INTERNATIONAL DOCTORAL
SCHOOL OF THE USC

Gabriel María
Carral López

PhD Thesis

Autocompensating two-photon quantum cryptography for optical fiber communication systems

Santiago de Compostela, 2023

Doctoral Programme in Laser, Photonics and Vision

ESCOLA DE DOUTORAMENTO
INTERNACIONAL DA USC

DOCTORAL THESIS

AUTOCOMPENSATING TWO-PHOTON QUANTUM CRYPTOGRAPHY FOR OPTICAL FIBER COMMUNICATION SYSTEMS

Author

Gabriel María Carral López

Supervisor/s: Jesús Liñares Beiras and Xesús Prieto Blanco

Tutor: Jesús Liñares Beiras

PHD PROGRAMME IN LASER, PHOTONICS AND VISION

SANTIAGO DE COMPOSTELA

Abstract

Quantum Key Distribution (QKD) is a technique that provides perfect secrecy for communication systems, which is crucial against quantum computers capable of breaking current public-key cryptosystems. QKD is becoming a mature technology but it still suffers from implementation problems due to imperfections on real hardware that soften it's security. To correct those is necessary to develop error mitigation mechanisms, as well as security by design through use of two-photon protocols. In this Thesis, we combine these two approaches in fiber-based QKD, particularizing for evolved fibers with improved data bandwidths. At the same time, we emphasize integration with quantum photonics, and carry out actual microfabrication of basic elements in the laboratory for future QKD applications.

Resumo

O algoritmo de Shor (1994) puxo sobre a mesa as notables capacidades dun ordenador cuántico en comparación coa súa contrapartida clásica. Shor demostrou que un ordenador cuántico podería ser capaz de resolver problemas como a factorización de números primos ou o problema do logaritmo discreto, intratables para un ordenador clásico. A partir de estes problemas, xa que difíciles, constrúense importantes sistemas criptográficos que garanten a nosa seguridade na rede á hora de protexer datos sensibles. Como solución a este problema atopamos dúas alternativas. A primeira, buscar mellores algoritmos, que poidan resistir ser atacados por un ordenador cuántico. A segunda, podemos usar a propia mecánica cuántica para protexer as nosas comunicacións, cifradas de forma clásica pero usando unha canle cuántica para transmitir a clave de cifrado. Xorde así o problema da distribución de chave cuántica (QKD, polas súas siglas en inglés).

Aínda que incodicionalmente segura na teoría, a QKD sofre na implementación física, xa que os elementos de hardware necesarios nunca son perfectos, e poden ser explotados por un adversario para extraer información sen ser detectado, cando a premisa fundamental da QKD é que calquer intento de obter información confidencial por unha parte non autorizada xera erros na información. Polo tanto un espía pode ser detectado.

Estes erros mesturanse cos que naturalmente aparecen ao comunicarse mediante un canal físico como poden ser fotóns viaxando ao longo dun cable de fibra óptica. Os fotóns, as excitacións do campo electromagnético que compoñen a luz, son fráxiles, aínda que non tanto coma outros sistemas cuánticos. Aínda así, poden ser absorbidos pola fibra e a información que codifican pode modificarse no transcurso da súa propagación. Todo isto leva a que a tasa de información segreda que se transmite caia repentinamente e a QKD só funcione a distancias pequenas, cando o desexable, a priori, sería estendela a redes de escala mundial.

Por outro lado, esta comunicación cuántica de natureza óptica require de hardware óptico dedicado, para poder xerar, procesar e medir os sinais ópticos que se empregan en QKD. Ditos dispositivos pretenden, en última instancia, traballar con fotóns individuais ou aproximacións destes. Co cal, han de ser estables, robustos e presentar perdas mínimas. A tecnoloxía fotónica integrada aparece aquí, polo tanto, coma un notable candidato, moi compatible con fibras ópticas, potencialmente barato e sinxelo, e coa capacidade de miniaturizarse. Unha implementación adecuada dun protocolo de QKD ten que ter en conta todos estes factores. Nesta Tese traballouse nestes aspectos de forma simultánea.

