponds to the state s of the base $\mathcal{B}^{(4)}_b$, and in this space the previous operators corresponds to the following matrices

$$M^{(4)}_{\pi/4} = \mathbb{I}^{(2)} \otimes M_{\pi/4}, \tag{P4.22}$$

$$\mathcal{S}_{-\pi/2} = \mathbb{I}^{(2)} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}, \tag{P4.23}$$

$$D_{\pi/2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{P4.24}$$

where $\mathbb{I}^{(2)}$ is the identity matrix in two dimensions. In short, operator $\hat{\mathcal{P}}_4$ is a four-dimensional PM device (4D-PM).

We can perform the explicit calculations for a particular case in order to make clear how it works. Let us consider the first state corresponding to base $\mathcal{B}^{(4)}_2$ in Eq. (P4.18):

$$\left|\psi_{2_1}\right\rangle = 2^{-1} \left(\left|1_1\right\rangle + i \left|1_2\right\rangle + i \left|1_3\right\rangle - \left|1_4\right\rangle\right). \tag{P4.25}$$

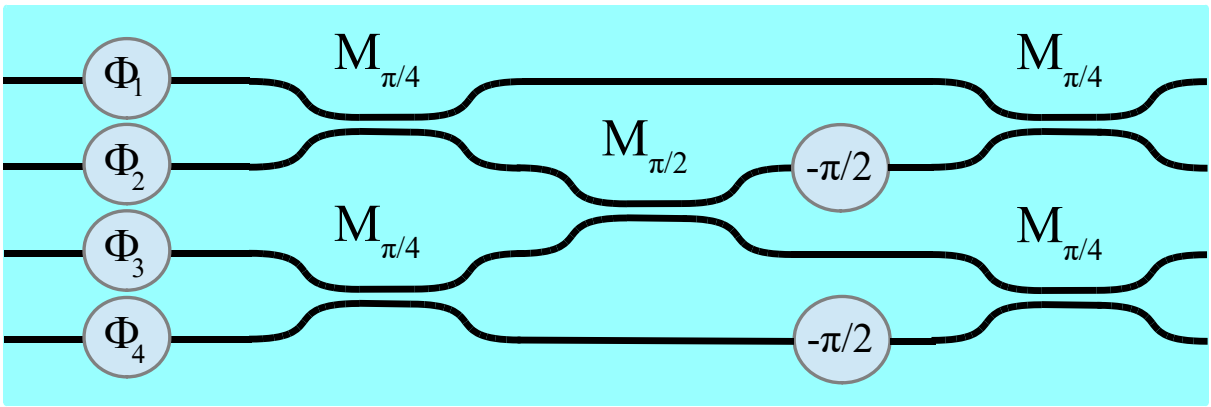


Figure P4.4: Projective measurement device for dimension $N = 4$.

The first two couplers $\tilde{\kappa} = \pi/4$ ($\hat{M}^{(4)}_{\pi/4}$) and the coupler $\tilde{\kappa} = \pi/2$ ($\hat{D}^{(4)}_{\pi/2}$) produce the following output state

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i & 0 & 0 \\ i & 1 & 0 & 0 \\ 0 & 0 & 1 & i \\ 0 & 0 & i & 1 \end{pmatrix} \begin{pmatrix} 1/2 \\ i/2 \\ i/2 \\ -1/2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ -1 \\ -1 \end{pmatrix}. \tag{P4.26}$$

Note that the first two couplers $\tilde{\kappa} = \pi/4$ project the 4-dimensional state into a 2-dimensional one (two active modes 2 and 4), while the coupler $\tilde{\kappa} = \pi/2$ groups the two active modes into nearest neighbour guides (3 and 4). Next, the $-\pi/2$-shifters ($\hat{\mathcal{S}}_{-\pi/2}$) are used to introduce a phase shift between nearest neighbour modes 3 and 4 in order to allow the next couplers $\tilde{\kappa} = \pi/4$ ($\hat{M}^{(4)}_{\pi/4}$) to project the 2 dimensional state into one, that is,

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i & 0 & 0 \\ i & 1 & 0 & 0 \\ 0 & 0 & 1 & i \\ 0 & 0 & i & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ -1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0 \end{pmatrix}. \tag{P4.27}$$

Therefore, state ψ_{21} is projected into the third output of the device. Doing the same with the rest of states of basis $\mathcal{B}^{(4)}_2$, we can see that the different states of basis $\mathcal{B}^{(4)}_2$ are projected into the different output states $|1_{oj}\rangle, j = 1, ..., 4$ emerging from the integrated device, that is,

$$\begin{aligned} \hat{\mathcal{P}}_4 |\psi_{21}\rangle &= -|1_{o3}\rangle, \\ \hat{\mathcal{P}}_4 |\psi_{22}\rangle &= i|1_{o2}\rangle, \\ \hat{\mathcal{P}}_4 |\psi_{23}\rangle &= -i|1_{o4}\rangle, \\ \hat{\mathcal{P}}_4 |\psi_{24}\rangle &= |1_{o1}\rangle. \end{aligned} \tag{P4.28}$$

In order to measure the rest of the bases, phase shifters Φ_i are required at the beginning of the device to be able to transform bases $\mathcal{B}^{(4)}_1$, $\mathcal{B}^{(4)}_3$ and $\mathcal{B}^{(4)}_4$ into base $\mathcal{B}^{(4)}_2$. The phases phi_i, with $i = 1, 2, 3, 4$, needed to implement these transformations are given by the following matrices

$$\mathcal{S}_{1\to 2} = diag\left(\ 1,\ i,\ i,\ -1\ \right), \tag{P4.29a}$$

$$\mathcal{S}_{3\to 2} = diag\left(\ 1,\ 1,\ i,\ -i\ \right), \tag{P4.29b}$$

$$\mathcal{S}_{4\to 2} = diag\left(\ 1,\ i,\ 1,\ -i\ \right). \tag{P4.29c}$$

Obviously, being $\hat{\mathcal{S}}_{2\to 2} = \mathbb{I}^{(4)}$, where $\mathbb{I}^{(4)}$ is the identity matrix in four dimensions. According to this we can redefine the operator $\hat{\mathcal{P}}_4$ in Eq. (P4.21) as follows

$$\hat{\mathcal{P}}_4 = \hat{P}^{(4)}_2 \cdot \hat{P}^{(4)}_4 \cdot \hat{\mathcal{S}}_{b\to 2}, \tag{P4.30}$$

where we separate the action of the device into three main parts. Thus, $\hat{\mathcal{S}}_{b\to 2}$ represents the phase shifters which select the measure basis, $\hat{P}_4^{(4)} = \hat{\mathcal{S}}_{-\pi/2} \cdot \hat{D}_{\pi/2}^{(4)} \cdot \hat{M}_{\pi/4}^{(4)}$ corresponds to the reducing circuit of couplers and phase shifters responsible of reducing a 4-dimensional state into a 2-dimensional state, and $\hat{P}_2^{(4)} = \hat{M}_{\pi/4}^{(4)}$ are the two last couplers responsible of projecting the 2-dimensional state into a 1-dimensional one. We must stress that when $\hat{\mathcal{P}}_4$, given by Eq. (P4.30), is used, the outputs states given by (P4.28) are independent of the basis used.

P4.4.2 Case $N = 8$

In Fig. P4.5 an example for $N = 8$ is shown. It works the same way that the previous device. First, four $\tilde{\kappa} = \pi/4$ couplers followed by a decreasing number of $\tilde{\kappa} = \pi/2$ couplers. Next, $-\pi/2$-shifters are used in even guides and they are followed by two 4D devices.

Mathematically, the transformation can be written as follows

$$\hat{\mathcal{P}}_8 \left|\psi_{bs}^{(8)}\right\rangle = \hat{\mathcal{P}}_4^{(8)} \cdot \hat{\mathcal{S}}_{-\pi/2} \cdot \hat{D}_{\pi/2}^{(8)} \cdot \hat{M}_{\pi/4}^{(8)} \cdot \hat{\mathcal{S}}_{b\to 2}(\phi_i) \left|\psi_{bs}^{(8)}\right\rangle , \tag{P4.31}$$

where $\mathcal{P}_4^{(8)} = \mathbb{I}^{(2)} \otimes \mathcal{P}_4$ is the transformation of the two 4D reducers (P4.30) and $\hat{D}_{\pi/2}^{(4)}$ represents the transformation of all the six couplers $\tilde{\kappa} = \pi/2$ which is the product of three matrices which can be inferred from Fig. P4.5. The entire transformation is given by the

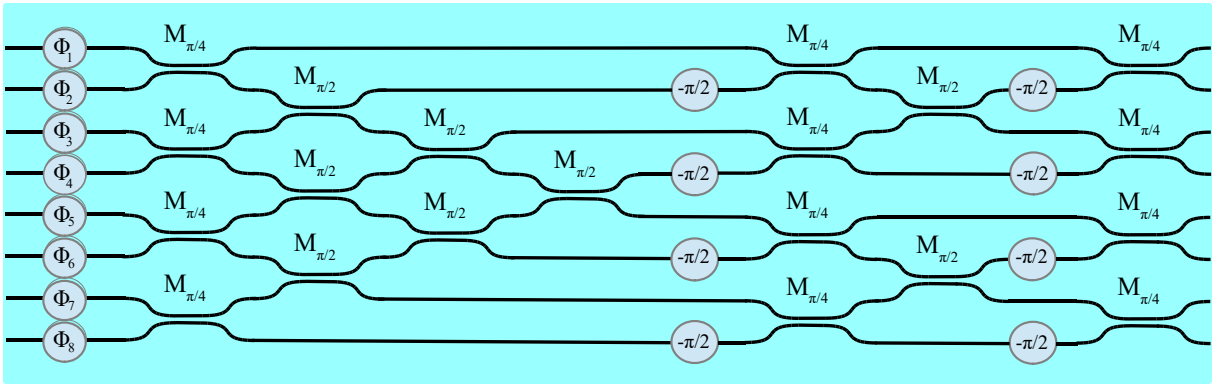


Figure P4.5: Projective measurement device for dimension $N = 8$.

matrix:

$$\mathcal{P}_8 = 2^{(-3/2)} \begin{pmatrix} 1 & i & i & -1 & -i & 1 & 1 & i \\ i & -1 & -1 & -i & -1 & -i & -i & 1 \\ -1 & -i & i & -1 & -i & 1 & -1 & -i \\ -i & 1 & -1 & -i & -1 & -i & i & -1 \\ 1 & -i & -i & -1 & -i & -1 & -1 & i \\ i & 1 & 1 & -i & -1 & i & i & 1 \\ -1 & i & -i & -1 & -i & -1 & 1 & -i \\ -i & -1 & 1 & -i & -1 & i & -i & -1 \end{pmatrix}. \tag{P4.32}$$

This allows us to make projective measures of base $\mathcal{B}_2^{(8)}$ given by Eq. (P4.19b). To measure in different bases, phase shifters Φ_i are required at the beginning of the device. If we want to measure in base $\mathcal{B}_1^{(8)}$ given by Eq. (P4.19a) then we have to introduce the following phases before the device

$$\begin{aligned} \mathcal{S}_{1\to 2}^{(8)} &= \mathrm{diag}\left\{(1,\mathrm{i}) \otimes \mathrm{diag}\,(1,\mathrm{i}) \otimes \mathrm{diag}\,(1,\mathrm{i})\right\} \\ &= \mathrm{diag}\left(\ 1,\ i,\ i,\ -1,\ i,\ -1,\ -1,\ -i\ \right). \end{aligned} \tag{P4.33}$$

As shown in the case $N = 4$ the outputs states$|1_{oj}\rangle, j = 1, ..., 8$ will be independent of the used basis, that is,

$$\begin{aligned} \hat{\mathcal{P}}_8 |\psi_{b1}\rangle &= |1_{o5}\rangle, & \hat{\mathcal{P}}_8 |\psi_{b2}\rangle &= -i\,|1_{o4}\rangle, \\ \hat{\mathcal{P}}_8 |\psi_{b3}\rangle &= -i\,|1_{o8}\rangle, & \hat{\mathcal{P}}_8 |\psi_{b4}\rangle &= |1_{o1}\rangle, \\ \hat{\mathcal{P}}_8 |\psi_{b5}\rangle &= i\,|1_{o6}\rangle, & \hat{\mathcal{P}}_8 |\psi_{b6}\rangle &= -|1_{o3}\rangle, \\ \hat{\mathcal{P}}_8 |\psi_{b7}\rangle &= -|1_{o7}\rangle, & \hat{\mathcal{P}}_8 |\psi_{b8}\rangle &= i\,|1_{o2}\rangle. \end{aligned} \tag{P4.34}$$

P4.4.3 Case $N = 2^n$

This device can be easily generalized to dimension $N = 2^n$ (Fig. P4.6). Such device consists of 2^{n-1} $\tilde{\kappa} = \pi/4$ couplers followed by a decreasing number of $\tilde{\kappa} = \pi/2$ couplers and $-\pi/2$-shifters in even waveguides. Then, two devices of dimension $N = 2^{n-1}$ follow, which, in turn, are respectively followed by two devices of dimension $N = 2^{n-2}$ and so on. As above, phase shifters at the beginning are needed in order to change the basis.

Consequently, the general transformation implemented by a 2^n-PM device will be given by the following operator

$$\hat{\mathcal{P}}_N |\psi_{bs}^{(N)}\rangle = \hat{P}_2^{(N)} \cdot \hat{P}_4^{(N)} \cdot \hat{P}_8^{(N)} \ldots \hat{P}_{2^{n-2}}^{(N)} \cdot \hat{P}_{2^{n-1}}^{(N)} \cdot \hat{P}_{2^n}^{(N)} \cdot \hat{\mathcal{S}}_{b\to 2} |\psi_{bs}^{(N)}\rangle, \tag{P4.35}$$

where $\hat{P}_{(m)}^N$ represents the part of the device that projects a m-dimension state into a

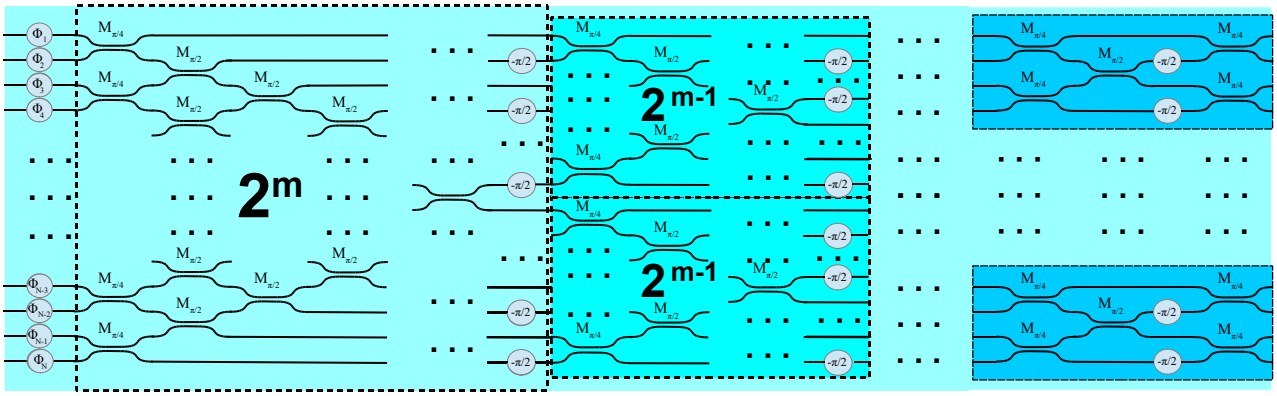


Figure P4.6: Projective measurement device for dimension $N = 2^n$.

$\frac{m}{2}$-dimension state expanded into N dimensions, as shown in Fig. P4.6, given by

$$\hat{P}_m^N = \mathbb{I}^{(N/m)} \otimes \left(\hat{\mathcal{S}}_{-\pi/2}^{(m)} \cdot \hat{D}^{(m)} \cdot \hat{M}_{\kappa_{\pi/4}}^{(m)} \right) = \hat{\mathcal{S}}_{-\pi/2}^{(N)} \cdot \left(\mathbb{I}^{(N/m)} \otimes \hat{D}^{(m)} \right) \cdot \hat{M}_{\pi/4}^{(N)}, \quad \text{(P4.36)}$$

where operators $\hat{\mathcal{S}}_{-\pi/2}^{(m)}$, $\hat{D}_m^{(m)}$ and $\hat{M}_{\pi/4}^{(m)}$ represent, respectively, the transformations corresponding to the $-\pi/2$-shifters, the $\tilde{\kappa} = \pi/4$ couplers and of decreasing series of $\tilde{\kappa} = \pi/2$ couplers in m dimensions. Note that $\mathbb{I}^{(N/m)} \otimes \hat{D}_m^{(m)} \neq \hat{D}^{(N)}$ as the decreasing structure of $\kappa_{\pi/2}$ couplers is different for the different dimensions, as we can see for the cases $N = 4, 8$ in Figs. P4.4-P4.5, so $\mathbb{I}^{(N/m)} \otimes \hat{D}_m^{(m)}$ represents the structure $\hat{D}_m^{(m)}$ repeated N/m times. Operators $\hat{\mathcal{S}}_{-\pi/2}^{(m)}$ and $\hat{M}_{\pi/4}^{(m)}$ are represented by the following matrices:

$$\hat{\mathcal{S}}_{-\pi/2}^{(N)} = \mathbb{I}^{(N/2)} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}, \quad \text{(P4.37)}$$

$$\hat{M}_{\kappa_{\pi/4}}^{(N)} = \mathbb{I}^{(N/2)} \otimes M_{\kappa_{\pi/4}}. \quad \text{(P4.38)}$$

This device measures always in base $\mathcal{B}_2^{(2^n)}$ given by Eq. (P4.20b). In order to measure in other basis like $\mathcal{B}_b^{(2^n)}$, we have to apply the phases given by matrix $\mathcal{S}^{2^n} = \mathcal{B}_2^{(2^n)} \cdot \left(\mathcal{B}_b^{(2^n)} \right)^{-1}$. In the case that we use the two basis $\mathcal{B}_1^{(2^n)}$ and $\mathcal{B}_2^{(2^n)}$, trivially obtained by Eq. (P4.20a) and Eq. (P4.20b), the phase-shifts between both basis are given by

$$\mathcal{S}_{1\to 2}^{2^n} = \mathrm{diag}\left\{ (1, \mathrm{i}) \otimes_1 (1, \mathrm{i}) \otimes_2 (1, \mathrm{i}) \otimes_3 \ldots \otimes_{\mathrm{n}} (1, \mathrm{i}) \right\}. \quad \text{(P4.39)}$$

P4.4.4 Splitter Device

As said in the previous sections, in order to measure in the different basis we have to apply phase shifts ϕ_i ($\hat{\mathcal{S}}_{i\to 2}$), which can be implemented by using integrated active phase

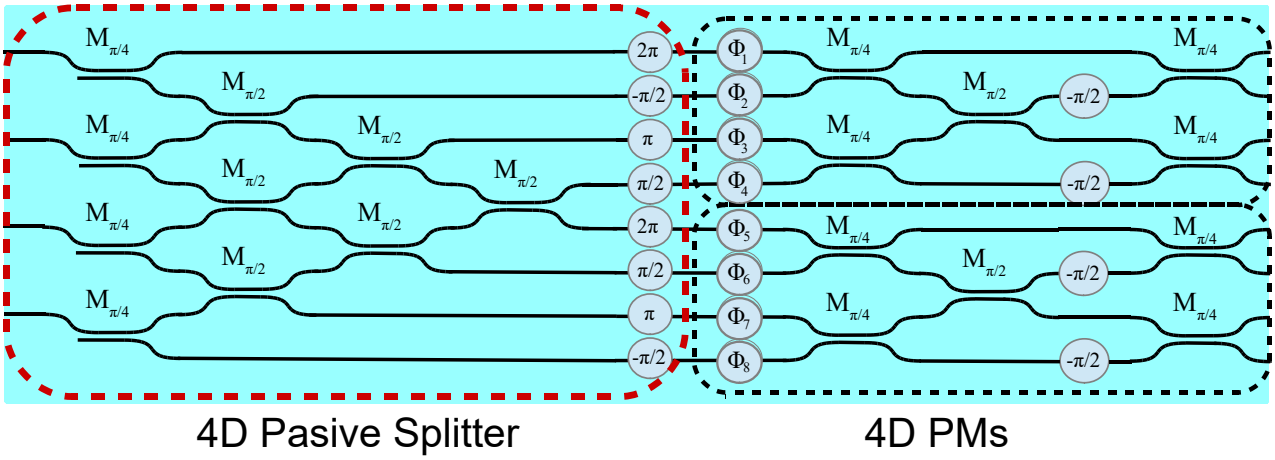


Figure P4.7: Integrated splitter for dimension $N = 4$ (4D-IS) together with 4D-PMs.

shifters. However, passive measurement is also possible. We could use SMFs and beam splitters to randomly send the incoming state (P4.16) to different PM devices with fixed phase shifts.