Na Introdución motivase a necesidade de protexer de forma cuántica as comunicacións, dada a posibilidade dun ordenador cuántico para romper importantes protocolos criptográficos estándar. Plantexase o debate, existente na actualidade, entre a necesidade de modificar ou propoñer protocolos novos que resistan un ordenador cuántico, a chamada *post-quantum cryptography* ou empregar as propiedades da cuántica para construir unha capa física que produzca un cifrado de clave simétrica totalmente seguro, isto é, a QKD. Xa que esta é a opción traballada nesta tese,

dase un breve panorama da súa situación actual, do traballo xa realizado pola comunidade, así como de problemas aínda por resolver. Péchase a Introdución explicando os obxectivos e a metodoloxía levada a cabo para esta Tese. Os traballos científicos publicados relacionados ca Tese recollense nun apéndice ao final da mesma (ApéndiceD).

O Capítulo 2, se ben recolle algunhas contribucións orixinais, é fundamentalmente introductorio, e reúne os ingredientes de hardware que se usarán despois no resto da Tese. Descríbense distintos compoñentes ópticos de uso en protocolos QKD. Enunméranse e detallase o funcionamento de dispositivos discretos que operan sobre distintos grados de liberdade do fotón: polarización e modos espaciais. Cada grado de liberdade require hardware específico. Así, a polarización adoita manipularse con láminas de onda, mentres que as funcións espaciais poden alterarse con montaxes de lentes cilíndricase prismas de Dove. De seguido, introdúcense dispositivos integrados, no cales se focaliza a Tese, e máis orientados a traballar coa codificación de tipo *dual-rail*, propia das fibras de varios núcleos. Descríbense os principios básicos das guías de onda e como isto se traduce á mecánica cuántica. Usando resultados coñecidos en computación cuántica mediante óptica lineal conclúese que o uso de acopladores direccionais e desfasadores (*phase shifters*) é suficiente para realizar calquera transformación unitaria nun qubit. A realización experimental de estes desfasadores será o obxecto do Capítulo 4. Por outro lado, propónse, de maneira teórica, a realización de fases de forma non dinámica, como se fai de cotío, senón topolóxica, a partir dun sistema formado por unha guía de dous modos cunha rede de difracción integrada. As fases de orixe xeométrico ou topolóxico son de interese xa que, a priori, son máis robustas que a súa contrapartida dinámica, ao estar imbuídas na propia estrutura fundamental da evolución do sistema, non esixindo da mesma precisión que un efecto dinámico. Polo tanto, enténdese como desexable ser capaz de xeralas no contexto da fotónica, para ser posiblemente usadas en apliacións como a QKD.

A continuación descríbese unha peza de hardware fundamental en comunicacións cuánticas: a fibra óptica. Esta está baseada na óptica integrada, pero ten as súas particularidades. Explícanse os distintos tipos de fibras (estruturas de un modo -*single-mode*-, de varios núcleos -*multicore*-, e de varios modos -*few-mode*-), e como se comporta o fotón cando as percorre. No tratamento cuántico (ou máis ben semiclásico) da fibra, analizase a modelización tanto da atenuación, dado que os fotóns son absorbidos pola fibra, coma das perturbacións, representadas por matrices unitarias de tipo SU(2) con coeficientes que resultan ser variables aleatorias. Descrébense asimesmo conectores básicos, de uso relevante nas codificacións consideradas (relativas ao tipo de fibra empregada), coma circuladores e lanternas fotónicas.

Para correxir esas perturbacións, optaremos por sistemas pasivos, que son sinxelos, non requirindo de monitorización activa nin consumo adicional de recursos e enerxía. Esta técnica pasiva coñecese co nome de *autocompensación* e está baseada en dar aos protocolos unha estrutura de ida e volta tal que, no punto de retorno, se colocan certos elementos ópticos que transforman o estado perturbado do fotón de modo que na volta, as perturbacións desfanse (auto-corríxense) e o estado orixinal restaurase. Os ingredientes descritos en dita sección serán utilizados constantemente

nos Capítulos 3 e 5.

Finalmente, para pechar o Capítulo, delíneanse o resto de ingredientes fundamentais presentes nun protocolo de QKD como son as fontes de pulsos ópticos, co seu tratamento cuántico, mencionando tanto fontes de pulsos febles (*weak-coherent pulses*), xa que se trata de aproximarse ao comportamento monofotón, coma de *estados entretecidos* (SPDC, idealmente monofotón). Do mesmo xeito, dase unha descrición básica do *endpoint* da comunicación cuántica: os detectores, particularizando para fotodetectores de avalancha (*avalanche photodetectors*) reunindo algúns resultados sobre probabilidades de detección empregados a cotío na literatura. Cando se compute nos Capítulos 3 e 5 o rendemento dos protocolos de QKD, os parámetros que caracterizen as fontes e aos detectores serán relevantes. En particular, no Capítulo 3 consideraránse pulsos multifotón, o que xera problemas de seguridade a menos que se introduzan estados "cebo" ou *decoy states*, o cal complica as expresións matemáticas resultantes, así coma en certa medida o hardware do protocolo, pero consigue incrementar de forma notable o rendemento dos protocolos. Por outro lado, os detectores actúan como factor limitante, ao ter unha eficiencia típicamente notablemente por baixo da unidade, e introducir ruido en forma de detección ou *clicks* espúreos chamados contas escuras ou *dark counts.*

No Capítulo 3 éntrase xa a fondo en QKD, a nivel de funcionamento de protocolos e formalizando a intuición que hai detrás da chamada seguridade baseada nas leis da física (cuántica). Explícase o protocolo pioneiro BB84, así coma o rol do espía, convencionalmente denominado Eve, que pretende lanzar ataques sobre a liña de comunicación que manteñen os axentes lexítimos chamados convencionalmente Alice e Bob. O protocolo BB84, chamado así polos nomes dos seus ideadores (Charles Bennet e Gilles Brassard) e polo ano no que foi proposto (1984), basease en codificar a información en estados cuánticos non ortogonais, de xeito que nunha única medida non sexa posible identificar de forma non ambigua cal dos estados foi medido. Xa que a mecánica cuántica prohibe as copias perfectas de estados, isto significa que un espía non vai ter máis remedio que introducir erros na comunición entre os usuarios Alice e Bob, cunha certa probabilidade que é detectable por estes.

Dado que é imposible eliminar a presencia dun espía, e distinguir, desde un punto de vista criptográfico, se os erros na clave son debidos a ela ou a erros experimentais, por moito que se minimizen estes, o obxectivo final do protocolo é conseguir que a información que o espía poida adquirir sexa despreciable. Así, eliminanse erros mediante algoritmos de correción de erros e limitase dita información mediante técnicas de amplificación de privacidade. Finalmente, Alice e Bob son capaces de extraer unha clave totalemente segreda, que só eles coñecen, cunha certa taxa, chamada *secret key rate - R, en idioma inglés* que depende da distancia que os separe, entanto depende da atenuación e ruido na liña de fibra. Este parámetro R permítenos avaliar o rendemento dun determinado protocolo QKD, e así o faremos cando analicemos os protocolos propostos.

De seguido, descríbese unha importante clase de protocolos que, polas súas propias características, están libres de calquer ataque nas unidades de detección. Por deseño, os protocolos son robustos ante calquer intento de manipulación da etapa de medida, non proporcionando esta información algunha a ningún adver-

sario, independentemente da súa capacidade para *hackear* os protocolos. Dito de outra forma, a detección pode deixarse en más dunha terceira parte (*Charlie*) e tratarse coma unha caixa negra que comunica ao exterior unha resposta binaria (mediuse isto ou o outro). Así, pódense construir protocolos chamados MDI-QKD, por *measurement-device-independent* ou independentes dos dispositivos de medida. Estes protocolos fan uso, se ben na última etapa e por post-selección, do xa mencionado entretecemento cuántico. Esta propiedade é exclusiva da física cuántica sen ningunha contrapartida clásica, e é de cotío considerada coma unha das se non a propiedade definitoria da física cuántica. Co cal, dase a circunstancia de que unha propiedade tan fundamental ten ao mesmo tempo unha aplicación práctica notabilísimamente relevante.