A passive integrated system can also be designed. The triangular structure of couplers previously explained and shown in Fig. P4.6, also works as an integrated beam splitter (IS). For example, a circuit of dimension $N = 8$ can be used as a beam splitter for states of dimension $N = 4$, that is, a 4D-IS. The idea is that the $\tilde{\kappa} = -\pi/4$ couplers duplicate the arriving state while the structure of $\tilde{\kappa} = -\pi/2$ couplers separate both copies and send them to two PM devices. Phase shifters are needed to compensate the introduced phases. We show the idea in Fig. P4.7.

In general, a structure of dimension $2N = 2^{n+1}$ works as a beam splitter for a quantum state of dimension $N = 2^n$. Mathematically, the splitter of dimension N will be given by

$$\hat{S}_N^{(2N)} = \hat{\mathcal{S}}_S^{(2N)} \cdot \hat{D}^{(2N)} \cdot \hat{M}_{\kappa_{\pi/4}}^{(2N)}, \tag{P4.40}$$

where $\hat{\mathcal{S}}_S^{(2N)}$ represents the phase compensation, which is

$$\hat{\mathcal{S}}_S^{(2N)} = diag\left((-i)^0, (-i)^1, ..., (-i)^{N-1}, (-i)^N, (-i)^{N-1}, ..., (-i)^1\right). \tag{P4.41}$$

If we have the state $\psi_{bs}^{(N)}$, this is, the vector s of the base b for dimension N, then the matrix transformation in the splitter can be calculated as

$$S_N^{(2N)} \cdot \left(\psi_{bs}^{(N)} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \psi_{bs}^{(N)}. \tag{P4.42}$$

We see that, as expected, our state has been duplicated. The most important consequence od this result is that we can perform projective measurements in random N-dimensional basis in the BOS system, which is a necessary condition in any high-dimensional QKD protocol. Note that in this way electro-optical devices can be reduced and therefore a robust detection is performed.

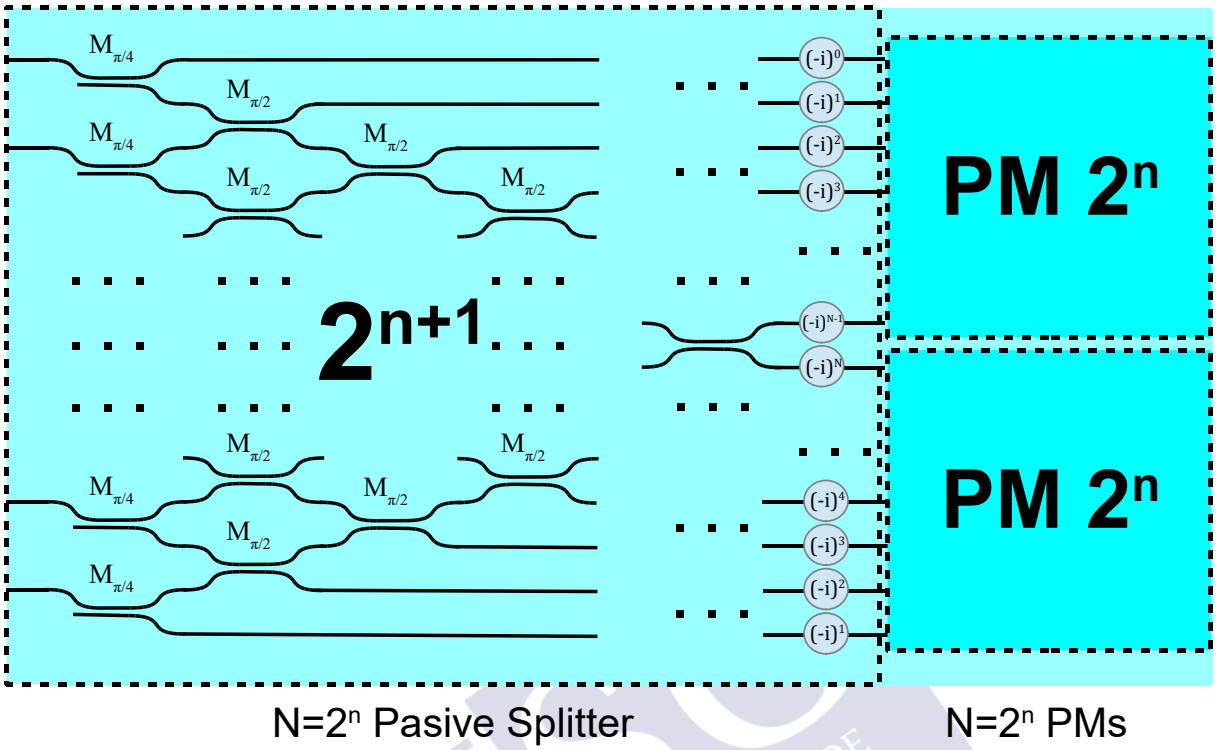


Figure P4.8: Passive splitter for dimension $N = 2^n$

P4.5 Security analysis

In this section we make a short analysis of security of our proposed cryptographic system. Security analyzes for one-way high-dimensional BB84 protocol have been made, thus, in reference [Cerf et al., 2002] security has been studied under attacks based on quantum cloning machines and different secret key rates R were obtained for different dimensions and number of basis used. The secret key rate R fulfils the following inequality

$$R \geq \max(I_{AB} - I_{AE}, I_{AB} - I_{BE}), \tag{P4.43}$$

where I_{AB}, I_{AE} and I_{EB} represent the mutual information shared between Alice and Bob, Alice and Eve, and Bob and Eve, respectively. The mutual information is defined as $I_{XY} = I(X;Y) = H(X) - H(X|Y)$, where H is the Shannon entropy. It has been proved that in Alice and Bob's case such a mutual information is given by

$$I_{AB} = \log_2 N + F \log_2 F + (1-F) \log_2 \left(\frac{1-F}{N-1} \right), \tag{P4.44}$$

being $F = 1 - Q$, with Q the error rate, and N the dimension. To obtain I_{AE}, two cases must be distinguished according to the number of basis n_b used. If only $n_b = 2$ basis are

used in the protocol, then I_{AE} is given by Eq. (P4.44) but replacing F by $F_E^{(2)}$, where

$$F_E^{(2)} = \frac{F}{d} + \frac{(d-1)(1-F)}{d} + \frac{2}{d}\sqrt{(d-1)F(1-F)}, \tag{P4.45}$$

On the other hand, if we want to use all the possible $N+1$ MUBs, then the mutual information I_{AE} would be given by

$$I_{AE}^{(N+1)} = \log_2 N + (F + F_E^{(N+1)} - 1)\log_2\left(\frac{F + F_E^{(N+1)} - 1}{F}\right) + (1 - F_E^{(N+1)})\log_2\left(\frac{1 - F_E^{(N+1)}}{(N-1)F}\right), \tag{P4.46}$$

where

$$F_E^{(N+1)} = 1 - \frac{N-1}{N}\cdot\left(\sqrt{\frac{(N+1)F-1}{N}} - \sqrt{\frac{1-F}{N(N-1)}}\right)^2. \tag{P4.47}$$

In Fig. P4.9, we represent the bit rate for cases with $N = 2, 4, 8$. We can observe the maximum quantum bit error rate (QBER) values from which no secret key rate is distilled in the different cases. For each dimension, we see that using more basis improves the maximum QBER which guarantees security as stated in [Cerf et al., 2002]. We show these QBERs in Table P4.1, and they provide us with a quantitative security limit to our cryptographic system.

Table P4.1: Upper bound on QBER that guarantees security against individual attacks for different dimension and number of basis.

N	Q_2 (%)	Q_{N+1} (%)
2	14.64	15.64
4	25	26.66
8	32.33	33.44

However, our protocol is not an one-way system. Instead, as explained in previous sections, in our system quantum light states make N round trips between Alice and Bob in order to autocompensate all fluctuations during transmission. This opens new attack possibilities for Eve to implement that are not possible in one-way protocols. An interesting new attack that Eve can perform is the phase-remapping (PR) attack [Fung et al., 2007, Xu et al., 2010]. This attack is an intercept-and-resend attack that exploits non ideal square response of Alice's modulators. More concretely, it takes advantage of the ascending and descending edges of the response. As commented in Section P4.3, Alice encrypts the information just before the last half-trip towards Bob. In the previous half-trip (to Alice), Eve can time-shift the light pulse (P4.7), sent by Bob for the last time, in

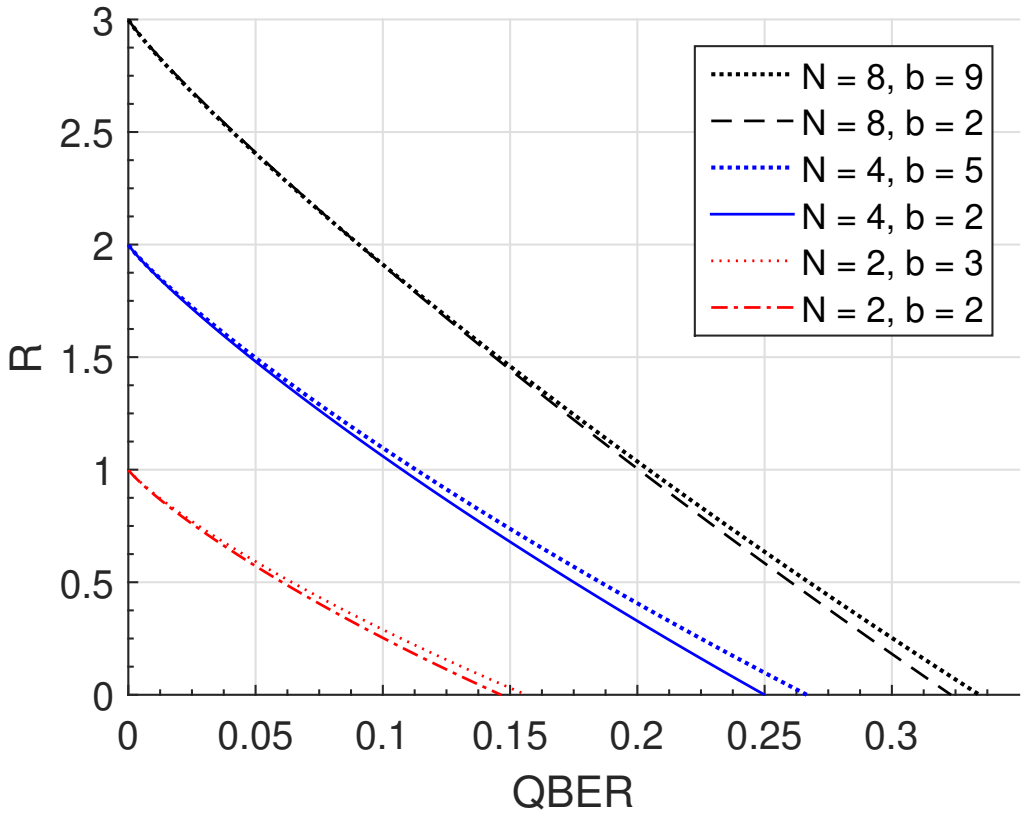


Figure P4.9: Bit rate in 2, 4 and 8 dimensions using 2 and $N+1$ basis.

such a way that it arrives at Alice's phase modulators on their ascending edge, as shown in Fig. P4.10. In this way, Eve can theoretically have control of the θ_i phases introduced by Alice in Eq. (P4.16). Next, she can just intercept and measure these modified states and resend unmodified ones according with her measurements. We analyze the influence of this attack on our proposed system by generalizing the results of Fung et al. [Fung et al., 2007].

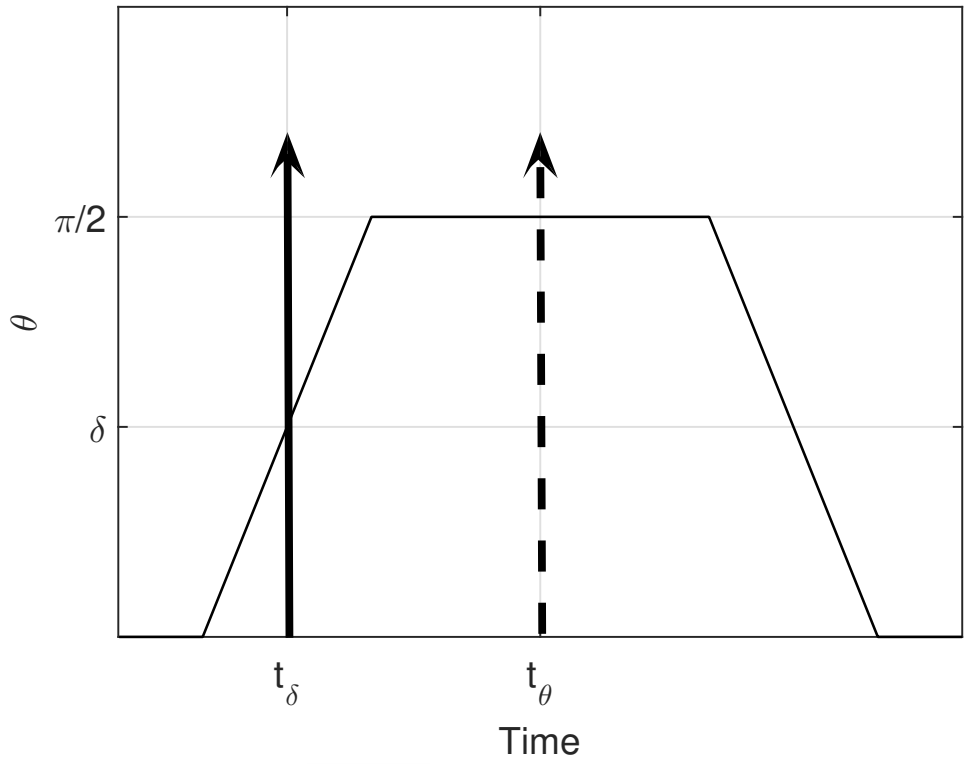


Figure P4.10: Time response of the phase modulator. The original pulse is time-shifted so it reaches the modulator at time t_δ instead of time t_θ.

Alice encrypts the information in the θ_i phases of the different spatial modes, as indicated in Eq. (P4.16). At this point, it is important to comment some properties of the encryption θ_i phases. Thus, if we look the MUBs for dimension $N = 2$ given by Eq. (P4.17), we can see that the four states are defined by a phase shift between the first and second mode of $\theta = \{0, \pi/2, \pi, 3\pi/2\}$. As MUBs for dimension $N = 2^n$ can be factorized in the two basis of dimension $N = 2$, as shown in reference [Tselniker et al., 2009], it is easy to check that each state of dimension 2^n is defined by m phase shifts $\{\theta_i\}_{i=1}^{n}$, and so each state corresponds to a m-qudit, while the rest of phases are functions of them $\{\theta_i\}_{i=n+1}^{N} = \{\theta_i\,(\{\theta_i\}_{i=1}^{m})\}_{i=m+1}^{N}$. Either way, as we can see in cases $N = 4$, such as the one given by Eq. (P4.18), and $N = 8$, such as the one given by Eq. (P4.19), all phase shifts $\{\theta_i\}_{i=1}^{N}$ introduced by Alice in state (P4.16) acquire values $\{0, \pi/2, \pi, 3\pi/2\}$.