O que nós faremos, e isto constitúe os principais resultados do Capítulo, será aplicar, a estes protocolos de tipo MDI, técnicas de autocompensación axeitadas. Deseñaremos a implementación física do protocolo, describindo en detalle a circulación da luz e todos os dipositivos necesarios para tal tarefa, tanto a nivel de codificación de información, como autocompensación, detección ou tarefas intermedias como introdución de retardos entre pulsos. Consideraremos tres codificacións distintas en grados de liberade do fotón. Cada unha delas requerirá dun hardware específico, isto é, de compoñentes ópticos capaces de manipular os devanditos graos de liberdade. Por un lado, analizaremos o da polarización, que é unha codificación estándar na literatura. Por outro, o dos modos espaciais, xa sexa en canto á forma da función de modo, relevante en fibras de poucos modos (*few-mode*), ou en canto ao núcleo de fibra (*core*) polo que circulan os fotóns, relevante en fibras de varios núcleos. Neste último caso faremos especial enfásis, xa que todo o hardware empregado pode ser integrado, o que faría a realización do protocolo unha tarefa moi compacta e ata de baixo custo.

Modelizaremos os erros debidos á fibra de forma heurística, para introducilos así na expresión de R, tendo en conta ademais pulsos multifotón, e determinar o rendemento do protocolo (cantidade de información segreda intercambiada por pulso de luz enviado fronte a distancia do enlace de fibra) así como principalmente os beneficios da autocompensación. O modelo dos erros terá en conta parámetros físicos das fibras de varios nucleos, como é o denominado *cross-talk*, que expresa cuantitativamente o feito de que parte da potencia óptica dun modo viaxando ao longo dun núcleo pode, por acoplamento modal, pasar a outro modo doutro núcleo. Este é un problema que xa se atopa nas comunicación ópticas clásicas neste tipo de fibra. Xa que a información se codifica precisamente, de forma binaria, mediante a presencia ou non, ou unha superposición de esta, nun núcleo ou noutro, o *cross-talk* vai ser unha das fontes de ruido máis relevantes en implementacións de QKD en fibras de varios núcleos. Finalmente, faremos unha breve reflexión sobre extensións destes protocolos a alta dimensión ou arquitecturas multicanle, resaltanto as dificultades encontradas.

O Capítulo 4 recolle os esforzos experimentais levados a cabo no contexto desta Tese. Partindo da idea xa antes exposta de que con acopladores direccionais e desfasadores calquer operación nun só qubit pode ser levado a cabo, e valéndose de coñecemento previo do grupo de investigación en acopladores direccionais, deseñase

e fabricase un chip óptico que contén acopladores e desfasadores en estruturas tipo Mach-Zehnder, que nos son útiles para medir ditas fases por inteferencia óptica. As fases xenéranse ensanchando unha guía chamada de canle. Para encaixar adecuadamente dita parte ensanchada ao resto da guía, minimizando perdas e non introducindo acoplamento a modos de orde superior (búscase operación monomodo) conclúese que a mellor solución consiste en facer a unión mediante estruturas denominadas *taper* que operen de forma adiabática. Así, o chip conterá multiples interferómetros Mach-Zehnder con desfasadores unidos mediante tapers, percorrendo un rango de lonxitudes de ditos desfasadores, para obter un modelo que nos permita predicir a fase introducida con respecto a lonxitude dos mesmos.