As stated before, in the PR attack Eve time-shifts the light pulses arriving to Alice before the encryption, in order to modify the applied phase. Therefore, Eve changes the values of $\{\theta_i\}_{i=1}^{N}$ from $\{0, \pi/2, \pi, 3\pi/2\}$ to $\{0, \delta, 2\delta, 3\delta\}$. In consequence, Alice is actually introducing phases $\theta_i = k_i\delta$ in state (P4.16), thus, she is indeed sending the state

$$|\tilde{\psi}_{bs}\rangle \approx 2^{-\frac{n}{2}} e^{i\sigma}\{e^{-i\sigma_1}e^{ik_1\delta}|1_1\rangle + e^{-i\sigma_2}e^{ik_2\delta}|1_2\rangle + ... + e^{-i\sigma_N}e^{ik_N\delta}|1_N\rangle\}. \tag{P4.48}$$

In order to analyze the influence of the attack we follow the same approach as in reference [Fung et al., 2007], but generalizing it to more dimensions. Let us call Alice's unmodified encrypted states (P4.16) $|\psi_{bs}\rangle$ and the modified ones (P4.48), as a result of the PR attack, $|\tilde{\psi}_{bs}\rangle$, where once again b represents the base of the state and s the qudit value of the state. As an example, $|\psi_{21}\rangle$ for dimension $N = 8$ corresponds to the first column of matrix in Eq. (P4.19). As explained before, Eve interference in the system modifies Alice encrypted states (P4.16) into states (P4.48), and then, she intercepts and measures them by performing a positive-operator valued measure (POVM). The POVM consists in $n_b \cdot N + 1$ elements $\{M_{vac}, M_{bs} : b = 1...n_b, s = 1 \dots N\}$, where n_b is the number of basis used and N the dimension of the states. This means that she performs measurements for each of all the possible states as well as the vacuum. When Eve gets a measurement in $M_{b's'}$, she sends the corresponding unmodified state $|\psi_{b's'}\rangle$ to Bob. If Alice sends a state $|\tilde{\psi}_{b_0s_0}\rangle$, the probability of Eve to measure $M_{b's'}$ is given by $\mathrm{Tr}(M_{b's'}\,|\tilde{\psi}_{b_0s_0}\rangle\,\langle\tilde{\psi}_{b_0s_0}|)$. To obtain Bob's QBER under the PR attack we have to analyze three different possibilities when he receives the state $|\psi_{b's'}\rangle$. First, if $b' = b_0, s' = s_0$, which means that Alice actually sent $|\tilde{\psi}_{b's'}\rangle$, then Eve sends to Bob the right state and so, no error is committed (QBER= 0). However, if Alice sends a different state of the same basis ($b' = b_0, s' \neq s_0$), Bob always gets an error (QBER= 1). Finally, if Alice sends a state from a different basis ($b' \neq b_0$), then Bob will get an error except when the qudit sent and received is the same in both basis $s' = s_0$; for dimension N, QBER= $\frac{N-1}{N}$. The total QBER will be given by the sum of the different QBERs weighted by the probabilities of each case happening for all the possible states and moreover normalized by the total probability of Eve sending states to Bob

$$\mathrm{QBER} = \frac{\sum_{b=1}^{n_b}\sum_{s=1}^{N}\mathrm{Tr}(M_{bs}L_{bs})}{\sum_{b=1}^{n_b}\sum_{s=1}^{N}\mathrm{Tr}(M_{bs}B)}, \tag{P4.49}$$

where n_b is the number of basis used, N is the dimension and

$$L_{bs} = \sum_{\substack{j=1\\ j\neq s}}^{N} |\tilde{\psi}_{bj}\rangle\,\langle\tilde{\psi}_{bj}| + \frac{N-1}{N}\sum_{\substack{i=1\\ i\neq b}}^{n_b}\sum_{j=1}^{N} |\tilde{\psi}_{ij}\rangle\,\langle\tilde{\psi}_{ij}|, \tag{P4.50}$$

$$B = \sum_{i=1}^{n_b}\sum_{j=1}^{N} |\tilde{\psi}_{ij}\rangle\,\langle\tilde{\psi}_{ij}|. \tag{P4.51}$$

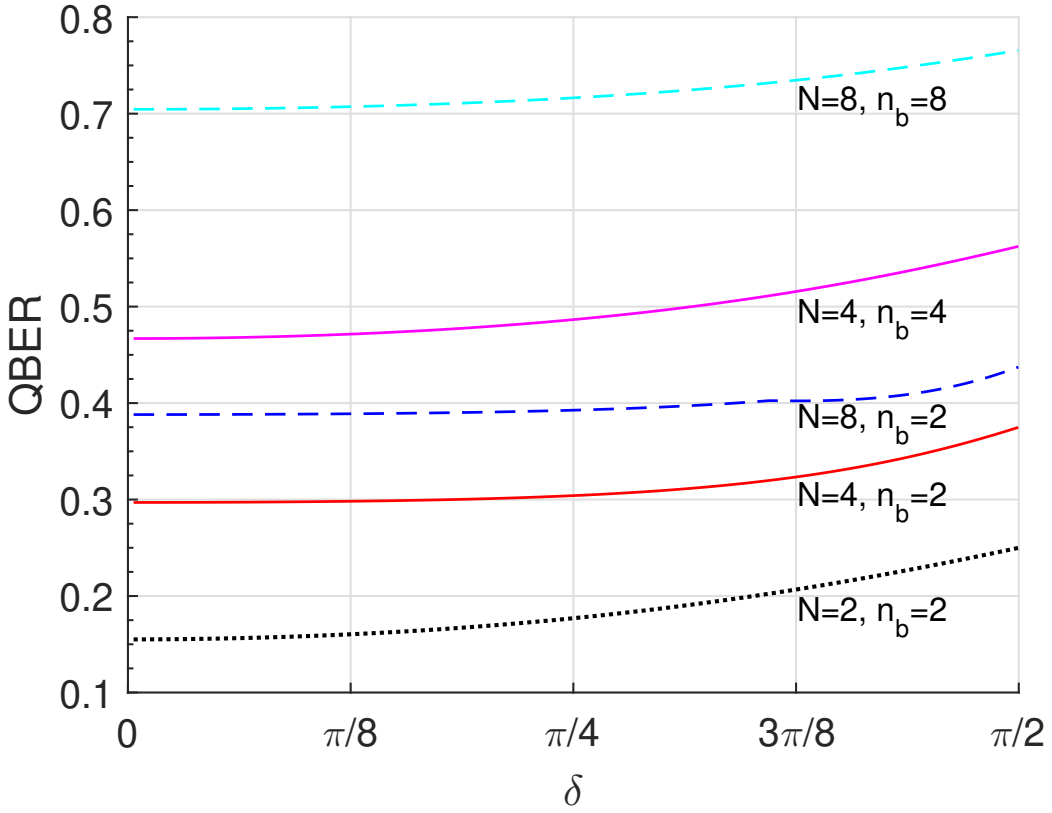


Figure P4.11: QBER achieved in a PR attack for different δ in different dimensions N and with n_b basis used.

Next, by using matrices (P4.50) and (P4.51) and following closely the procedure introduced in reference [Fung et al., 2007], we can minimize the QBER for a general set $\{M_{vac}, M_{bs} : b = 1...n_b, s = 0 \dots N-1\}$. The results are shown in Fig. P4.11, where we represent the QBER curves for dimensions $N = 2, 4, 8$ using both 2 and N basis in each case. We can see that, in every curve, we obtain the maximum QBER when $\delta = \pi/2$, this is, when there is no PR attack. At the same time, we can observe that Eve achieves better QBER results when the modified phase δ tends to zero. In $\delta = 0$ there is a singularity, as in such a case Alice is always sending the same modified state and Eve acquires no information. In Table P4.2 we show the maximum QBER values obtained

Comparing the values for $\delta \to 0$ in Table P4.2 with those shown in Table P4.1, we can observe that the PR attack can not reduce the QBER enough in order to enter in the range of values that generates a secret key rate under a cloning attack. In consequence, it is easy to detect if an eavesdropper is performing a PR attack, and then, with QBER values inferior to those shown in Table P4.1, security should be guaranteed excluding other possible attacks. Finally, note that if $\delta = \pi/2$, we obtain the expected results from

a classical intercept-and-resend attack for each n, that is, QBER $= \{\frac{1}{4}\ \frac{3}{8}, \frac{7}{16}, \frac{9}{16}, \frac{49}{64}\}$.

Table P4.2: Maximum and minimum QBER values under PR attack

N	n_b	$\delta \to 0$ (%)	$\delta = \pi/2$ (%)
2	2	15.5	25
4	2	29.7	37.5
8	2	38.8	43.75
4	4	46.6	56.25
8	8	70.4	76.56

P4.6 Conclusions

In this work we have proposed a method for phase and polarization autocompensating in N-dimensional QKD by using the spatial modes of MCFs. As shown, this method would not only help prevent problems in real systems, which will inevitably present phase and polarization drifts, but will also compensate for the delays and attenuations of the different modes The autocompensating method is based in the use of strong coherent pulses making N trips between Alice and Bob and implemented through the use of optical circulators (with HWPs in Alice system) combined with electro-optical reconfigurable directional couplers to control circulation in Bob system. The attenuation up to a quasi-single-photon level and encryption of the quantum light can be done in the last trip of the system by Alice using any attenuation system and electro-optic phase shifters, respectively. Moreover, we must stress that the optical fiber losses themselves are not considered as a drawback because they contribute also to the attenuation of the coherent states. Likewise, we have proposed specific integrated devices for generation and projective measurement in random basis of states for the particular cases $N = 4, 8$, although its extension to an arbitrary N dimension is direct, as shown along the work. Finally, we have shown that an intercept-and-resend attack allowed by our system, like the phase-remapping attack, does not achieve better results than a quantum cloning attack, also employed in one-way QKD protocols, which probes robustness of our proposal.

Acknowledgements

Authors wish to acknowledge the financial support of this work by Xunta de Galicia, Consellería de Educación, Universidades e FP, by a predoctoral grant (D. Balado), co-financied with the European Social Fund within the FSE Galicia 2014-2020 Operational Programme, and a grant GRC no. ED431C 2018/11 by the former institution.

P5 Fully autocompensating high-dimensional quantum cryptography by optical phase conjugation

ARXIV PREPRINT
arXiv:2009.13915

SUBMITTED 29 Sep 2020

by JESÚS LIÑARES[1] & XESÚS PRIETO-BLANCO & DANIEL BALADO[1] & GABRIEL M. CARRAL

[1] Quantum Materials and Photonics Research Group, Optics Area, Department of Applied Physics, Faculty of Physics / Faculty of Optics and Optometry, University of Santiago de Compostela, Campus Vida s/n, E-15782, Santiago de Compostela, Galicia, Spain

Abstract: *We present a bidirectional quantum communication system based on optical phase conjugation for achieving fully autocompensating high-dimensional quantum cryptography. We prove that random phase shifts and couplings among $2N$ spatial and polarization optical modes described by SU(2N) transformations due to perturbations are autocompensated after a single round trip between Alice and Bob. Bob can use a source of single photons or, alternatively, coherent states and then Alice attenuates them up to a single photon level, and thus non-perturbed 1-qudit states are generated for high-dimensional QKD protocols, as the BB84 one, of a higher security.*

Daniel Balado Souto

P5.1 Introduction

Quantum cryptography is based on the properties of quantum mechanics to obtain secure quantum key distribution (QKD) by using different protocols. One of them is the seminal so-called BB84 protocol in which four states define a set of two mutually unbiased basis (MUBs). On the other hand, space division multiplexing has been proposed to further increase the data bandwidth in optical fiber communications [Bai et al., 2012], and accordingly, high interest has arisen in new optical fibers such as few-mode fibers and multicore fibers. Likewise, optical satellite communications, and in general free space optical communications, based on spatial modes, such as those ones carrying orbital angular momentum, constitutes a promising communications technology [Zou et al., 2018].

In parallel, the interest in the implementation of quantum cryptography in both these new optical fibers and in free space has also remarkably increased in the last few years. The main reason is that by using spatial optical modes a high-dimensional QKD (HD-QKD) can be implemented, which in turn improves cryptographical security [Ding et al., 2017]. Different optical systems have been proposed to implement QKD cryptography in both optical fibers and free space; such systems can use different kind of modes, for instance, polarization modes in monomode optical fibers [Muller et al., 1997] and free space [Bedington et al., 2017], collinear spatial modes in few-mode optical fibers [Cozzolino et al., 2019] and free space [Jin et al., 2020] and spatial codirectional modes in multicore optical fibers [Cañas et al., 2017]. However, one of the most important drawbacks is that all guided and free space modes need to keep stable over long propagation distances along optical fibers or the atmosphere. Modes undergo instability because light, in its propagation in free space or along optical fibers, finds small spatial perturbations (imperfections) or slow temporal perturbations. This gives rise to random modal coupling (modal crosstalking) which, together with random intermodal phases, causes instability of both modes and quantum states. To overcome this drawback, specific (partial) autocompensating techniques have been proposed in bidirectional quantum communication systems. For instance, polarization autocompensating quantum cryptography with 1-qubit states excited in polarization modes [Muller et al., 1997, Bethune and Risk, 2002], or more recently with 1-qudit states excited in spatial modes acquiring random relative phases [Balado et al., 2019, Balado Souto et al., 2019]. However, to our knowledge, a fully autocompensating solution has not been proposed.

In this Letter we propose and prove a fully autocompensating quantum cryptography technique based on optical phase conjugation (OPC) and valid for both free space optical communication and optical fiber communications where spatial and polarization modal couplings are not negligible. In a most formal way, by using OPC we compensate for unwanted effects in 1-qudit states caused by an arbitrary number q of unpredictable unitary transformations $\mathrm{SU}(2N)$, where $2N$ is the number of spatial modes with two polarizations. For the sake of expositional convenience we present a detailed study for multicore optical fibers (MCF) which can in turn be formally applied to both few-mode optical fibers (FMFs) and free space communications. Input multimode single photon

states can be used, or alternatively, coherent states which are attenuated in their way back up to a single photon level (weak coherent states), so that 1-qudit states are produced. In this case, decoy states [Hwang, 2003] have also to be generated for security purposes, as usual.

P5.2 Optical phase conjugator

Let us consider a four-wave mixing (FWM) non-linear interaction system as shown in Fig. P5.1. In general, an input spatial multimode optical quantum state $|L\rangle$ propagating along $-z$ direction and with frequency ω reaches the FWM system; such state emerges from an optical fiber (OF). After the OF a collimating lens (CL) is inserted for collimating the optical fiber modes $\mathbf{e}_j(x,y)$, j=1, ..., N. This CL is not strictly necessary but helps to understand the physical process. After the collimating lens, a polarizing beam-splitter (PBS) separates horizontal and vertical polarization modes (x and y-modes). The linear x-polarization mode is rotated $\pi/2$ by means of a $\mathrm{HWP}_{\pi/4}$ (HWP rotated $\pi/4$). Finally, we have a third order non linear material of length l in which it is considered that there are two strong vertically polarized counter-propagating intense pump modes (strong coherent states) of frequency ω and amplitudes A_{1y} and A_{2y}. A possible isotropic non linear material for implementing OPC can be CS_2 [Pepper et al., 1978], which would contribute for vertical polarization with the term $\chi^{(3)}_{yyyy}$ of the third order non linear tensor. For the moment, let us consider that $|L\rangle$ is a single mode state excited in the incident mode 3 coming from an OF and with an associated optical field operator $\hat{\mathrm{E}}_{3y} \propto \hat{a}_{3y}$, with $\hat{a}_{3y}$ an absorption operator. When $|L\rangle$ reaches the non linear material then a fourth mode (reflected mode 4) arises, with an associated field operator $\hat{\mathrm{E}}_{4y} \propto \hat{a}_{4y}$. We are interested on the quantum states propagating along z-direction in modes 3 and 4 (idler and signal modes) after non linear interaction, that is, in spatial propagation not in temporal evolution (Hamiltonian operator) [Ben-Aryeh and Serulnik, 1991]. Therefore, for spatial non-linear coupling is convenient to use the Momentum operator describing the quantum mode interaction [Pepper et al., 1978, Ben-Aryeh and Serulnik, 1991, Liñares et al., 2008],

$$\hat{M}_I = \int \chi^{(3)}_{yyyy} \mathrm{E}_{1y} \mathrm{E}_{2y} \hat{\mathrm{E}}_{3y} \hat{\mathrm{E}}_{4y}\, dxdydt, \tag{P5.1}$$

where the intense pump waves 1 and 2 can be treated classically and modes 3 and 4 in a quantum way, that is,

$$\mathrm{E}_{\binom{1y}{2y}} = \mathrm{A}_{\binom{1y}{2y}}\, e^{\mp ik_o nx}\, e^{-i\omega t} + c.c., \tag{P5.2}$$

$$\hat{\mathrm{E}}_{\binom{3y}{4y}} = \sqrt{\hbar\omega}\, \mathrm{e}^{\binom{3}{4}}_j(x,y)\, \hat{a}_{\binom{3y}{4y}}\, e^{\mp ik_o nz}\, e^{-i\omega t} + h.c., \tag{P5.3}$$

where e_j is a jth normalized spatial mode of the OF with x or y-polarization. As these modes are collimated by the CL then $\mathrm{e}^{(3)}_j \approx \mathrm{e}^{(4)}_j$. By inserting the above pump waves and operators into Eq. (P5.1) and performing the temporal integrations the following operator

is found

$$\hat{M}_I = \hbar\chi_{eff} \mathrm{A}_{1y}\mathrm{A}_{2y}\hat{a}^\dagger_{3y}\hat{a}^\dagger_{4y} + h.c., \tag{P5.4}$$

where χ_{eff} is an effective non-linear susceptibility which groups together all physical constants. From this operator the spatial Heisenberg equations [Ben-Aryeh and Serulnik, 1991] can be obtained,

$$-i\hbar\frac{\partial \hat{a}_{my}}{\partial z} = [\hat{a}_{my}, \hat{M}_I], \tag{P5.5}$$

where $m=3,4$. Let us denote the input operators as $\hat{a}_{3y}(l) \equiv \hat{a}_{o3}$ and $\hat{a}_{4y}(0) \equiv \hat{a}_{o4}$, and the output operators as $\hat{a}_{3y}(0) \equiv \hat{a}_3$, associated to the optical mode transmitted along system, and $\hat{a}_{4y}(l) \equiv \hat{a}_4$, associated to the reflected optical mode (see Fig. P5.1). As mentioned, there are two pump waves with very large amplitudes A_{1y} and A_{2y} and initial phases equal to zero, then the non-linear interaction strength is given by a coupling coefficient $\kappa = \chi_{eff}|\mathrm{A}_{1\mathrm{y}}||\mathrm{A}_{2\mathrm{y}}|$, therefore the coupling is parametrically governed by $|\mathrm{A}_{1\mathrm{y}}||\mathrm{A}_{2\mathrm{y}}|$, that is, the efficiency of the process is governed by pumping. It is easy to check that the solutions of the spatial Heisenberg equations obtained by inserting Eq. (P5.4) into Eq. (P5.5) provide the well-known operator transformations [Pepper et al., 1978, Mandel and Wolf, 1995]

$$\hat{a}_{3y}(l) \equiv \hat{a}_{o3} = \sec(\kappa l)\,\hat{a}_3 + i\tan(\kappa l)\,\hat{a}^\dagger_4 \tag{P5.6}$$

$$\hat{a}_{4y}(0) \equiv \hat{a}_{o4} = \sec(\kappa l)\,\hat{a}_4 + i\tan(\kappa l)\,\hat{a}^\dagger_3. \tag{P5.7}$$

Next, let us consider a coherent state $|L\rangle = |\alpha_3 0_4\rangle$ excited in an optical fiber mode. By taking into account the complex displacement operator and using Eq. (P5.6) the output state can be rewritten as follows

$$|L\rangle = e^{\alpha\hat{a}^\dagger_{o3} - \alpha^\star \hat{a}_{o3}}\,|00\rangle \rightarrow |L_c\rangle = |s\alpha\rangle\,|\text{-}it\alpha^\star\rangle, \tag{P5.8}$$

where s=sec(κl) and t=tan(κl). Note that the reflected coherent state has been conjugated, that is, the FWM is an OPC; besides, quantum-mechanically the OPC means that $\hat{a}_{o3} \propto \hat{a}^\dagger_4$. Let us recall, however, that we are interested in multimode coherent states, that is, $|L\rangle = |\alpha_1 ... \alpha_N\rangle$ excited in N optical modes, therefore, the OPC produces the multimode coherent state $|L_c\rangle = (|s\alpha_1\rangle\,|\text{-}it\alpha_1^\star\rangle) \ldots (|s\alpha_N\rangle\,|\text{-}it\alpha_N^\star\rangle)$. Alternatively, we could have a single photon source, therefore we can generate an input 1-qudit state $|L_o\rangle = \sum_{o3j} c_j|1_{o3j}\rangle$, with, $j=1,...N$, where the subindex $o3j$ indicates that the N modes are incident on the OPC. By taking into account that $|1_{o3j}\rangle = (\hat{a}^\dagger_{o3j} + \hat{a}_{o3j})|0\rangle$, we obtain the output quantum state $|L\rangle = s\sum_{3j} c_j|1_{3j}\rangle + it\sum_{4j} c_j|1_{4j}\rangle$.