Descríbense en detalle todas as fases de fabricación. En primeiro lugar, o deseño, cos criterios anteriormente descritos. Despois, a fabricación de máscaras de aluminio sobre sustratos de vidro mediante fotolitografía. Esta técnica consiste en iluminar unha capa de fotorresina sobre o aluminio previamente depositado no vidro, de acordo co patrón deseñado, reducindose o seu tamaño (miniaturizando) no proceso. Así, as partes da fotorresina expostas á luz serán reveladas. Posteriormente, as mostras introdúcense nun ácido capaz de morder o aluminio, deixando o vidro á vista, mentres que dito alumnio protexe o resto. Coa máscara correctamente realizada, a mostra introdúcese nun forno a alta temperatura nun baño dun sal determinado, dando lugar a intercambio iónico nas zonas onde o vidro permaneceu exposto, e por tanto, a un incremento no índice de refracción, o que permite o guíado de luz. Así, obténse finalmente un chip de vidro con guías de onda seguindo a estrutura Mach-Zehnder impresas nel. Este chip vai ser caracterizado de dúas maneiras. A primeira, para asegurarse de que despois de todo o proceso as medidas dos elementos son as adecuadas, mediante métodos de recuperación de fase empregando un microscopio óptico coa técnica *DIC* ou contraste por interferencia diferencial. A segunda, para ver se os desfasadores funcionan como deberían, introdúcese luz na entrada da guía para que a percorra, e mídese a saída. Para facer isto dunha forma rápida e flexible constrúese de forma ad-hoc unha montaxe de tipo acoplamento por prisma. Os prismas empregados fabrícanse a propósito no laboratorio a partir de adhesivo óptico. Un feixe láser incidente focalizase a través do primeiro prisma na entrada das guías, dando lugar ao acoplamento. A luz correspondente aos modos guíados é extraída por un segundo prisma, e recollida por outra cámara. O sinal adquirido procésanse de forma computacional mediante algoritmos de *thresholding* automático. Fanse pois medidas da potencia relativa entre as saídas para poder calcular así a fase.

O desenvolvemento do Capítulo 5 é similar ao Capítulo 3. Neste caso, analízase a autocompensación pero aplicada a protocolos que usan desde un inicio estados entretecidos, coma é o protocolo denominado BBM92, que é unha versión do protocolo E91 pero que non necesita de empregar *desigualdades de Bell*. Estas desigualdades constitúen un resultado crucial a nivel dos fundamentos da mecánica cuántica, así coma teñen un gran interese aplicado. A propia estrutura do protocolo BBM92 restrinxe decisivamente a autocompensación, o cal suxire a introdución dun novo protocolo que si poida ser autocompensable. Para avaliar isto numéricamente faise un estudo das perturbacións da fibra cando actúan sobre un estado entretecido.

Dado que os coeficientes da perturbación son variables aleatorias, aquí tómase unha ruta distinta ca no Capítulo 3, consistente en asumir certos modelos razonables de ruído para ditas variables, isto é, supoñer que se distribúen de acordo con certas funcións de probabilidade. Así, computase a taxa de clave para o caso monofotón comparando o protocolo BBM92 para distintos niveis de ruido co protocolo proposto. Dito protocolo está baseado nas propiedades dos *estados de Bell*, que son un conxunto (unha base) de estados máximamente entrelazados, cando se permutan as *etiquetas* das partículas, neste caso fotóns, ás que se refiren. Pola forma na que se codifica a información, en termos dunha fase relativa, o protocolo pode construírse coma de ida e volta, sendo así posible a compensación de perturbacións tanto de fase coma por acoplamento modal, entanto o protocolo BBM92 só vai admitir compensación de fase, e aínda así de forma pouco práctica. Do mesmo xeito ca no Capítulo 5, faise unha análise en detalle da circulación da luz, así coma se detallan todos os compoñentes ópticos relevantes para implementar o protocolo.

Para rematar, xa no Capítulo 5.2.4 conclúese a tese, facendo un resumo dos resultados obtidos así coma das dificultades atopadas e as posibilidades futuras de mellora e investigación. En particular, abrénse posibilidades en case todos os puntos tocados na Tese. Por un lado, a xeración de fases topolóxicas en fotónica, se ben non falto de complicación, polo feito de facerse necesario a cancelación da parte dinámica, non sen complicación. Por outro lado, para que ditas fases sexan realmente utéis (computación universal a dimensión arbitraria), precisase de usar interación entre fotóns: esta é debil por natureza, necesitando de procesos non lineais moi fortes. En calqueira caso sería desexable, ao menos nos casos máis simples, ser capaces de fabricar dispositivos topolóxicos no laboratorio, e ser capaces de medir as fases (topolóxicas) xeradas.

Por outro lado, en canto aos protocolos QKD, quedan pendentes dúas cousas: en primeiro lugar, un análise máis refinado dos erros introducidos polas perturbacións nas fibras. En particular, serían desexables simulacións numéricas e cálculos máis elaborados que permitisen ser máis precisos á hora de dar modelos de ruído máis axustados aplicables a escenarios de tipo QKD, cunha conexión máis precisa cos parámetros experimentais. Por outro lado, tamén sería desexable a comprobación en laboratorio dos mecanismos de autocompensación descritos na Tese, por exemplo en experimentos en entornos controlados que emulen o comportamento das fibras consideradas en escenarios reais.

Contents

Acknowledgements

En primeiro lugar, quero agradecer aos meus directores Suso Liñares e Xesús Prieto por ter supervisado esta tese. Asimismo, quero agradecer tamén ao resto da área de Óptica pola axuda recibida: Vicente, Lola, Carlos, Ana... Tamén, como non, á xente do despacho de bolseiros do piso de arriba: Alejandro, Ana, Bruno, Damián e en especial ao gran Bastián. A Héctor, polo ben que sempre se portou comigo e tanto que me axudou; ese xeito rápido e fugaz de resolver problemas no laboratorio.

I will like to thank all the people from INL, which made those three months the most amenable experience: Bejoys, Jana, Bruno, Filipe, Christian, Leonor, Joao Silva, Joao Azevedo, Artur, Beatriz... e especialmente Miguel, que tanta sorte tiven de atopar.

Aos meus amigos A. Brea (A de Aro, longa historia), Capitán Casais, Gonzalo (club de fans de), Lomba, Fidelio, Abraham. Fostes (e sodes) o mellor da experiencia santiaguesa, sen dúbida. Ao resto dos autodenominados vimers: Marcos, Moncho, Asier, Pablo, Saúl. A Miguel o Celíaco, gran persoa (casi 2 m de estatura). A David e a Guille, estamos lonxe pero retornaremos, coma sempre.

Last but not least, quero agraceder por suposto a miña familia: a meus pais, a meu irmao, a meus abuelos. Sen o seu apoio e cariño todo carecería de sentido. A Laura, por terme aguantado tanto e tan ben. Ancla e vela ao mesmo tempo, que vou dicir. Gracias.

List of abbreviations

A-MDI-QKD Autocompensating Measurement-Device-Independent Quantum Key Distribution