P5.3 Autocompensation with codirectional modes

First of all and for the sake of expositional convenience, we provisionally assume that polarization is maintained under propagation (we will consider spatial and polarization couplings later, although in atmosphere and special optical fibers polarization can be maintained), therefore we only consider coupling among N spatial modes with the same linear polarization. In particular, let us consider codirectional modes of a MCF with

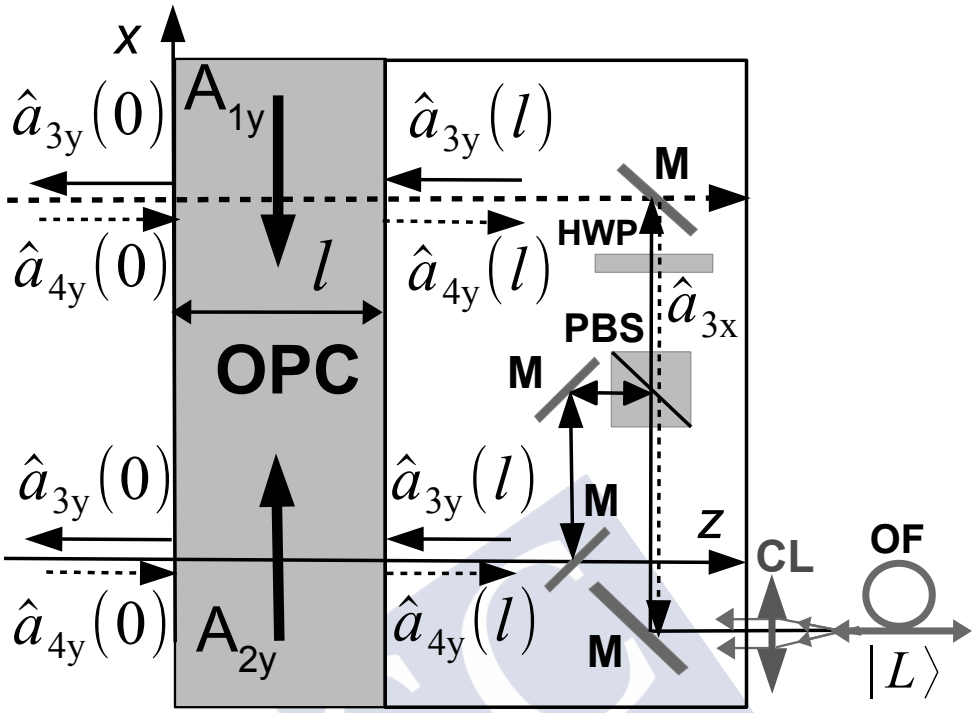


Figure P5.1: Four-wave mixing system with two pump waves A_{1y} and A_{2y} and an input state $|L\rangle$ emerging from an optical fiber (OF) along $-z$. Optical fiber modes are collimated by a lens (CL) and redirected by mirrors (M). PBS separates polarizations, and vertical or x-polarization becomes vertical or y-polarization by using a HWP rotated $\pi/4$. Finally, the non-linear medium implements an optical phase conjugation of the reflected modes $\hat{a}_{4y}$.

N modes (cores) whose propagation constants are β_{oi}, $i=1,...,N$ and with associated absorption operators $\hat{a}_i$. We must stress that the results that we are going to obtain are also valid for collinear modes of FMF or a free space optical modes. The quantum state reaching Bob system from the Alice system will be an unpredictable quantum state, and as a consequence, modal coupling prevents us to implement any QKD protocol. Next, we show how to overcome this drawback by OPC. Let us consider a perturbation $P_s(x,y)$ that induces modal coupling and can be considered as z-invariant along a distance s, then the spatial Heisenberg equation describing modal coupling among N optical field operator modes $\hat{E}_i \propto \hat{a}_i$ can be written as follows [Liñares et al., 2008]

$$-i\hbar\frac{\partial \hat{a}_i}{\partial z} = \hbar\{\beta_i \sum_{j=1}^{N} \delta_{ij}\hat{a}_j + \sum_{j\neq i}^{N} \kappa_{ij}\hat{a}_j\} \equiv \hbar \sum_{j=1}^{N} C_{ij}\hat{a}_j, \tag{P5.9}$$

here $\beta_i = \beta_{oi} + \kappa_{ii}$ are the perturbed propagation constants due to (random) modal self-coupling (κ_{ii}), and κ_{ij} are (random) modal coupling coefficients due to cross coupling. From a most fundamental point of view, an arbitrary coupling coefficient of spatial modes

i,j is given by $\kappa_{ij}=\int \mathrm{e}_i(x,y)P_s(x,y)\mathrm{e}_j(x,y)dxdy$, where $\mathrm{e}_{(i,j)}(x,y)$ are the mode amplitudes. Note that $\kappa_{ij}=\kappa_{ji}$ and therefore $[C_{ij}]\equiv C$ is a symmetric matrix. Therefore, by using the algebraic properties of symmetric matrices, the formal matrix solution $[S_{ij}]\equiv S=\exp\{iCz\}$ of differential equation in Eq. (P5.9) is a complex symmetric matrix, that is, $S_{ij}=S_{ji}$. On the other hand, modal coupling is an unitary transformation, therefore $[S_{ij}]^{-1}=[S_{ji}]^{\star}=[S_{ij}]^{\star}$. In general, we will have an arbitrary number q of perturbations, accordingly, the total effect along z direction from a system B (Bob) to system A (Alice) can be represented by the total matrix $M=S_1\cdots S_q$. Then, if we have an OPC at A, the matrix M becomes $M^{\star}=S_1^{\star}\cdots S_q^{\star}$. Now, the quantum state is propagated back to system B, therefore we have to use a reflected coordinate system which is defined, without loss of generality, by $(-x)y(-z)$ with respect to the incident coordinate system xyz. The coupling coefficients κ_{ij} are invariant under the transformation $x\rightarrow -x$ and consequently the matrices C are also invariant. Once the light has travelled the path back and forth, the total coupling matrix is $M^tM^{\star}=\mathbb{I}$, with super index t indicating transpose. Then, the unpredictable modal coupling has been removed. In short, if Bob launches a state $|L\rangle$ undergoing modal coupling along an OF or in the atmosphere, the state after the OPC and travelling its way back is $|L_c\rangle=(|s\alpha_1\rangle\,|\text{-}it\alpha_1^{\star}\rangle)\ldots(|s\alpha_N\rangle\,|\text{-}it\alpha_N^{\star}\rangle)$, that is, we recover the initial state except phases π and conjugations.

P5.4 Autocompensation with spatial and polarization modes

As commented, we also have to remove unpredictable polarization modal coupling together with the above spatial modal coupling. First of all we characterize the matrix transformation produced by an arbitrary coupling between linearly polarized spatial modes (e.g., LP modes). Since there are $2N$ modes we consider the new subindices $i,j=\{1H,1V,2H,2V,...,NH,NV\}$, with $H\equiv x$, $V\equiv y$. As in the above (scalar) case, the coupling matrix $[C_{ij}]\equiv C$ is also a complex symmetric matrix. However, when considering back propagation, this matrix gets modified because, as commented, the incident coordinate system xyz becomes $(-x)y(-z)$ under reflection. Indeed, an arbitrary coupling coefficient of spatial modes m,n with different polarization is given by $\kappa_{mHnV}=\int \mathrm{e}_{mH}(x,y)P_v(x,y)\mathrm{e}_{nV}(x,y)dxdy$, where $P_v(x,y)$ is an arbitrary perturbation producing polarization (vector) modal coupling. Obviously, under reflection (back path) we have $\mathrm{e}_{nH}(x,y)\rightarrow-\mathrm{e}_{nH}(x,y)$, then $\kappa_{ij}\equiv\kappa_{mHnV}\rightarrow-\kappa_{mHnV}\equiv-\kappa_{ij}$. Note that for the same polarization the coupling coefficient is positive (or zero) under reflection. Therefore, the coupling matrix $[B_{ij}]\equiv B$ under reflection can be written as follows

$$B=(I_N\otimes\sigma_z)\,C\,(I_N\otimes\sigma_z)\equiv D\,C\,D, \tag{P5.10}$$

with I_N the N-dimensional identity matrix, $\otimes$ the tensor product and σ_z the third Pauli matrix. Next, by taking into account that $DD=(I_N\otimes\sigma_z)(I_N\otimes\sigma_z)=I_{2N}$ (I_{2N} the identity matrix $2N$x$2N$), it is easy to check that the transformation matrix produced by the perturbation $P_v(x,y)$, that is, the formal matrix solution $[R_{ij}]\equiv R=\exp\{iBz\}$ can be

written, by using the Taylor expansion of an exponential function, as follows

$$R = (I_N \otimes \sigma_z)\, S\, (I_N \otimes \sigma_z) \equiv D\, S\, D. \tag{P5.11}$$

where S=exp$\{iCz\}$. Note that matrix R (transformation of the absorption operators $\hat{a}_{jH}, \hat{a}_{jV}$) is also symmetric. On the other hand, it is also easy to check that the HWP$_{\pi/4}$ introduces a phase π between H-mode and V-mode of every spatial mode in its way back. Therefore, after OPC system, when polarization modes are recombined in the PBS (see Fig. P5.1), the matrix $D = I_N \otimes \sigma_z$ is implemented. Consequently, by considering the general case of q random couplings, we obtain, after the path back to Bob, the total matrix

$$M_T = R_q \cdots R_1 D S_1^\star \cdots S_q^\star = D, \tag{P5.12}$$

where we have taken into account the following relationships $R_k = DS_kD$, $DD = I_{2N}$ and $S_k S_k^\star = I_{2N}$, $k = 1, ...q$. In short, symmetric spatial perturbations together with polarization perturbations have been removed.

P5.5 General SU($2N$) autocompensation

The above results have made clear autocompensation of symmetric unitary coupling transformations. Now, we generalize the above results for non symmetric unitary coupling transformations, for example, rotations due to optical activity (N=1), $2N$x$2N$ abstract rotations and so on, that is, SU($2N$) perturbations. In order to prove this assertion we must take into account that all unitary transformation SU(2N) can be factorized as a ordered product of SU(2) transformations of subspaces i, j [Reck et al., 1994,de Guise et al., 2018]. Thus, by proving autocompensation by OPC of an arbitrary SU(2) transformation the case SU($2N$) is also proven. A general SU(2) transformation S can be represented by

$$S = \begin{pmatrix} \cos\theta & i\sin\theta e^{-i\delta} \\ i\sin\theta e^{i\delta} & \cos\theta \end{pmatrix} \equiv Z(\delta)X(\theta)Z(-\delta) \tag{P5.13}$$

with $Z(\pm\delta)$=$diag(1, e^{\pm i\delta})$ the matrix of a phase retarder $\pm\delta$ generated by the the Pauli's matrix σ_z, and $X(\theta)$ a matrix whose generator is the Pauli's matrix σ_x, with elements $X_{11}(\theta)$=$X_{22}(\theta)$=cos$\,\theta$, and $X_{12}(\theta)$=$X_{21}(\theta)$=$i\sin\theta$. By considering that we are in a polarization two-mode subspace, it is easy to check that the matrix by reflection is characterized by the changes $\delta, \theta \to -\delta, -\theta$, then $T = D_2 S^T D_2$, where $D_2 = \sigma_z$. Therefore, after OPC and by taking into account the action of the HWP$_{\pi/4}$ (D_2) we obtain the following result

$$T S^\star = D_2 S^T D_2\, D_2\, S^\star = D_2 S^T\, S^\star = D_2, \tag{P5.14}$$

and then autocompensation is again achieved. Rigorously, a general SU(2) matrix requires to consider an additional matrix corresponding to a α-phase retarder, that is, $Z(\alpha)S$; however, a retarder is also autocompensated, as proven above. We must also stress that similar results are found for spatial two-mode subspace. Likewise, topological phases due to helical paths, torsions and so on of an OF can be also autocompensated because such

phases also correspond to unitary transformations (rotations and so on) [Berry, 1987]. In short, a multimode coherent state $|L\rangle = |\alpha_{1H}\alpha_{1V}...\alpha_{NH}\alpha_{NV}\rangle$ coming from Bob, becomes a predictable reflected multimode coherent state $|L_c\rangle = |-it\alpha_{1H}\, it\alpha_{1V}...-it\alpha_{NH}\, it\alpha_{NV}\rangle$, therefore, we have proved that OPC has cancelled a number q of unpredictable perturbations represented by SU($2N$) transformations.

P5.6 Optical fiber setup for HD-QKD

By taking into account the results obtained we can implement an autocompensating optical system for HD-QKD BB84 quantum cryptography in optical fibers. Such a system is shown in the sketch of Fig. P5.2. Its optical configuration is as follows: the first device is a coherent states generator (CSG) located in Bob system, which emits coherent states $|L\rangle = |\alpha_{1H}\alpha_{1V}...\alpha_{NH}\alpha_{NV}\rangle$ to be excited in $2N$ optical modes of a MCF (or a FMF fiber, or free space), with $\alpha_{1H} = ... = \alpha_{NV}$, for generating quantum states belonging to MUBs. Next, optical fiber delayers (OFD_1) produce modal delays τ_j ($j = 1, ..., 2N$), that is, we have a multimode coherent state formed by the tensor product of delayed single mode coherent states. These delays will allow to Alice introduce phases in each spatial mode. Afterwards, a set of optical circulators (SOC) launches the state towards Alice system. Besides, a multiplexing/demultiplexing (MUX/DEMUX) device is also needed if collinear propagation is required as in a FMF or even in free space. Different spatial multiplexing devices can be implemented according to the kind of collinear modes [Liñares et al., 2017c, Leach et al., 2002]. Note that If we use a MCF then the MUX/DEMUX device is not required (codirectional modes).

After propagation along the OF each jth delayed single mode coherent state (excited in each core of a MCF) becomes a multimode coherent state due to modal coupling. Such an state reaches the OPC device described in detail in Fig. P5.1 and explained above. Note that now we have placed an electro-optic phase shifter (EPS) and an electro-optic

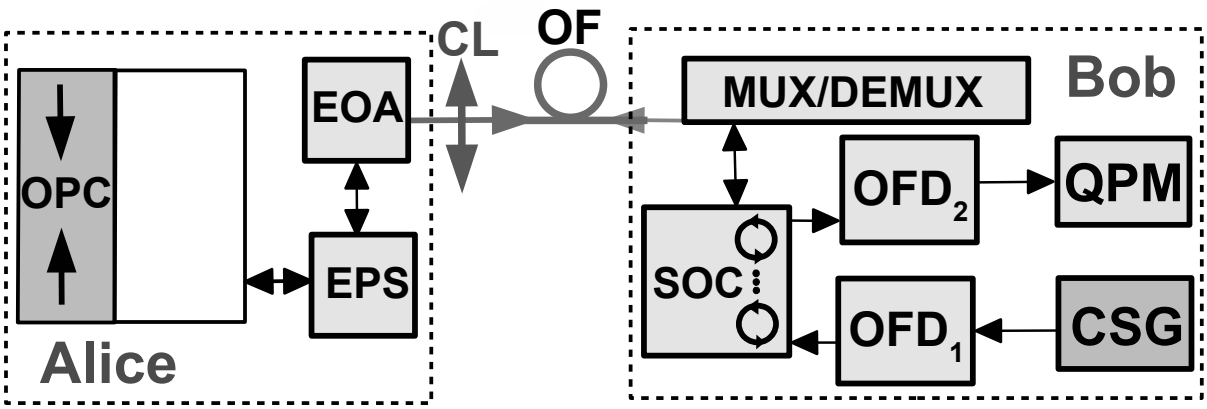


Figure P5.2: Basic optical fiber setup for autocompensating HD-QKD by OPC (see text under *Optical fiber setup for HD-QKD* for description).

attenuator (EOA) [Balado et al., 2019] in off-position between the OPC and the CL-OF (see Fig. P5.2). We must stress that after the OPC the reflected state has to be coupled again to the OF, however, the OPC implements by itself this transverse modal coupling to the OF (analogous to the well-known image restoration by OPC [Pepper et al., 1978, Mandel and Wolf, 1995]), although different systems can be used to optimize this coupling, for example, as in our case, by means of a CL. Next, the reflected state in the OPC device goes through the EPS which introduces global phases θ_j on the mentioned multimode coherent states, and the EOA attenuates the state up to single photon level (note that at Bob system each of these multimode states will become again a jth delayed single mode coherent state due to OPC). The purpose of the EOA is not only to attenuate but also to increase the security of the system, i.e., the attenuation of the EOA can be controlled, enabling the production of different attenuated pulses: signal and decoy states against different attacks of an eavesdropper Eve, as in the photon-number-splitting attack, although we must stress that modal coupling is also a defense against attacks in line. Therefore, Alice system generates 1-qudit states which propagate along the OF up to the Bob system and thus the modal coupling and relative phases are fully removed. Next, the set of optical circulators SOC sends the 1-qudit state to the OFD_2 device which cancels the delays τ_j between states $|1_j\rangle$ of the 1-qudit. In short, the quantum state generated is

$$|L_c\rangle \approx \frac{-i}{\sqrt{2N}}\{\sum_{j=1}^{N} e^{i\theta_{jH}}|1_{jH}\rangle - \sum_{j=1}^{N} e^{i\theta_{jV}}|1_{jV}\rangle\}. \tag{P5.15}$$

These states allow to implement pairs of $2N$-dimensional MUBs [Ding et al., 2017] for QKD. Finally, the state reaches a quantum projective measurer (PM). Since both PM and CSG are relevant devices it is worth showing a possible physical implementation of them. A CSG can be easily made by integrated devices with concatenated directional couplers 2x2, that is, each output of a coupler is connected to other coupler and so on [Ding et al., 2017, Balado et al., 2019]. Such couplers can be represented by matrices $X(\theta)$ such as the one presented in Eq.(P5.13) where $\theta{=}\kappa d$ with κ a linear coupling coefficient and d the coupling distance. We start from a single-mode coherent state $|L_{sm}\rangle = |\beta\rangle$, and by modal coupling with concatenated directional couplers $X(\pi/4)$ a multimode state $|L'_{sm}\rangle = |\alpha\rangle|i\alpha\rangle|-\alpha\rangle|i\alpha\rangle...|-\alpha\rangle|-i\alpha\rangle|-\alpha\rangle|i\alpha\rangle$ is obtained, where $\alpha = 2^{-N/2}\beta$. The relative phases $\{\pm\pi/2, \pi\}$ can easily be cancelled by using the EPS of the Alice system when the proper phases $\theta_{1H}, ...\theta_{NV}$ are introduced, then $|L\rangle = |\alpha\rangle...|\alpha\rangle$. As to the PM, a passive integrated quantum projective measurer that randomly selects bases of dimension $N{=}2^m$ in MCFs has been recently proposed by using $X(\pi/4)$ and $X(\pi/2)$ couplers and phase shifters $Z(\delta)$ [Balado et al., 2019]. Obviously, if we had used single photon sources both the attenuation and decoy states would not be required. Finally, we must indicate that bidirectional QKD systems are subject to new lateral attacks like the phase-remapping (PR) one. Likewise, recent security analysis considering such an attack have been made [Balado et al., 2019, Balado Souto et al., 2019], and it was shown that PR can not reduce the QBER bellow the minimum in which a secret key rate is guaranteed under a cloning

attack in a normal one-way system. Therefore, bidirectionality does not necessarily make the system more vulnerable.

P5.7 Free space optical communications

As commented, free space optical communications can be considered as a problem of $2N$ collinear modes. As in the case of FMFs, the generation and measurement of quantum states have to be made by a MUX/DEMUX process. A detailed study of this case would incorporate mode diffraction, however in most of cases it can be reduced thanks to the high directionality of lasers, or it can simply be ignored since OPC also compensates diffraction (note that a diverging wave incident on an OPC becomes a converging wave).

P5.8 Summary

We have presented a fully autocompensating technique based on optical phase conjugation for high-dimensional quantum cryptography in optical fibers and free space. A single round trip allows to auto-compensate the undesired modal coupling and random phase shifts among spatial and polarization modes, and thus HD-QKD protocols such as the BB84 can be implemented.

P5.9 Acknowledgements

Authors wish to acknowledge the financial support of this work by Xunta de Galicia, Consellería de Educación, Universidades e FP, with a grant Consolidation-GRC Ref.-ED431C2018/11, grant Strategic Grouping of Materials (AeMAT) Ref.-ED431E 2018/08, and a predoctoral grant (D. Balado, 2017), co-financied with the European Social Fund.

6

Conclusions

Quantum cryptography represents one of the quantum technologies with the highest potential to change our current society. Quantum key distribution will allow the establishment of totally secure communication systems. This dissertation has been dedicated to research and introduce improvements in the field of quantum cryptography. In particular, the main interest of the thesis has been to design new autocompensating systems to perform QKD in high dimension, as well as propose new devices to generate and measure quantum states.

To begin with, we have designed systems to generate quantum vortex states of light in different kind of modes, which have great potential for applications in several fields of quantum information processing. First, bulk generation methods with discrete photonic devices and based on spontaneous parametric down conversion (SPDC) were proposed to obtain vortex in polarization and colinear spatial modes. Then, these methods were translated into integrated optics. In this way, we have published two works where we have designed two integrated devices to generate vortex states in codirectional spatial modes (path modes) by means of SPDC. One works in a passive way, while the other has two active phase shifters that allows to modify the generated state. Finally, we have shown how we can use our devices to randomly generate four single-photon qubit states by lowering the pump in order to implement the two dimensional BB84 protocol. Moreover, we have extended our generator to produce all the possible states belonging to mutally unbiased bases in higher dimensions.

Next, we have presented an autocompensation system to perform the BB84 protocol in high dimension by spatial modes multiplexing in a few-mode fiber by using bulk systems with discrete photonic devices. The modes in a fiber are highly subjected to anisotropic effects and phase fluctuations and delays, as well as to coupling between them. We have minimized the latter by means of employing elliptical core fibers. In order to compensate the former, we proposed a multi-loop system of communication between the message sender, Alice, and the receiver, Bob. This strategy consists of the states making several back and forth trips between Alice and Bob, with an exchange between the base modes of the states by means of an "effective Faraday mirror" to make all modes experiment the same fluctuations. In addition, we have published a work where we combine polarization

and spatial modes to perform a four dimension autocompensating system, designing as well bulk systems for generation and meassurement of the states. Moreover, we have made a review of the security of QKD under side channel attacks and have made an analysis of our system's security under the phase remapping attack, which is specific to two-way systems like ours. However, we have proven that this attack does not represent a bigger threat to our system than other attacks for on-way systems, even when combining it with a detector efficiency mismatch attack.

Simultaneously, we have demonstrated in our lab the possibility of manufacturing integrated devices made of potassium in glass through ion exchange for being used in quantum cryptography. Integrated devices are a better approach to perform the required operations of generation and measurement of states than discrete devices. In this thesis, we have successfully fabricated and characterized couplers employing lithographic and ion exchange techniques with silver and potassium. We developed a two step lithographic system that allow us to get a reduction of about $\times 70.55$ to easily obtain waveguides of 3 μm, and we have determined the fabrication parameters required to obtain single-mode waveguides. Moreover, we have characterized these couplers through polarizing interference microscopy, to measure their characteristics, and through coherent light, to show how they are fully functional. Lastly, we show how the couplers can be used to divide and project incident light, which means that they can be used to generate and measure quantum states.

Finally, we have combined such integrated devices with multi-core fibers in order to design autocompensation systems to perform high dimension quantum key distribution with path modes.We have proposed two different strategies.

To begin with, we have applied our proposed multi-loop autocompensation system using path modes with integrated devices. In this case, optical circulators work as an "effective Faraday mirror" exchanging the path modes of the state and half-wave plates are also used to compensate polarization fluctuations in each core of the fiber. A second strategy is based in utilising phase conjugation. We have demonstrated that phase conjugation can compensate the different modal couplings happening between polarization modes and different cores, while correcting phase shifts between them at the same time. Thus, Alice can apply phase conjugation to an incident pulse sent by Bob before coding information in it and resend it back. Moreover, we have designed a generic integrated quantum projectors to measure all possible states in path modes belonging to all the mutually unbiased basis of dimension 2^n. These devices can be used in these systems and are natural detectors for our proposed generators.

Bibliography

[Agarwal et al., 1982] Agarwal, G. S., Friberg, A. T., and Wolf, E. (1982). Elimination of distortions by phase conjugation without losses or gains. *Optics Communications*, 43(6):446–450.

[Agarwal et al., 1983] Agarwal, G. S., Friberg, A. T., and Wolf, E. (1983). Scattering theory of distortion correction by phase conjugation. *JOSA*, 73(5):529–538.

[Agarwal and Tara, 1991] Agarwal, G. S. and Tara, K. (1991). Nonclassical properties of states generated by the excitations on a coherent state. *Physical Review A*, 43(1):492.

[Agarwal et al., 1997] Agarwal, G. S., Puri, R. R., and Singh, R. P. (1997). Vortex states for the quantized radiation field. *Physical Review A*, 56(5):4207.

[Agarwal and Banerji, 2006] Agarwal, G. S. and Banerji, J. (2006). Entanglement by linear SU(2) transformations: generation and evolution of quantum vortex states. *Journal of Physics A: Mathematical and General*, 39(37):11503.

[Agarwal, 2011] Agarwal, G. S. (2011). Engineering non-Gaussian entangled states with vortices by photon subtraction. *New Journal of Physics*, 13(7):073008.

[Agarwal, 2012] Agarwal, G. S. (2012). *Quantum Optics*. Cambridge University Press.

[Alibart et al., 2016] Alibart, O., D'Auria, V., De Micheli, M., Doutre, F., Kaiser, F., Labonté, L., Lunghi, T., Picholle, É., and Tanzilli, S. (2016). Quantum photonics at telecom wavelengths based on lithium niobate waveguides. *Journal of Optics*, 18(10):104001.

[Allen et al., 1992] Allen, L., Beijersbergen, M. W., Spreeuw, R. J. C., and Woerdman, J. P. (1992). Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. *Physical Review A*, 45(11):8185.

[Andersen et al., 2015] Andersen, U. L., Neergaard-Nielsen, J. S., Van Loock, P., and Furusawa, A. (2015). Hybrid discrete-and continuous-variable quantum information. *Nature Physics*, 11(9):713–719.

[Antoniades et al., 2004] Antoniades, I. P., Chouvardas, V. G., Hatalis, M. K., and Bleris, G. L. (2004). Quantum cryptography: A short historical overview and recent developments.

[Aspect et al., 1982] Aspect, A., Dalibard, J., and Roger, G. (1982). Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49(25):1804.

[Babazadeh et al., 2017] Babazadeh, A., Erhard, M., Wang, F., Malik, M., Nouroozi, R., Krenn, M., and Zeilinger, A. (2017). High-dimensional single-photon quantum gates: concepts and experiments. *Physical Review Letters*, 119(18):180510.

[Bacco et al., 2016] Bacco, D., Christensen, J. B., Castaneda, M. A. U., Ding, Y., Forchhammer, S., Rottwitt, K., and Oxenløwe, L. K. (2016). Two-dimensional distributed-phase-reference protocol for quantum key distribution. *Scientific Reports*, 6(1):1–7.

[Bahadur et al., 2016] Bahadur, V., Selvakumar, D., Sobha, P. M., et al. (2016). Reconfigurable side channel attack resistant true random number generator. In *2016 International Conference on VLSI Systems, Architectures, Technology and Applications (VLSI-SATA)*, pages 1–6. IEEE.

[Bai et al., 2012] Bai, N., Ip, E., Huang, Y.-K., Mateo, E., Yaman, F., Li, M.-J., Bickham, S., Ten, S., Liñares, J., Montero, C., et al. (2012). Mode-division multiplexed transmission with inline few-mode fiber amplifier. *Optics Express*, 20(3):2668–2680.

[Balado et al., 2017] Balado, D., Prieto-Blanco, X., and Liñares, J. (2017). Spatial mode quantum cryptography in few-mode optical fibers. In *X Reunión Española de Optoelectrónica (OPTOEL 2017)*, Santiago de Compostela.

[Balado et al., 2018] Balado, D., Prieto-Blanco, X., Barral, D., and Liñares, J. (2018). Autocompensating high-dimensional quantum cryptography by using integrated photonic devices in multicore optical fiber spatial multiplexing systems. In *International Conference on Integrated Quantum Photonics (ICIQP 2018)*, volume 75.

[Balado et al., 2019] Balado, D., Liñares, J., Prieto-Blanco, X., and Barral, D. (2019). Phase and polarization autocompensating N-dimensional quantum cryptography in multicore optical fibers. *JOSA B*, 36(10):2793–2803.

[Balado Souto et al., 2016] Balado Souto, D., Liñares Beiras, J., Montero Orille, C., Moreno de las Cuevas, V., Moure Cerijo, D., Nistal Fernández, M. C., and Prieto Blanco, X. (2016). Generación de modos LP con placas de fase producidas por intercambio iónico en vidrio. In *XXXI Simposium Nacional de la Unión Cinetífica Internacional de Radio (URSI 2016)*, Madrid. Escuela Politécnica Superior Universidad Autónoma de Madrid.

[Balado Souto et al., 2019] Balado Souto, D., Liñares, J., and Prieto-Blanco, X. (2019). Phase auto-compensating high-dimensional quantum cryptography in elliptical-core few-mode fibres. *Journal of Modern Optics*, 66(9):947–957.

[Bandyopadhyay et al., 2011] Bandyopadhyay, A., Prabhakar, S., and Singh, R. P. (2011). Entanglement of a quantum optical elliptic vortex. *Physics Letters A*, 375(19):1926–1929.

[Bandyopadhyay and Singh, 2011] Bandyopadhyay, A. and Singh, R. P. (2011). Wigner distribution of elliptical quantum optical vortex. *Optics Communications*, 284(1):256–261.

[Banerji et al., 2014] Banerji, A., Singh, R. P., and Bandyopadhyay, A. (2014). Entanglement measure using wigner function: case of generalized vortex state formed by multiphoton subtraction. *Optics Communications*, 330:85–90.

[Barral et al., 2013] Barral, D., Liñares, J., and Nistal, M. C. (2013). Optical field-strength generalized polarization of non-stationary quantum states in waveguiding photonic devices. *Journal of Modern Optics*, 60(12):941–955.

[Barral et al., 2015] Barral, D., Thompson, M. G., and Liñares, J. (2015). Detection of two-mode spatial quantum states of light by electro-optic integrated directional couplers. *JOSA B*, 32(6):1165–1173.

[Barral and Liñares, 2015] Barral, D. and Liñares, J. (2015). Spatial propagation of quantum light states in longitudinally inhomogeneous waveguides. *JOSA B*, 32(9):1993–2002.

[Barral et al., 2016] Barral, D., Liñares, J., and Balado, D. (2016). Engineering continuous and discrete variable quantum vortex states by nonlocal photon subtraction in a reconfigurable photonic chip. *JOSA B*, 33(11):2225–2235.

[Barral and Liñares, 2016] Barral, D. and Liñares, J. (2016). Engineering continuous variable and coherent state bell-like states in a reconfigurable photonic chip. *IEEE Journal of Quantum Electronics*, 53(1):1–10.

[Barral and Liñares, 2017] Barral, D. and Liñares, J. (2017). Comment on "Generating a perfect quantum optical vortex". *Physical Review A*, 96(4):047802.

[Barral et al., 2017] Barral, D., Balado, D., and Liñares, J. (2017). Generation and detection of continuous variable quantum vortex states via compact photonic devices. *Photonics*, 4(1):2.

[Bechmann-Pasquinucci and Gisin, 1999] Bechmann-Pasquinucci, H. and Gisin, N. (1999). Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A*, 59(6):4238.

[Bedington et al., 2017] Bedington, R., Arrazola, J. M., and Ling, A. (2017). Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):1–13.

[Beijersbergen et al., 1993] Beijersbergen, M. W., Allen, L., Van der Veen, H. E. L. O., and Woerdman, J. P. (1993). Astigmatic laser mode converters and transfer of orbital angular momentum. *Optics Communications*, 96(1-3):123–132.

[Bell, 1964] Bell, J. S. (1964). On the Einstein-Podolsky-Rosen paradox. *Physics Physique Fizika*, 1(3):195.

[Ben-Aryeh and Serulnik, 1991] Ben-Aryeh, Y. and Serulnik, S. (1991). The quantum treatment of propagation in non-linear optical media by the use of temporal modes. *Physics Letters A*, 155(8-9):473–479.

[Bengtsson et al., 2007] Bengtsson, I., Bruzda, W., Ericsson, Å., Larsson, J.-Å., Tadej, W., and Życzkowski, K. (2007). Mutually unbiased bases and Hadamard matrices of order six. *Journal of Mathematical Physics*, 48(5):052106.

[Bengtsson, 2007] Bengtsson, I. (2007). Three ways to look at mutually unbiased bases. In *AIP Conference Proceedings*, volume 889, pages 40–51. American Institute of Physics.

[Bennett et al., 1983] Bennett, C. H., Brassard, G., Breidbart, S., and Wiesner, S. (1983). Quantum cryptography, or unforgeable subway tokens. In *Advances in Cryptology*, pages 267–275. Springer.

[Bennett and Brassard, 1984] Bennett, C. H. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179. IEEE New York.

[Bennett et al., 1988] Bennett, C. H., Brassard, G., and Robert, J.-M. (1988). Privacy amplification by public discussion. *SIAM journal on Computing*, 17(2):210–229.

[Bennett and Brassard, 1989] Bennett, C. H. and Brassard, G. (1989). Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. *ACM Sigact News*, 20(4):78–80.

[Bennett et al., 1992a] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J. (1992a). Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28.

[Bennett et al., 1992b] Bennett, C. H., Brassard, G., and Ekert, A. K. (1992b). Quantum cryptography. *Scientific American*, 267(4):50–57.

[Bennett, 1992] Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121.

[Bennett et al., 1993] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895.

[Bennett et al., 1995] Bennett, C. H., Brassard, G., Crépeau, C., and Maurer, U. M. (1995). Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923.

[Bennett et al., 1996] Bennett, C. H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J. A., and Wootters, W. K. (1996). Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76(5):722.

[Berry, 1987] Berry, M. V. (1987). Interpreting the anholonomy of coiled light. *Nature*, 326(6110):277–278.

[Bethune and Risk, 2000] Bethune, D. S. and Risk, W. P. (2000). An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light. *IEEE Journal of Quantum Electronics*, 36(3):340–347.

[Bethune and Risk, 2002] Bethune, D. S. and Risk, W. P. (2002). Autocompensating quantum cryptography. *New Journal of Physics*, 4(1):42.

[Bethune et al., 2002] Bethune, D. S., Navarro, M., and Risk, W. P. (2002). Enhanced autocompensating quantum cryptography system. *Applied Optics*, 41(9):1640–1648.

[Bohr, 1913] Bohr, N. (1913). I. On the constitution of atoms and molecules. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 26(151):1–25.

[Bonneau et al., 2012] Bonneau, D., Lobino, M., Jiang, P., Natarajan, C. M., Tanner, M. G., Hadfield, R. H., Dorenbos, S. N., Zwiller, V., Thompson, M. G., and O'Brien, J. L. (2012). Fast path and polarization manipulation of telecom wavelength single photons in lithium niobate waveguide devices. *Physical Review Letters*, 108(5):053601.

[Born and Wolf, 1999] Born, M. and Wolf, E. (1999). Principles of optics, 7th (expanded) edition. *United Kingdom: Press Syndicate of the University of Cambridge*, 461.

[Brandt et al., 2020] Brandt, F., Hiekkamäki, M., Bouchard, F., Huber, M., and Fickler, R. (2020). High-dimensional quantum gates using full-field spatial modes of photons. *Optica*, 7(2):98–107.

[Brassard, 2005] Brassard, G. (2005). Brief history of quantum cryptography: A personal perspective. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.*, pages 19–23. IEEE.

[Braunstein and Kimble, 1998] Braunstein, S. L. and Kimble, H. J. (1998). A posteriori teleportation. *Nature*, 394(6696):840–841.

[Braunstein and Van Loock, 2005] Braunstein, S. L. and Van Loock, P. (2005). Quantum information with continuous variables. *Reviews of Modern Physics*, 77(2):513.

[Brierley et al., 2009] Brierley, S., Weigert, S., and Bengtsson, I. (2009). All mutually unbiased bases in dimensions two to five. *arXiv preprint arXiv:0907.4097*.

[Brillouin, 1926] Brillouin, L. (1926). La mécanique ondulatoire de Schrödinger; une méthode générale de résolution par approximations successives. *Compt. Rend. Hebd. Seances Acad. Sci.*, 183:24–26.

[Brinkmeyer, 1981] Brinkmeyer, E. (1981). Forward-backward transmission in birefringent single-mode fibers: interpretation of polarization-sensitive measurements. *Optics Letters*, 6(11):575–577.

[Broglie, 1924] Broglie, L. d. (1924). XXXV. A tentative theory of light quanta. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 47(278):446–458.

[Bruß, 1998] Bruß, D. (1998). Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018.

[Bruß et al., 2000] Bruß, D., Cinchetti, M., D'Ariano, G. M., and Macchiavello, C. (2000). Phase-covariant quantum cloning. *Physical Review A*, 62(1):012302.

[Burnham and Weinberg, 1970] Burnham, D. C. and Weinberg, D. L. (1970). Observation of simultaneity in parametric production of optical photon pairs. *Physical Review Letters*, 25(2):84.

[Bussieres et al., 2006] Bussieres, F., Soudagar, Y., Berlin, G., Lacroix, S., and Godbout, N. (2006). Manipulating time-bin qubits with fiber optics components. In *2006 Digest of the LEOS Summer Topical Meetings*, pages 22–23. IEEE.

[Bužek and Hillery, 1996] Bužek, V. and Hillery, M. (1996). Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54(3):1844.

[Calkins et al., 2013] Calkins, B., Mennea, P. L., Lita, A. E., Metcalf, B. J., Kolthammer, W. S., Lamas-Linares, A., Spring, J. B., Humphreys, P. C., Mirin, R. P., Gates, J. C., et al. (2013). High quantum-efficiency photon-number-resolving detector for photonic on-chip information processing. *Optics Express*, 21(19):22657–22670.

[Campos et al., 1989] Campos, R. A., Saleh, B. E. A., and Teich, M. C. (1989). Quantum-mechanical lossless beam splitter: SU(2) symmetry and photon statistics. *Physical Review A*, 40(3):1371.

[Cañas et al., 2017] Cañas, G., Vera, N., Cariñe, J., González, P., Cardenas, J., Connolly, P. W. R., Przysiezna, A., Gómez, E., Figueroa, M., Vallone, G., et al. (2017). High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers. *Physical Review A*, 96(2):022317.