AA-phase Aharonov-Anandan phase

AES Advanced Encryption Standard

BB84 Bennet-Brassard 1984 protocol

BBM92 Bennet-Brassard-Mermin 1992 protocol

BMD Bell Measurement Device

BPM beam propagation method

BS beam-splitter

BSEP Bell states exchange parity

CLC cylindrical lens converter

d.o.f degrees of freedom

DC directional coupler

DIC differential interference contrast

DP Dove prism

DSA Digital Signature Algorithm

EM electromagnetic

FM Faraday mirror

FMF few-mode fiber

GRIN gradient refractive index

HG Hermite-Gauss

HOM Hong-Ou-Mandel

HWP half-wave plate

Ionex ion-exchange

ISG initial states generator

LP linearly polarized

MCF multicore fiber

MDI Measurement-Device-Independent

MMI multimode interference coupler

MUBs mutually unbiased bases

MZI Mach-Zehnder interferometer

OC optical circulator

OFD optical fiber delay

P&P Plug and Play

PBS polarizing beam-splitter

PDF probability density function

PL photonic lantern

PM phase modulator

PMF polarization-maintaining fiber

PNS Photon Number Splitting

PQC Post Quantum Cryptography

PSA phase shifting algorithm

QBER quantum bit error rate

QDS quantum digital signature

QKD Quantum Key Distribution

QM Quantum Mechanics

QND quantum nondemolition

QWP quarter-wave plate

RDC reconfigurable directional coupler

ROI region of interest

RSA Rivert-Shamir-Adleman

RV random variable

SDM spatial division multiplexing

SMF single-mode fiber

SPDC spontaneous parametric down-conversion

SSPD superconducting single-photon detector

TE transverse electric

TIR total internal reflection

TM transverse magnetic

TRL technological readiness level

VOA variable optical attenuator

WCP weak coherent pulse

WKB Wentzel-Kramers-Brillouin

List of Figures

List of Tables

Chapter 1

Introduction, objectives and methodology

Concealing information from unintended eyes has been a constant throughout all human history [1]. And not only human, as many other life forms conceal information (normally, about their whereabouts) in order to prey or avoid being preyed. In today's society, there is a vast circulation of information. Optical fiber networks, satellite communications, radio-frequency signals... support this interchange. A great deal of this information is confidential. E-commerce, online banking, e-mails, messaging apps, are some of the examples of applications needing from some sort of secrecy. Part of this secrecy is furnished by a form of *mathematical cryptography* called *public-key* or asymmetric cryptography [2, 3]. According to this system, the *key* (a string of bits) used for ciphering (convolving with the message rendering it unreadable to illegitimate parties) is different from that used to de-cipher the message. Consider for instance two users that wish to exchange private information. They are usually called *Alice and Bob*. Say Alice wants to send a message to Bob. First, Bob makes some *mathematical manipulations*, generating a pair of keys, one private and one public. He then sends the public one to Alice. Anyone can access this key, even an spy, or *eavesdropper*, which is usually called Eve. With that public key Alice encodes its message, and sends it back to Bob, on the same untrusted channel. Then, Bob uses his private key to decipher Alice's message[1].

At the heart of the security of such scheme are the mathematical manipulations that we mentioned. *They depend on computational complexity assumptions*, meaning that the security of the system depends on the fact that there exist some mathematical operations that are extremely difficult to reverse, such as *prime number factoring* or the *discrete logarithm problem* [5]. One the most used cryptographic systems, the Rivert-Shamir-Adleman (RSA) algorithm, relays on the first of such hard problems [6].

As far as classical computing is concerned, those schemes are safe because those problems are too difficult for a classical computer (at least for now, as we cannot

[1]It may be pointed here that often public.key cryptosystems are quite slow, thus they are used to actually cipher keys for symmetric key cryptosystems [4]

rule out the possibility of progresses in classical computation in this very direction). However, such hardness assumption would not longer hold for another class of computer, a *quantum* computer. This realisation came into the spotlight when Peter Shor proposed his famous algorithm [7]. If we are able to build a computer based on quantum mechanical laws, then we may be able to solve prime number factorization and discrete logarithms in polynomial time. Thus the RSA scheme and other relevant cryptosystems like Elliptic-curve cryptography and the Digital Signature Algorithm (DSA) [8] are no longer secure. In general, with a quantum computer present, public key cryptography is at risk, while for symmetric cryptography some minor problems arise[2], with Grover's algorithm coming into play, in particular, the need for bigger key sizes [8]. Importantly, this applies not only to future communications, but also to secrets kept now under such scheme. This could be unveiled in the future, if the adversary were to have a quantum computer at its disposal.

Thus, as the practical implementation of a quantum computer becomes less and less challenging, solutions are required to keep the safety of the communications. There, are, at least, two main ways to deal with the problem. The first one is to develop new cryptographic algorithms that are resistant to attacks coming from quantum computers, *i.e* which are *quantum safe*. This is termed as Post Quantum Cryptography (PQC), as it is (mathematical) cryptography after the emergence of quantum computers. On the other side, we can use a *quantum channel* to transmit information. According to Quantum Mechanics (QM), gaining information about an unknown quantum system induces appreciable disturbances on it. If we encode information in quantum systems, then a spy looking into it will inevitably introduce a disturbance that *we, the legitimate users, can sense*, thus uncovering its presence. This principle can be use to *distribute* key safely, which then can be used as input for classical provably secure symmetric algorithms like the one-time pad or the Advanced Encryption Standard (AES). As such, this cryptosystem is called Quantum Key Distribution (QKD).

In the cryptographic community, often PQC and QKD are perceived as separate (even rivalling) alternatives [9]. One of the main drawbacks of QKD, as is often argued, is the fact that the channel needs to be authenticated prior to the running of any protocol, and that QKD alone cannot be used for that matter. Indeed, some classical algorithm would need to be used. This is seen as a weakness, as public-key cryptosystems like Diffie-Hellman allow users to communicate without the need to have a pre-shared key for authentication [10]. If QKD needs to authenticate the users through a previous round of public-key cryptography, then it does not solve in full the problem it was aimed for, even tough the authentication step would require for little keying material and be done efficiently [11]. However, some solutions within the field, quantum digital signature (QDS) [12] are been developed, an cross-fertilization between PQC and QKD will likely be beneficial for the matter. Specifically, PQC may be used to authenticate Alice and Bob for subsequent QKD [13].