[Carolan et al., 2015] Carolan, J., Harrold, C., Sparrow, C., Martín-López, E., Russell, N. J., Silverstone, J. W., Shadbolt, P. J., Matsuda, N., Oguma, M., Itoh, M., et al. (2015). Universal linear optics. *Science*, 349(6249):711–716.

[Carré, 1966] Carré, P. (1966). Installation et utilisation du comparateur photoélectrique et interférentiel du Bureau International des Poids et Mesures. *Metrologia*, 2(1):13.

[Cerf, 2000] Cerf, N. J. (2000). Pauli cloning of a quantum bit. *Physical Review Letters*, 84(19):4497.

[Cerf et al., 2001] Cerf, N. J., Levy, M., and Van Assche, G. (2001). Quantum distribution of gaussian keys using squeezed states. *Physical Review A*, 63(5):052311.

[Cerf et al., 2002] Cerf, N. J., Bourennane, M., Karlsson, A., and Gisin, N. (2002). Security of quantum key distribution using d-level systems. *Physical Review Letters*, 88(12):127902.

[Chen et al., 2018] Chen, H., Meng, H., Liu, X., Ding, J., Jiang, J., Chen, G., and Hao, Y. (2018). Comparison of integrated optical phase shifters designed in different regime. In *MATEC Web of Conferences*, volume 173, page 01034. EDP Sciences.

[Chen et al., 2008] Chen, W., Han, Z., Mo, X., Xu, F., Wei, G., and Guo, G. (2008). Active phase compensation of quantum key distribution system. *Chinese Science Bulletin*, 53(9):1310–1314.

[Clements et al., 2016] Clements, W. R., Humphreys, P. C., Metcalf, B. J., Kolthammer, W. S., and Walmsley, I. A. (2016). Optimal design for universal multiport interferometers. *Optica*, 3(12):1460–1465.

[Cozzolino et al., 2019] Cozzolino, D., Bacco, D., Da Lio, B., Ingerslev, K., Ding, Y., Dalgaard, K., Kristensen, P., Galili, M., Rottwitt, K., Ramachandran, S., et al. (2019). Orbital angular momentum states enabling fiber-based high-dimensional quantum communication. *Physical Review Applied*, 11(6):064058.

[Creath, 1988] Creath, K. (1988). Phase-measurement interferometry techniques. *Progress in Optics*, 26(26):349–393.

[Csiszár and Korner, 1978] Csiszár, I. and Korner, J. (1978). Broadcast channels with confidential messages. *IEEE transactions on information theory*, 24(3):339–348.

[Curty et al., 2010] Curty, M., Ma, X., Qi, B., and Moroder, T. (2010). Passive decoy-state quantum key distribution with practical light sources. *Physical Review A*, 81(2):022310.

[Dakna et al., 1997] Dakna, M., Anhut, T., Opatrnỳ, T., Knöll, L., and Welsch, D.-G. (1997). Generating Schrödinger-cat-like states by means of conditional measurements on a beam splitter. *Physical Review A*, 55(4):3184.

[Day, 1976] Day, D. E. (1976). Mixed alkali glasses—their properties and uses. *Journal of Non-Crystalline Solids*, 21(3):343–372.

[de Guise et al., 2018] de Guise, H., Di Matteo, O., and Sánchez-Soto, L. L. (2018). Simple factorization of unitary transformations. *Physical Review A*, 97(2):022328.

[Deutsch et al., 1996] Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S., and Sanpera, A. (1996). Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Physical Review Letters*, 77(13):2818.

[Dieks, 1982] Dieks, D. G. B. J. (1982). Communication by epr devices. *Physics Letters A*, 92(6):271–272.

[Ding et al., 2017] Ding, Y., Bacco, D., Dalgaard, K., Cai, X., Zhou, X., Rottwitt, K., and Oxenløwe, L. K. (2017). High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Information*, 3(1):1–7.

[Donkor, 2012] Donkor, E. (2012). Experimental auto-compensating multi-user quantum key distribution network using a wavelength-addressed bus line architecture. In *Enabling Photonics Technologies for Defense, Security, and Aerospace Applications VIII*, volume 8397, page 839704. International Society for Optics and Photonics.

[Duplinskiy et al., 2019] Duplinskiy, A. V., Ustimchik, V. E., Kurochkin, Y. V., Kurochkin, V. L., and Miller, A. V. (2019). High-speed autocompensation scheme of quantum key distribution. US Patent 10,171,237.

[Dutt et al., 2015] Dutt, A., Luke, K., Manipatruni, S., Gaeta, A. L., Nussenzveig, P., and Lipson, M. (2015). On-chip optical squeezing. *Physical Review Applied*, 3(4):044005.

[Dynes et al., 2016] Dynes, J. F., Kindness, S. J., Tam, S. W. B., Plews, A., Sharpe, A. W., Lucamarini, M., Fröhlich, B., Yuan, Z. L., Penty, R. V., and Shields, A. J. (2016). Quantum key distribution over multicore fiber. *Optics Express*, 24(8):8081–8087.

[Eimerl, 1987] Eimerl, D. (1987). Electro-optic, linear, and nonlinear optical properties of KDP and its isomorphs. *Ferroelectrics*, 72(1):95–139.

[Einstein, 1905] Einstein, A. (1905). Über einem die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt. *Annalen der Physik*, 4.

[Einstein, 1917] Einstein, A. (1917). Zur quantentheorie der strahlung. *Phys. Z.*, 18:124.

[Einstein et al., 1935] Einstein, A., Podolsky, B., and Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777.

[Eisaman et al., 2011] Eisaman, M. D., Fan, J., Migdall, A., and Polyakov, S. V. (2011). Invited review article: Single-photon sources and detectors. *Review of Scientific Instruments*, 82(7):071101.

[Eisert et al., 2002] Eisert, J., Scheel, S., and Plenio, M. B. (2002). Distilling Gaussian states with Gaussian operations is impossible. *Physical Review Letters*, 89(13):137903.

[Ekert, 1991] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Retters*, 67(6):661.

[Eto et al., 2008] Eto, Y., Tajima, T., Zhang, Y., and Hirano, T. (2008). Observation of quadrature squeezing in a $\chi(2)$ nonlinear waveguide using a temporally shaped local oscillator pulse. *Optics Express*, 16(14):10650–10657.

[Eucalypt,] Eucalypt. image: Flaticon.com. https://www.flaticon.com/authors/eucalyp.

[Fearn and Loudon, 1987] Fearn, H. and Loudon, R. (1987). Quantum theory of the lossless beam splitter. *Optics Communications*, 64(6):485–490.

[Ferraro et al., 2005] Ferraro, A., Olivares, S., and Paris, M. G. A. (2005). *Gaussian states in quantum information*. Bibliopolis.

[Fickler et al., 2012] Fickler, R., Lapkiewicz, R., Plick, W. N., Krenn, M., Schaeff, C., Ramelow, S., and Zeilinger, A. (2012). Quantum entanglement of high angular momenta. *Science*, 338(6107):640–643.

[Findakly, 1985] Findakly, T. (1985). Glass waveguides by ion exchange: a review. *Optical Engineering*, 24(2):242244.

[Fiurášek, 2002] Fiurášek, J. (2002). Gaussian transformations and distillation of entangled Gaussian states. *Physical Review Letters*, 89(13):137904.

[Freedman and Clauser, 1972] Freedman, S. J. and Clauser, J. F. (1972). Experimental test of local hidden-variable theories. *Physical Review Letters*, 28(14):938.

[Fung et al., 2007] Fung, C.-H. F., Qi, B., Tamaki, K., and Lo, H.-K. (2007). Phase-remapping attack in practical quantum-key-distribution systems. *Physical Review A*, 75(3):032314.

[Furusawa, 2015] Furusawa, A. (2015). *Quantum States of Light*. Springer.

[Galindo and Pascual, 1989] Galindo, A. and Pascual, P. (1989). Mecánica Cuántica Vol. I y II. *Eudema Universidad*.

[Ganeev et al., 2004] Ganeev, R. A., Kulagin, I. A., Ryasnyansky, A. I., Tugushev, R. I., and Usmanov, T. (2004). Characterization of nonlinear optical parameters of KDP, LiNbO3 and BBO crystals. *Optics Communications*, 229(1-6):403–412.

[Gao et al., 2019] Gao, X., Krenn, M., Kysela, J., and Zeilinger, A. (2019). Arbitrary d-dimensional Pauli X Gates of a flying Qudit. *Physical Review A*, 99(2):023825.

[García-Patrón et al., 2004] García-Patrón, R., Fiurášek, J., Cerf, N. J., Wenger, J., Tualle-Brouri, R., and Grangier, P. (2004). Proposal for a loophole-free Bell test using homodyne detection. *Physical Review Letters*, 93(13):130409.

[García-Patrón and Cerf, 2009] García-Patrón, R. and Cerf, N. J. (2009). Continuous-variable quantum key distribution protocols over noisy channels. *Physical Review Letters*, 102(13):130501.

[Gerry et al., 2005] Gerry, C., Knight, P., and Knight, P. L. (2005). *Introductory Quantum Optics*. Cambridge University Press.

[Giedke and Cirac, 2002] Giedke, G. and Cirac, J. I. (2002). Characterization of Gaussian operations and distillation of Gaussian states. *Physical Review A*, 66(3):032316.

[Gisin et al., 2006] Gisin, N., Fasel, S., Kraus, B., Zbinden, H., and Ribordy, G. (2006). Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2):022320.

[Giuliano, 1981] Giuliano, C. R. (1981). Applications of optical phase conjugation. *Physics Today*, 34(4):27–35.

[Glatzel, 1980] Glatzel, E. (1980). New lenses for microlithography. In *1980 International Lens Design Conference*, volume 237, pages 310–320. International Society for Optics and Photonics.

[Glauber, 1963a] Glauber, R. J. (1963a). Coherent and incoherent states of the radiation field. *Physical Review*, 131(6):2766.

[Glauber, 1963b] Glauber, R. J. (1963b). Photon correlations. *Physical Review Letters*, 10(3):84.

[Glauber, 1963c] Glauber, R. J. (1963c). The quantum theory of optical coherence. *Physical Review*, 130(6):2529.

[González-Andrade et al., 2018] González-Andrade, D., Wangüemert-Pérez, J. G., Velasco, A. V., Ortega-Moñux, A., Herrero-Bermello, A., Molina-Fernández, I., Halir, R., and Cheben, P. (2018). Ultra-broadband mode converter and multiplexer based on sub-wavelength structures. *IEEE Photonics Journal*, 10(2):1–10.

[González-Andrade et al., 2020] González-Andrade, D., Luque-González, J. M., Wangüemert-Pérez, J. G., Ortega-Moñux, A., Cheben, P., Molina-Fernández, Í., and Velasco, A. V. (2020). Ultra-broadband nanophotonic phase shifter based on subwavelength metamaterial waveguides. *Photonics Research*, 8(3):359–367.

[Gottesman and Preskill, 2003] Gottesman, D. and Preskill, J. (2003). Secure quantum key distribution using squeezed states. In *Quantum Information with Continuous Variables*, pages 317–356. Springer.

[Gottesman et al., 2004] Gottesman, D., Lo, H.-K., Lutkenhaus, N., and Preskill, J. (2004). Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, page 136. IEEE.

[Griffiths and Niu, 1997] Griffiths, R. B. and Niu, C.-S. (1997). Optimal eavesdropping in quantum cryptography. II. A quantum circuit. *Physical Review A*, 56(2):1173.

[Grosshans et al., 2003] Grosshans, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N. J., and Grangier, P. (2003). Quantum key distribution using Gaussian-modulated coherent states. *Nature*, 421(6920):238–241.

[Hadfield, 2009] Hadfield, R. H. (2009). Single-photon detectors for optical quantum information applications. *Nature Photonics*, 3(12):696.

[Hammer and Ivanova, 2009] Hammer, M. and Ivanova, O. V. (2009). Effective index approximations of photonic crystal slabs: a 2-to-1-D assessment. *Optical and Quantum Electronics*, 41(4):267–283.

[Han et al., 2015] Han, L., Liang, S., Zhu, H., Qiao, L., Xu, J., and Wang, W. (2015). Two-mode de/multiplexer based on multimode interference couplers with a tilted joint as phase shifter. *Optics Letters*, 40(4):518–521.

[Harris et al., 2014] Harris, N. C., Ma, Y., Mower, J., Baehr-Jones, T., Englund, D., Hochberg, M., and Galland, C. (2014). Efficient, compact and low loss thermo-optic phase shifter in silicon. *Optics Express*, 22(9):10487–10493.

[Heisenberg, 1927] Heisenberg, W. (1927). Uber den anschaulichen Inhalt der quanten theoretischen Kinematik und Mechanik. *Zeit. für Phys.*, 43:172–198.

[Herrero-Bermello et al., 2017] Herrero-Bermello, A., Velasco, A. V., Podmore, H., Cheben, P., Schmid, J. H., Janz, S., Calvo, M. L., Xu, D.-X., Scott, A., and Corredera, P. (2017). Temperature dependence mitigation in stationary Fourier-transform on-chip spectrometers. *Optics Letters*, 42(11):2239–2242.

[Hibbs and Feynman, 1965] Hibbs, A. R. and Feynman, R. P. (1965). *Quantum Mechanics and Path Integrals*. McGraw-Hill Interamericana.

[Humphreys et al., 2014] Humphreys, P. C., Metcalf, B. J., Spring, J. B., Moore, M., Salter, P. S., Booth, M. J., Kolthammer, W. S., and Walmsley, I. A. (2014). Strain-optic active control for quantum integrated photonics. *Optics Express*, 22(18):21719–21726.

[Huttner et al., 1990] Huttner, B., Serulnik, S., and Ben-Aryeh, Y. (1990). Quantum analysis of light propagation in a parametric amplifier. *Physical Review A*, 42(9):5594.

[Huttner et al., 1995] Huttner, B., Imoto, N., Gisin, N., and Mor, T. (1995). Quantum cryptography with coherent states. *Physical Review A*, 51(3):1863.

[Hwang, 2003] Hwang, W.-Y. (2003). Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters*, 91(5):057901.

[Ikeda et al., 2010] Ikeda, T., Takahashi, K., Kanamori, Y., and Hane, K. (2010). Phase-shifter using submicron silicon waveguide couplers with ultra-small electro-mechanical actuator. *Optics Express*, 18(7):7031–7037.

[Ip et al., 2015] Ip, E., Milione, G., Li, M.-J., Cvijetic, N., Kanonakis, K., Stone, J., Peng, G., Prieto, X., Montero, C., Moreno, V., et al. (2015). SDM transmission of real-time 10 GbE traffic using commercial SFP+ transceivers over 0.5 km elliptical-core few-mode fiber. *Optics Express*, 23(13):17120–17126.

[Isard, 1969] Isard, J. O. (1969). The mixed alkali effect in glass. *Journal of Non-Crystalline Solids*, 1(3):235–261.

[Islam et al., 2017] Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J., and Gauthier, D. J. (2017). Provably secure and high-rate quantum key distribution with time-bin qudits. *Science advances*, 3(11):e1701491.

[Ittner, 1977] Ittner, G. (1977). Future possibilities of dioptric lenses in microelectronics. In *Developments in Semiconductor Microlithography II*, volume 100, pages 115–119. International Society for Optics and Photonics.

[Jacobs and Franson, 1996] Jacobs, B. C. and Franson, J. D. (1996). Quantum cryptography in free space. *Optics Letters*, 21(22):1854–1856.

[Jaeger, 2002] Jaeger, R. C. (2002). *Introduction to microelectronic fabrication*, volume 2. Prentice Hall Upper Saddle River, NJ.

[Jain et al., 2014] Jain, N., Anisimova, E., Khan, I., Makarov, V., Marquardt, C., and Leuchs, G. (2014). Trojan-horse attacks threaten the security of practical quantum cryptography. *New Journal of Physics*, 16(12):123030.

[Jeong et al., 2001] Jeong, H., Kim, M. S., and Lee, J. (2001). Quantum-information processing for a coherent superposition state via a mixedentangled coherent channel. *Physical Review A*, 64(5):052308.

[Jin et al., 2020] Jin, D., Guo, Y., Wang, Y., and Huang, D. (2020). Parameter estimation of orbital angular momentum based continuous-variable quantum key distribution. *Journal of Applied Physics*, 127(21):213102.

[Jin et al., 2014] Jin, H., Liu, F., Xu, P., Xia, J., Zhong, M., Yuan, Y., Zhou, J. W., Gong, Y. X., Wang, W., and Zhu, S. (2014). On-chip generation and manipulation of entangled photons based on reconfigurable lithium-niobate waveguide circuits. *Physical Review Letters*, 113(10):103601.

[Kaiser et al., 2016] Kaiser, F., Fedrici, B., Zavatta, A., D'Auria, V., and Tanzilli, S. (2016). A fully guided-wave squeezing experiment for fiber quantum networks. *Optica*, 3(4):362–365.

[Kak, 2006] Kak, S. (2006). A three-stage quantum cryptography protocol. *Foundations of Physics Letters*, 19(3):293–296.

[Kanter et al., 2002] Kanter, G. S., Kumar, P., Roussev, R. V., Kurz, J., Parameswaran, K. R., and Fejer, M. M. (2002). Squeezing in a LiNbO 3 integrated optical waveguide circuit. *Optics Express*, 10(3):177–182.

[Kim et al., 2002] Kim, M. S., Son, W., Bužek, V., and Knight, P. L. (2002). Entanglement by a beam splitter: Nonclassicality as a prerequisite for entanglement. *Physical Review A*, 65(3):032323.

[Kim, 2008] Kim, M. S. (2008). Recent developments in photon-level operations on travelling light fields. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 41(13):133001.

[Kim et al., 2008] Kim, M. S., Jeong, H., Zavatta, A., Parigi, V., and Bellini, M. (2008). Scheme for proving the bosonic commutation relation using single-photon interference. *Physical Review Letters*, 101(26):260401.

[Kim et al., 2014] Kim, Y., Takenaka, M., Osada, T., Hata, M., and Takagi, S. (2014). Strain-induced enhancement of plasma dispersion effect and free-carrier absorption in sige optical modulators. *Scientific reports*, 4:4683.

[Klappenecker and Rötteler, 2003] Klappenecker, A. and Rötteler, M. (2003). Constructions of mutually unbiased bases. In *International Conference on Finite Fields and Applications*, pages 137–144. Springer.

[Klyshko et al., 1970] Klyshko, D. N., Penin, A. N., and Polkovnikov, B. F. (1970). Parametric luminescence and light scattering by polaritons. *Soviet Journal of Experimental and Theoretical Physics Letters*, 11:5.

[Korolkova et al., 2002] Korolkova, N., Leuchs, G., Loudon, R., Ralph, T. C., and Silberhorn, C. (2002). Polarization squeezing and continuous-variable polarization entanglement. *Physical Review A*, 65(5):052306.

[Kramers, 1926] Kramers, H. A. (1926). Wellenmechanik und halbzahlige Quantisierung. *Zeitschrift für Physik*, 39(10-11):828–840.

[Krapick et al., 2013] Krapick, S., Herrmann, H., Quiring, V., Brecht, B., Suche, H., and Silberhorn, C. (2013). An efficient integrated two-color source for heralded single photons. *New Journal of Physics*, 15(3):033010.

[Landauer, 1961] Landauer, R. (1961). Irreversibility and heat generation in the computing process. *IBM journal of research and development*, 5(3):183–191.

[Leach et al., 2002] Leach, J., Padgett, M. J., Barnett, S. M., Franke-Arnold, S., and Courtial, J. (2002). Measuring the orbital angular momentum of a single photon. *Physical Review Letters*, 88(25):257901.

[Leach et al., 2012] Leach, J., Bolduc, E., Gauthier, D. J., and Boyd, R. W. (2012). Secure information capacity of photons entangled in many dimensions. *Physical Review A*, 85(6):060304.

[Lee et al., 2011] Lee, N., Benichi, H., Takeno, Y., Takeda, S., Webb, J., Huntington, E., and Furusawa, A. (2011). Teleportation of nonclassical wave packets of light. *Science*, 332(6027):330–333.

[Leonhardt, 1997] Leonhardt, U. (1997). *Measuring the Quantum State of Light*, volume 22. Cambridge university press.

[Levinson, 2005] Levinson, H. J. (2005). *Principles of Lithography*, volume 146. SPIE press.

[Li et al., 2015] Li, Y.-Z., Jia, F., Zhang, H.-L., Huang, J.-H., and Hu, L.-Y. (2015). Hermite polynomial excited squeezed vacuum as quantum optical vortex states. *Laser Physics Letters*, 12(11):115203.

[Liao et al., 2017] Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., et al. (2017). Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47.

[Liñares et al., 1994] Liñares, J., Prieto, X., and Montero, C. (1994). A novel refractive index profile for optical characterization of non-linear diffusion processes and planar waveguides in glass. *Optical Materials*, 3(4):229–236.

[Liñares et al., 2000] Liñares, J., Montero, C., Moreno, V., Nistal, M. C., Prieto, X., Salgueiro, J. R., and Sotelo, D. (2000). Glass processing by ion exchange to fabricate integrated optical planar components: applications. In *Integrated Optics Devices IV*, volume 3936, pages 227–238. International Society for Optics and Photonics.

[Liñares et al., 2001] Liñares, J., Moreno, V., Nistal, M. C., and Salgueiro, J. R. (2001). Modelling of ion-exchanged monomode channel guides with quasi-exact modal solutions by the effective index method. *Journal of Modern Optics*, 48(5):789–795.

[Liñares and Nistal, 2003] Liñares, J. and Nistal, M. C. (2003). Quantization of coupled modes propagation in integrated optical waveguides. *Journal of Modern Optics*, 50(5):781–790.

[Liñares et al., 2008] Liñares, J., Nistal, M. C., and Barral, D. (2008). Quantization of coupled 1D vector modes in integrated photonic waveguides. *New Journal of Physics*, 10(6):063023.

[Liñares and Nistal, 2009] Liñares, J. and Nistal, M. C. (2009). Spin operator for quantum light in integrated photonic waveguides. *Journal of Modern Optics*, 56(11):1244–1254.

[Liñares et al., 2011] Liñares, J., Barral, D., Nistal, M. C., and Moreno, V. (2011). Optical field-strength generalized polarization of multimode single photon states in integrated directional couplers. *Journal of Modern Optics*, 58(8):711–725.

[Liñares et al., 2012] Liñares, J., Barral, D., and Nistal, M. C. (2012). Spatial propagation of quantum light in non-linear waveguiding devices: theory and applications. *Journal of Nonlinear Optical Physics & Materials*, 21(03):1250032.

[Liñares et al., 2017a] Liñares, J., Prieto-Blanco, X., Moreno, V., Montero-Orille, C., Mouriz, D., Nistal, M. C., and Barral, D. (2017a). Interferometric space-mode multiplexing based on binary phase plates and refractive phase shifters. *Optics Express*, 25(10):10925–10938.

[Liñares et al., 2017b] Liñares, J., Montero-Orille, C., Moreno, V., Mouriz, D., Nistal, M. C., and Prieto-Blanco, X. (2017b). Ion-exchanged binary phase plates for mode multiplexing in graded-index optical fibers. *Applied Optics*, 56(25):7099–7106.

[Liñares et al., 2017c] Liñares, J., Prieto-Blanco, X., Montero-Orille, C., and Moreno, V. (2017c). Spatial mode multiplexing/demultiplexing by Gouy phase interferometry. *Optics Letters*, 42(1):93–96.

[Liñares et al., 2020] Liñares, J., Prieto-Blanco, X., Balado, D., and Carral, G. M. (2020). Fully autocompensating high-dimensional quantum cryptography by optical phase conjugation. *ArXiv preprint arXiv:2009.13915*.

[Liñares Beiras et al., 2011] Liñares Beiras, J., Nistal Fernández, M. C., Barral Raña, D., Moreno de las Cuevas, V., Montero Orille, C., and Prieto Blanco, X. (2011). Quantum integrated optics: Theory and applications. *Optica pura y aplicada*, 44(2):241–253.

[Liñares-Beiras et al., 2020] Liñares-Beiras, J., Prieto-Blanco, X., Balado, D., and Carral, G. M. (2020). Autocompensating high-dimensional quantum cryptography by phase conjugation in optical fibers. In *EPJ Web of Conferences*, volume 238, page 11004. EDP Sciences.

[Liu et al., 2013] Liu, Y., Chen, T.-Y., Wang, L.-J., Liang, H., Shentu, G.-L., Wang, J., Cui, K., Yin, H.-L., Liu, N.-L., Li, L., et al. (2013). Experimental measurement-device-independent quantum key distribution. *Physical Review Letters*, 111(13):130502.

[Liu et al., 2018] Liu, Y., Yang, Z., Zhao, J., Zhang, L., Li, Z., and Li, G. (2018). Intrinsic loss of few-mode fibers. *Optics Express*, 26(2):2107–2116.

[Lo and Chau, 1999] Lo, H.-K. and Chau, H. F. (1999). Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056.

[Lo and Zhao, 2008] Lo, H.-K. and Zhao, Y. (2008). Quantum cryptography. *arXiv preprint arXiv:0803.2507*.

[Lo et al., 2012] Lo, H.-K., Curty, M., and Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13):130503.

[Lugani et al., 2011] Lugani, J., Ghosh, S., and Thyagarajan, K. (2011). Generation of modal-and path-entangled photons using a domain-engineered integrated optical waveguide device. *Physical Review A*, 83(6):062333.

[Luis and Sanz, 2013] Luis, A. and Sanz, Á. S. (2013). Reconciling quantum trajectories and stationary quantum distributions in single-photon polarization states. *Physical Review A*, 87(6):063844.

[Luis and Sanz, 2015] Luis, A. and Sanz, Á. S. (2015). Nonclassical polarization dynamics in classical-like states. *Physical Review A*, 92(2):023832.

[Lund and Ralph, 2005] Lund, A. P. and Ralph, T. C. (2005). Coherent-state linear optical quantum computing gates using simplified diagonal superposition resource states. *Physical Review A*, 71(3):032305.

[Lütkenhaus, 2000] Lütkenhaus, N. (2000). Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5):052304.

[Lütkenhaus and Jahma, 2002] Lütkenhaus, N. and Jahma, M. (2002). Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4(1):44.

[Ma et al., 2007] Ma, H.-Q., Zhao, J.-L., and Wu, L.-A. (2007). Quantum key distribution based on phase encoding and polarization measurement. *Optics Letters*, 32(6):698–700.

[Ma et al., 2005] Ma, X., Qi, B., Zhao, Y., and Lo, H.-K. (2005). Practical decoy state for quantum key distribution. *Physical Review A*, 72(1):012326.

[Ma, 2008] Ma, X. (2008). Quantum cryptography: theory and practice. *arXiv preprint arXiv:0808.1385*.

[Mafu et al., 2013] Mafu, M., Dudley, A., Goyal, S., Giovannini, D., McLaren, M., Padgett, M. J., Konrad, T., Petruccione, F., Lütkenhaus, N., and Forbes, A. (2013). Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Physical Review A*, 88(3):032305.

[Makarov et al., 2006] Makarov, V., Anisimov, A., and Skaar, J. (2006). Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2):022313.

[Makarov and Skaar, 2007] Makarov, V. and Skaar, J. (2007). Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *arXiv preprint quant-ph/0702262*.

[Mandel and Wolf, 1995] Mandel, L. and Wolf, E. (1995). *Optical Coherence and Quantum Optics*. Cambridge University Press.

[Mao et al., 2013] Mao, D., Liu, X., Sun, Z., Lu, H., Han, D., Wang, G., and Wang, F. (2013). Flexible high-repetition-rate ultrafast fiber laser. *Scientific Reports*, 3:3223.

[Marand and Townsend, 1995] Marand, C. and Townsend, P. D. (1995). Quantum key distribution over distances as long as 30 km. *Optics Letters*, 20(16):1695–1697.

[Marchildon and Helmy, 2016] Marchildon, R. P. and Helmy, A. S. (2016). Dispersion-enabled quantum state control in integrated photonics. *Optica*, 3(3):243–251.

[Marquez et al., 1995] Marquez, H., Salazar, D., Villalobos, A., Paez, G., and Rincón, J. M. (1995). Experimental study of Cuˆ+–Naˆ+ exchanged glass waveguides. *Applied Optics*, 34(25):5817–5822.

[Martin et al., 2012] Martin, A., Alibart, O., De Micheli, M. P., Ostrowsky, D. B., and Tanzilli, S. (2012). A quantum relay chip based on telecommunication integrated optics technology. *New Journal of Physics*, 14(2):025002.

[Martinelli, 1989] Martinelli, M. (1989). A universal compensator for polarization changes induced by birefringence on a retracing beam. *Optics Communications*, 72(6):341–344.

[Masada et al., 2015] Masada, G., Miyata, K., Politi, A., Hashimoto, T., O'brien, J. L., and Furusawa, A. (2015). Continuous-variable entanglement on a chip. *Nature Photonics*, 9(5):316–319.

[Maslennikov et al., 2003] Maslennikov, G. A., Zhukov, A. A., Chekhova, M. V., and Kulik, S. (2003). Practical realization of a quantum cryptography protocol exploiting polarization encoding in qutrits. *Journal of Optics B: Quantum and Semiclassical Optics*, 5:S530–S534.

[Mattioli et al., 2015] Mattioli, F., Zhou, Z., Gaggero, A., Gaudio, R., Jahanmirinejad, S., Sahin, D., Marsili, F., Leoni, R., and Fiore, A. (2015). Photon-number-resolving superconducting nanowire detectors. *Superconductor Science and Technology*, 28(10):104001.

[Mayers, 2001] Mayers, D. (2001). Unconditional security in quantum cryptography. *Journal of the ACM (JACM)*, 48(3):351–406.

[Metricon-Corporation,] Metricon-Corporation. http://www.metricon.com/.

[Milione et al., 2016a] Milione, G., Ip, E., Li, M.-J., Stone, J., Peng, G., and Wang, T. (2016a). Mode crosstalk matrix measurement of a 1 km elliptical core few-mode optical fiber. *Optics Letters*, 41(12):2755–2758.

[Milione et al., 2016b] Milione, G., Ip, E., Li, M.-J., Stone, J., Peng, G., and Wang, T. (2016b). Spatial mode analysis of an elliptical-core, few-mode, optical fiber for mimoless space-division-multiplexing. In *2016 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3. IEEE.

[Milione et al., 2017] Milione, G., Ip, E., Ji, P., Huang, Y.-K., Wang, T., Li, M.-J., Stone, J., and Peng, G. (2017). MIMO-less space division multiplexing with elliptical core optical fibers. In *Optical Fiber Communication Conference*, pages Tu2J–1. Optical Society of America.

[Minář et al., 2008] Minář, J., De Riedmatten, H., Simon, C., Zbinden, H., and Gisin, N. (2008). Phase-noise measurements in long-fiber interferometers for quantum-repeater applications. *Physical Review A*, 77(5):052325.

[Molina-Terriza et al., 2007] Molina-Terriza, G., Torres, J. P., and Torner, L. (2007). Twisted photons. *Nature physics*, 3(5):305–310.

[Monat et al., 2006] Monat, C., Alloing, B., Zinoni, C., Li, L. H., and Fiore, A. (2006). Nanostructured current-confined single quantum dot light-emitting diode at 1300 nm. *Nano Letters*, 6(7):1464–1467.

[Montero-Orille et al., 2013] Montero-Orille, C., Moreno, V., Prieto-Blanco, X., Mateo, E. F., Ip, E., Crespo, J., and Liñares, J. (2013). Ion-exchanged glass binary phase plates for mode-division multiplexing. *Applied optics*, 52(11):2332–2339.

[Montero-Orille et al., 2020] Montero-Orille, C., González-Núñez, H., Prieto-Blanco, X., Moreno, V., Mouriz, D., Nistal, M. C., and Liñares, J. (2020). Optimising zero-order suppression in ion-exchanged phase gratings. In *EPJ Web of Conferences*, volume 238, page 03006. EDP Sciences.

[Morrissey and Peters, 2015] Morrissey, P. E. and Peters, F. H. (2015). Multimode interference couplers as compact and robust static optical phase shifters. *Optics Communications*, 345:1–5.

[Muller et al., 1993] Muller, A., Breguet, J., and Gisin, N. (1993). Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km. *EPL (Europhysics Letters)*, 23(6):383.

[Muller et al., 1995] Muller, A., Zbinden, H., and Gisin, N. (1995). Underwater quantum coding. *Nature*, 378(6556):449–449.

[Muller et al., 1996] Muller, A., Zbinden, H., and Gisin, N. (1996). Quantum cryptography over 23 km in installed under-lake telecom fibre. *EPL (Europhysics Letters)*, 33(5):335.

[Muller et al., 1997] Muller, A., Herzog, T., Huttner, B., Tittel, W., Zbinden, H., and Gisin, N. (1997). "Plug and play" systems for quantum cryptography. *Applied Physics Letters*, 70(7):793–795.

[Munhoz et al., 2008] Munhoz, P. P., Semiao, F. L., Vidiella-Barranco, A., and Roversi, J. A. (2008). Cluster-type entangled coherent states. *Physics Letters A*, 372(20):3580–3585.

[Najafi et al., 2015] Najafi, F., Mower, J., Harris, N. C., Bellei, F., Dane, A., Lee, C., Hu, X., Kharel, P., Marsili, F., Assefa, S., et al. (2015). On-chip detection of non-classical light by scalable integration of single-photon detectors. *Nature Communications*, 6(1):1–8.

[Najafi, 1992] Najafi, S. I. (1992). *Introduction to Glass Integrated Optics*. Artech House.

[Namekata et al., 2010] Namekata, N., Takahashi, Y., Fujii, G., Fukuda, D., Kurimura, S., and Inoue, S. (2010). Non-Gaussian operation based on photon subtraction using a photon-number-resolving detector at a telecommunications wavelength. *Nature Photonics*, 4(9):655.

[Neergaard-Nielsen et al., 2006] Neergaard-Nielsen, J. S., Nielsen, B. M., Hettich, C., Mølmer, K., and Polzik, E. S. (2006). Generation of a superposition of odd photon number states for quantum information networks. *Physical Review Letters*, 97(8):083604.

[Neergaard-Nielsen, 2008] Neergaard-Nielsen, J. S. (2008). *Generation of single photons and Schrödinger kitten states of light*. PhD thesis, University of Copenhagen, 2008. http://www. nbi. ku. dk ....

[Neergaard-Nielsen et al., 2010] Neergaard-Nielsen, J. S., Takeuchi, M., Wakui, K., Takahashi, H., Hayasaka, K., Takeoka, M., and Sasaki, M. (2010). Optical continuous-variable qubit. *Physical Review Letters*, 105(5):053602.

[Nha and Carmichael, 2004] Nha, H. and Carmichael, H. J. (2004). Proposed test of quantum nonlocality for continuous variables. *Physical Review Letters*, 93(2):020401.

[Nielsen and Chuang, 2002] Nielsen, M. A. and Chuang, I. (2002). *Quantum Computation and Quantum Information*. American Association of Physics Teachers.

[Nieto, 1997] Nieto, M. M. (1997). Displaced and squeezed number states. *Physics Letters A*, 229(3):135–143.

[Nikogosyan, 1991] Nikogosyan, D. N. (1991). Beta barium borate (BBO). *Applied Physics A*, 52(6):359–368.

[Niu and Griffiths, 1999] Niu, C.-S. and Griffiths, R. B. (1999). Two-qubit copying machine for economical quantum eavesdropping. *Physical Review A*, 60(4):2764.

[Niu et al., 2016] Niu, M. Y., Xu, F., Shapiro, J. H., and Furrer, F. (2016). Finite-key analysis for time-energy high-dimensional quantum key distribution. *Physical Review A*, 94(5):052323.

[O'brien et al., 2009] O'brien, J. L., Furusawa, A., and Vučković, J. (2009). Photonic quantum technologies. *Nature Photonics*, 3(12):687–695.

[Ohliger et al., 2010] Ohliger, M., Kieling, K., and Eisert, J. (2010). Limitations of quantum computing with Gaussian cluster states. *Physical Review A*, 82(4):042336.

[Ourjoumtsev et al., 2007a] Ourjoumtsev, A., Jeong, H., Tualle-Brouri, R., and Grangier, P. (2007a). Generation of optical 'schrödinger cats' from photon number states. *Nature*, 448(7155):784–786.

[Ourjoumtsev et al., 2007b] Ourjoumtsev, A., Dantan, A., Tualle-Brouri, R., and Grangier, P. (2007b). Increasing entanglement between gaussian states by coherent photon subtraction. *Physical Review Letters*, 98(3):030502.

[Ourjoumtsev et al., 2009] Ourjoumtsev, A., Ferreyrol, F., Tualle-Brouri, R., and Grangier, P. (2009). Preparation of non-local superpositions of quasi-classical light states. *Nature Physics*, 5(3):189–192.

[Pantchev and Danesh, 1997] Pantchev, B. and Danesh, P. (1997). Masking problem in the fabrication of optical waveguide structures in glass by double ion exchange. *Japanese Journal of Applied Physics*, 36(7R):4320.

[Parmigiani et al., 2017] Parmigiani, F., Jung, Y., Grüner-Nielsen, L., Geisler, T., Petropoulos, P., and Richardson, D. (2017). MIMO-less space division multiplexing transmission over 1 km elliptical core few mode fiber. In *CLEO: Science and Innovations*, pages SW1I–1. Optical Society of America.

[Pepper et al., 1978] Pepper, D. M., Fekete, D., and Yariv, A. (1978). Observation of amplified phase-conjugate reflection and optical parametric oscillation by degenerate four-wave mixing in a transparent medium. *Applied Physics Letters*, 33(1):41–44.

[Phillips, 1998] Phillips, W. D. (1998). Nobel lecture: Laser cooling and trapping of neutral atoms. *Reviews of Modern Physics*, 70(3):721.

[Planck, 1900a] Planck, M. (1900a). Zur Theorie des Gesetzes der Energieverteilung im Normalspektrum. *Verhandlungen der Deutschen Physikalischen Gesellschaft*, 2:238.

[Planck, 1900b] Planck, M. K. E. L. (1900b). Über eine Verbesserung der Wienschen Spectralgleichung. *Verhandlungen der Deutschen Physikalischen Gesellschaft*, 2:202.

[Pluta, 1988] Pluta, M. (1988). *Advanced Light Microscopy*, volume 1. Elsevier Amsterdam.

[Pluta, 1994] Pluta, M. (1994). Nomarski's DIC microscopy: a review. In *Phase Contrast and Differential Interference Contrast Imaging Techniques and Applications*, volume 1846, pages 10–25. International Society for Optics and Photonics.

[Politi et al., 2008] Politi, A., Cryan, M. J., Rarity, J. G., Yu, S., and O'brien, J. L. (2008). Silica-on-silicon waveguide quantum circuits. *Science*, 320(5876):646–649.

[Poot and Tang, 2014] Poot, M. and Tang, H. X. (2014). Broadband nanoelectromechanical phase shifting of light on a chip. *Applied Physics Letters*, 104(6):061101.

[Pratap Singh et al., 2006] Pratap Singh, R., Roychowdhury, S., and Kumar Jaiswal, V. (2006). Wigner distribution of an optical vortex. *Journal of Modern Optics*, 53(12):1803–1808.

[Prieto and Liñares, 1998] Prieto, X. and Liñares, J. (1998). Reflective integrated optical elements produced by ion exchange in glass. *Applied Optics*, 37(27):6375–6380.

[Prieto-Blanco, 2006] Prieto-Blanco, X. (2006). Interferometric characterization and analysis of silver-exchanged glass waveguides buried by electromigration: slab, channel and slab-sided channel configurations. *Journal of Optics A: Pure and Applied Optics*, 8(2):123.

[Prieto-Blanco, 2008] Prieto-Blanco, X. (2008). Electro-diffusion equations of monovalent cations in glass under charge neutrality approximation for optical waveguide fabrication. *Optical Materials*, 31(2):418–428.

[Prieto Blanco, 2016] Prieto Blanco, X. (2016). *Guías ópticas integradas fabricadas por intercambio iónico en vidro mediante difusión asistida por campo eléctrico con efecto ión mixto*. PhD thesis, Universidade de Santiago de Compostela.

[Pulker, 1984] Pulker, H. K. (1984). Thin Film Science and Technology. *Coatings on Glass*, 6:391.

[Ramirez et al., 2015] Ramirez, L. P., Hanna, M., Bouwmans, G., El Hamzaoui, H., Bouazaoui, M., Labat, D., Delplace, K., Pouysegur, J., Guichard, F., Rigaud, P., et al. (2015). Coherent beam combining with an ultrafast multicore Yb-doped fiber amplifier. *Optics Express*, 23(5):5406–5416.

[Reck et al., 1994] Reck, M., Zeilinger, A., Bernstein, H. J., and Bertani, P. (1994). Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73(1):58.

[Ribordy et al., 2000] Ribordy, G., Brendel, J., Gautier, J.-D., Gisin, N., and Zbinden, H. (2000). Long-distance entanglement-based quantum key distribution. *Physical Review A*, 63(1):012309.

[Ribordy, 2006] Ribordy, G. (2006). Practical quantum key distribution systems based on faint laser pulses. In *2006 Digest of the LEOS Summer Topical Meetings*, pages 28–29. IEEE.

[Richardson et al., 2013] Richardson, D. J., Fini, J. M., and Nelson, L. E. (2013). Space-division multiplexing in optical fibres. *Nature Photonics*, 7(5):354–362.

[Rogers et al., 2015] Rogers, S., Lu, X., Jiang, W. C., and Lin, Q. (2015). Twin photon pairs in a high-Q silicon microresonator. *Applied Physics Letters*, 107(4):041102.

[Sahin et al., 2014] Sahin, D., Gaggero, A., Weber, J.-W., Agafonov, I., Verheijen, M. A., Mattioli, F., Beetz, J., Kamp, M., Höfling, S., van de Sanden, M. C., et al. (2014). Waveguide nanowire superconducting single-photon detectors fabricated on gaas and the study of their optical properties. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(2):1–10.

[Saleh et al., 2009] Saleh, M. F., Saleh, B. E., and Teich, M. C. (2009). Modal, spectral, and polarization entanglement in guided-wave parametric down-conversion. *Physical Review A*, 79(5):053842.

[Salgueiro et al., 1998] Salgueiro, J. R., Roman, J. F., and de las Cuevas, V. M. (1998). System for laser writing to lithograph masks for integrated optics. *Optical Engineering*, 37(4):1115–1123.

[Salgueiro-Piñeiro, 2001] Salgueiro-Piñeiro, J. R. (2001). *Diseño de dispositivos ópticos de modo separable y desarrollo de tecnologías de litografía láser para su integración*. PhD thesis, Universidade de Santiago de Compostela.

[Sammut and Pask, 1991] Sammut, R. A. and Pask, C. (1991). Gaussian and equivalent-step-index approximations for nonlinear waveguides. *JOSA B*, 8(2):395–402.

[Schlederer et al., 2016] Schlederer, F., Krenn, M., Fickler, R., Malik, M., and Zeilinger, A. (2016). Cyclic transformation of orbital angular momentum modes. *New Journal of Physics*, 18(4):043019.

[Schleich, 2001] Schleich, W. P. (2001). *Quantum Optics in Phase Space*. VCH Verlag.

[Schneider-Kreuznach,] Schneider-Kreuznach. Xenon-sapphire 4.5/95. https://schneiderkreuznach.com/application/files/7815/8495/1960/Xenon-Sapphire˙4.5˙95˙1068013˙datasheet.pdf.

[Scully and Suhail, 1997] Scully, M. O. and Suhail, M. (1997). *Zubairy: Quantum Optics*. Cambridge: Cambridge University Press.

[Seshadreesan et al., 2015] Seshadreesan, K. P., Dowling, J. P., and Agarwal, G. S. (2015). Non-Gaussian entangled states and quantum teleportation of Schrödinger-cat states. *Physica Scripta*, 90(7):074029.

[Setzpfandt et al., 2016] Setzpfandt, F., Solntsev, A. S., Titchener, J., Wu, C. W., Xiong, C., Schiek, R., Pertsch, T., Neshev, D. N., and Sukhorukov, A. A. (2016). Tunable generation of entangled photons in a nonlinear directional coupler. *Laser & Photonics Reviews*, 10(1):131–136.

[Shadbolt et al., 2012] Shadbolt, P. J., Verde, M. R., Peruzzo, A., Politi, A., Laing, A., Lobino, M., Matthews, J. C. F., Thompson, M. G., and O'Brien, J. L. (2012). Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit. *Nature Photonics*, 6(1):45.

[Shan, 2010] Shan, K. S. (2010). *Quantitative Phase Imaging and Reconstruction For Biological Applications*. PhD thesis.

[Shannon, 1948] Shannon, C. E. (1948). A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423.

[Sheridan and Scarani, 2010] Sheridan, L. and Scarani, V. (2010). Security proof for quantum key distribution using qudit systems. *Physical Review A*, 82(3):030301.

[Shor and Preskill, 2000] Shor, P. W. and Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441.

[Silberhorn, 2007] Silberhorn, C. (2007). Detecting quantum light. *Contemporary Physics*, 48(3):143–156.

[Sit et al., 2017] Sit, A., Bouchard, F., Fickler, R., Gagnon-Bischoff, J., Larocque, H., Heshami, K., Elser, D., Peuntinger, C., Günthner, K., Heim, B., et al. (2017). High-dimensional intracity quantum cryptography with structured photons. *Optica*, 4(9):1006–1010.

[Slusher et al., 1985] Slusher, R., Hollberg, L., Yurke, B., Mertz, J., and Valley, J. (1985). Observation of squeezed states generated by four-wave mixing in an optical cavity. *Physical Review Letters*, 55(22):2409.

[Slusher et al., 1987] Slusher, R. E., Yurke, B., Grangier, P., LaPorta, A., Walls, D. F., and Reid, M. (1987). Squeezed-light generation by four-wave mixing near an atomic resonance. *JOSA B*, 4(10):1453–1464.

[Sochacka et al., 1994] Sochacka, M., Lago, E. L., and Jaroszewicz, Z. (1994). Refractive-index profiling of planar gradient-index waveguides by phase-measuring microinterferometry. *Applied Optics*, 33(16):3342–3347.

[Soref and Bennett, 1987] Soref, R. and Bennett, B. (1987). Electrooptical effects in silicon. *IEEE journal of quantum electronics*, 23(1):123–129.

[Stucki et al., 2002] Stucki, D., Gisin, N., Guinnard, O., Ribordy, G., and Zbinden, H. (2002). Quantum key distribution over 67 km with a plug & play system. *New Journal of Physics*, 4(1):41.

[Sudarshan, 1963] Sudarshan, E. (1963). Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams. *Physical Review Letters*, 10(7):277.

[Suhara, 2009] Suhara, T. (2009). Generation of quantum-entangled twin photons by waveguide nonlinear-optic devices. *Laser & Photonics Reviews*, 3(4):370–393.

[Suzuki et al., 2006] Suzuki, S., Tsujino, K., Kannari, F., and Sasaki, M. (2006). Analysis on generation schemes of Schrödinger cat-like states under experimental imperfections. *Optics Communications*, 259(2):758–764.

[Takahashi et al., 2010] Takahashi, H., Neergaard-Nielsen, J. S., Takeuchi, M., Takeoka, M., Hayasaka, K., Furusawa, A., and Sasaki, M. (2010). Entanglement distillation from Gaussian input states. *Nature Photonics*, 4(3):178.

[Takeuchi et al., 2004] Takeuchi, S., Okamoto, R., and Sasaki, K. (2004). Single photon source using parametric down conversion. In *Quantum Communications and Quantum Imaging*, volume 5161, pages 101–108. International Society for Optics and Photonics.

[Tamaki et al., 2016] Tamaki, K., Curty, M., and Lucamarini, M. (2016). Decoy-state quantum key distribution with a leaky source. *New Journal of Physics*, 18(6):065008.

[Tang and Reed, 1995] Tang, C. K. and Reed, G. T. (1995). Highly efficient optical phase modulator in SOI waveguides. *Electronics Letters*, 31(6):451–452.

[Tanzilli et al., 2001] Tanzilli, S., De Riedmatten, H., Tittel, W., Zbinden, H., Baldi, P., De Micheli, M., Ostrowsky, D. B., and Gisin, N. (2001). Highly efficient photon-pair source using periodically poled lithium niobate waveguide. *Electronics Letters*, 37(1):26–28.

[Tanzilli et al., 2012] Tanzilli, S., Martin, A., Kaiser, F., De Micheli, M. P., Alibart, O., and Ostrowsky, D. B. (2012). On the genesis and evolution of integrated quantum optics. *Laser & Photonics Reviews*, 6(1):115–143.

[Teja et al., 2007] Teja, V., Banerjee, P., Sharma, N., and Mittal, R. (2007). Quantum cryptography: state-of-art, challenges and future perspectives. In *2007 7th IEEE Conference on Nanotechnology (IEEE NANO)*, pages 1296–1301. IEEE.

[Tien and Ulrich, 1970] Tien, P. K. and Ulrich, R. (1970). Theory of prism–film coupler and thin-film light guides. *JOSA*, 60(10):1325–1337.

[Toren and Ben-Aryeh, 1994] Toren, M. and Ben-Aryeh, Y. (1994). The problem of propagation in quantum optics, with applications to amplification, coupling of em modes and distributed feedback lasers. *Quantum Optics: Journal of the European Optical Society Part B*, 6(5):425.

[Townsend et al., 1993] Townsend, P. D., Rarity, J. G., and Tapster, P. R. (1993). Single photon interference in 10 km long optical fibre interferometer. *Electronics Letters*, 29(7):634–635.

[Tselniker et al., 2009] Tselniker, I., Nazarathy, M., and Orenstein, M. (2009). Mutually unbiased bases in 4, 8, and 16 dimensions generated by means of controlled-phase gates with application to entangled-photon QKD protocols. *IEEE Journal of Selected Topics in Quantum Electronics*, 15(6):1713–1723.

[Ulrich and Torge, 1973] Ulrich, R. and Torge, R. (1973). Measurement of thin film parameters with a prism coupler. *Applied Optics*, 12(12):2901–2908.

[Van Assche, 2006] Van Assche, G. (2006). *Quantum cryptography and secret-key distillation*. Cambridge University Press.

[Van Campenhout et al., 2009] Van Campenhout, J., Green, W. M., Assefa, S., and Vlasov, Y. A. (2009). Low-power, 2× 2 silicon electro-optic switch with 110-nm bandwidth for broadband reconfigurable optical networks. *Optics Express*, 17(26):24020–24029.

[Vidal and Werner, 2002] Vidal, G. and Werner, R. F. (2002). Computable measure of entanglement. *Physical Review A*, 65(3):032314.

[Vidrighin et al., 2013] Vidrighin, M., Bartley, T. J., Donati, G., Jin, X.-M., Barbieri, M., Kolthammer, W. S., Datta, A., and Walmsley, I. A. (2013). Requirements for two-source entanglement concentration. *Quantum Measurements and Quantum Metrology*, 1:5–11.

[Walls, 1983] Walls, D. F. (1983). Squeezed states of light. *Nature*, 306(5939):141–146.

[Wang et al., 2016] Wang, J., Qin, X., Jiang, Y., Wang, X., Chen, L., Zhao, F., Wei, Z., and Zhang, Z. (2016). Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units. *Optics Express*, 24(8):8302–8309.

[Wenger et al., 2004] Wenger, J., Tualle-Brouri, R., and Grangier, P. (2004). Non-Gaussian statistics from individual pulses of squeezed light. *Physical Review Letters*, 92(15):153601.

[Wentzel, 1926] Wentzel, G. (1926). Eine verallgemeinerung der quantenbedingungen für die zwecke der wellenmechanik. *Zeitschrift für Physik*, 38(6-7):518–529.

[Wiesner, 1983] Wiesner, S. (1983). Conjugate coding. *ACM Sigact News*, 15(1):78–88.

[Wolf et al., 1984] Wolf, E., Agarwal, G. S., and Friberg, A. (1984). Wavefront correction and scattering with phase-conjugate waves. In *Coherence and Quantum Optics V*, pages 107–116. Springer.

[Wootters and Zurek, 1982] Wootters, W. K. and Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299(5886):802–803.

[Wu et al., 1987] Wu, L.-A., Xiao, M., and Kimble, H. (1987). Squeezed states of light from an optical parametric oscillator. *JOSA B*, 4(10):1465–1475.

[Wyant, 1982] Wyant, J. C. (1982). Interferometric optical metrology: basic systems and principles. *Laser Focus*, pages 65–71.

[Wyant, 2015] Wyant, J. C. (2015). Interferometric optical metrology. *OSA Century of Optics*.

[Xia et al., 2012] Xia, C., Amezcua-Correa, R., Bai, N., Antonio-Lopez, E., Arrioja, D. M., Schulzgen, A., Richardson, M., Liñares, J., Montero, C., Mateo, E., et al. (2012). Hole-assisted few-mode multicore fiber for high-density space-division multiplexing. *IEEE Photonics Technology Letters*, 24(21):1914–1917.

[Xu et al., 2010] Xu, F., Qi, B., and Lo, H.-K. (2010). Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 12(11):113026.

[Xu et al., 2014] Xu, F., Curty, M., Qi, B., and Lo, H.-K. (2014). Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):148–158.

[Xu et al., 2005] Xu, Q., Schmidt, B., Pradhan, S., and Lipson, M. (2005). Micrometre-scale silicon electro-optic modulator. *nature*, 435(7040):325–327.

[Xu et al., 2008] Xu, Q., e Silva, M. C., Gallion, P., and Mendieta, F. (2008). Auto-compensating quantum cryptosystem using homodyne detection. In *OFC/NFOEC 2008-2008 Conference on Optical Fiber Communication/National Fiber Optic Engineers Conference*, pages 1–3. IEEE.

[Yariv, 1987] Yariv, A. (1987). Operator algebra for propagation problems involving phase conjugation and nonreciprocal elements. *Applied optics*, 26(21):4538–4540.

[Yegnanarayanan et al., 1997] Yegnanarayanan, S., Trinh, P. D., Coppinger, F., and Jalali, B. (1997). Compact silicon-based integrated optic time delays. *IEEE Photonics Technology Letters*, 9(5):634–635.

[Yin et al., 2016] Yin, H.-L., Chen, T.-Y., Yu, Z.-W., Liu, H., You, L.-X., Zhou, Y.-H., Chen, S.-J., Mao, Y., Huang, M.-Q., Zhang, W.-J., et al. (2016). Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters*, 117(19):190501.

[Yokoyama et al., 2013] Yokoyama, S., Ukai, R., Armstrong, S. C., Sornphiphatphong, C., Kaji, T., Suzuki, S., Yoshikawa, J.-i., Yonezawa, H., Menicucci, N. C., and Furusawa, A. (2013). Ultra-large-scale continuous-variable cluster states multiplexed in the time domain. *Nature Photonics*, 7(12):982.

[Yoshino et al., 2007] Yoshino, K.-i., Aoki, T., and Furusawa, A. (2007). Generation of continuous-wave broadband entangled beams using periodically poled lithium niobate waveguides. *Applied Physics Letters*, 90(4):041111.

[Yuen, 1996] Yuen, H. P. (1996). Quantum amplifiers, quantum duplicators and quantum cryptography. *Quantum and Semiclassical Optics: Journal of the European Optical Society Part B*, 8(4):939.

[Zavatta et al., 2004] Zavatta, A., Viciani, S., and Bellini, M. (2004). Quantum-to-classical transition with single-photon-added coherent states of light. *Science*, 306(5696):660–662.

[Zavatta et al., 2009] Zavatta, A., Parigi, V., Kim, M. S., Jeong, H., and Bellini, M. (2009). Experimental demonstration of the bosonic commutation relation via superpositions of quantum operations on thermal light fields. *Physical Review Letters*, 103(14):140406.

[Zavriyev et al., 2009] Zavriyev, A., Trifonov, A., and LaGasse, M. (2009). Two-way QKD system with active compensation. US Patent 7,606,371.

[Zbinden et al., 1997] Zbinden, H., Gautier, J. D., Gisin, N., Huttner, B., Muller, A., and Tittel, W. (1997). Interferometry with Faraday mirrors for quantum cryptography. *Electronics Letters*, 33(7):586–588.

[Zheng et al., 2008] Zheng, C.-T., Ma, C.-S., Yan, X., Wang, X.-Y., and Zhang, D.-M. (2008). Analysis of response characteristics for polymer directional coupler electro-optic switches. *Optics Communications*, 281(24):5998–6005.

[Zhou and Duan, 2006] Zhou, Z. and Duan, X. (2006). Integrated waveguide splitter fabricated by Csˆ+–Naˆ+ ion-exchange. *Optics Communications*, 266(1):129–131.

[Zhu et al., 2012a] Zhu, K., Li, S., Zheng, X., and Tang, H. (2012a). Non-Gaussian state with vortex structure of quantized radiation field. *JOSA B*, 29(6):1179–1186.

[Zhu et al., 2012b] Zhu, K.-C., Li, S.-X., Tang, Y., Zheng, X.-J., and Tang, H.-Q. (2012b). Wigner function and the entanglement of a quantized Bessel-Gaussian vortex state of a quantized radiation field. *Chinese Physics B*, 21(8):084204.

[Zou et al., 2018] Zou, L., Gu, X., and Wang, L. (2018). High-dimensional free-space optical communications based on orbital angular momentum coding. *Optics Communications*, 410:333–337.