Other disadvantage commonly associated with QKD is the difficulty of building a reliable quantum channel [14]. On the one hand, it is hard to have realistic quantum

[2]Note however that classical symmetric cryptography has its own disadvantages, mainly what happens if the key is obtained by an untrusted third party.

mechanical models that accurate describe the devices involved, in order to avoid any backdoor Eve may access. Progress is being made in this realm, both at figuring out possible hacks on quantum channels and possible countermeasures, by designing QKD protocols that can work even if (some of) the devices are untrusted [15, 16]. On the other hand, it is a established fact that quantum systems are very fragile, and that inevitably leads to errors in the communication process. One of the preferred implementations of a quantum channel is photons travelling along optical fibers. Information may be encoded in some degrees of freedom (d.o.f) of the photon. Real fibers, however, do not work exactly as intended. They have imperfections, which couple to the photon's d.o.fs, introducing errors in the keying material. Substituting the fibers for better ones is an option, but expensive. One ideally would want to use already existing fiber infrastructure, or at least not to depend to much on future developments of fiber technology, in the sense of searching for fundamentally practical solutions. The aim of this Thesis goes precisely in this direction. To mitigate errors arising from imperfections on real fibers, by characterizing them and showing how to restore the photon-encoded information by the appropriate mechanisms. At the same time, we want to incorporate protocol designs that avoid the need for trusting some of the devices, thus aligning with the idea of more realistic QKD protocols.

The status of the QKD field is not easy to determine, but what can be said is that, on the one hand, it constitutes a very intense academic field, with many efforts in various directions, and many connections to other realms, with great progress in finding more feasible versions of QKD [17]. On the other hand, improved practical QKD systems are being deployed [18]. Also, the commercialization of the technology has started, and it is expected to grow, not without difficulty, as commercial QKD systems have been shown to be vulnerable in the past (for instance, see [19]). The need for standardization is ongoing [20, 21]. Achieving a higher technological readiness level (TRL) in QKD is also necessary. One of the ultimate goals will be building reliable QKD networks for a secure Quantum Internet. That will require from novel quantum technologies such as quantum repeaters, possibly including quantum memories among others [22].

1.1 Symmetric cryptography and QM

QM is, in a way, a potential threat to security, as long as we can build a device capable to break classical cryptographic schemes. On the other side, QM itself gives a possible solution to this problem. Actually, not only by itself, but if we make use of an information-theoretic secure [23] symmetric cryptographic scheme known as the *one-time pad* or *Vernam* cipher. It consists on mingling the message we want to secure with a random key of ones and zeroes. Most importantly, the ciphertext obtained is completely impossible to decipher for someone not in possession of the key. More specifically, given the message in the form of a 0 and 1's sequence, the key (another string of the same number of elements) is to be added to it mod 2 (i.e XOR operation):

$$plaintext \oplus key = 1001010 \oplus 1100011 = 0101001\ (ciphertext).$$

For an spy, the resulting string is totally random: any possible message deciphered from it is equally probable, thus bears no information to the unintended eyes. The key cannot be re-utilized to cipher more than one message; if done so, by simply applying the XOR operation to both cipher texts we would have

$$plaintext1 \oplus key \oplus plaintext2 \oplus key = plaintext1 \oplus plaintext2,$$

as the mod 2 sum of a 0's and 1's string and itself (the key and itself) is always a string of zeroes, which does not affect the other terms in the sum. Hence, part of the message would be unveiled.

Now, this system, which, we insist, is totally secure, suffers from one big problem. *What if some third party obtains the key?* For the one-time pad to work the key needs to be kept secret, but shared by the parties interested in exchanging information. The kind of information circulation we are interested in happens between distant parties on a daily basis. That begs the question of how to ensure that such parties can share a key at a distance while keeping it secure. And, not only secure, but fundamentally secure, without relying on trusted couriers or other methods. Fortunately, the quantum mechanic world offers some possibilities to achieve this, if we are able, of course, to encode, transport and decode information in things (the photon) that behave *quantum-ly*.

The realization that this can be possible is the fact that a quantum state cannot be cloned as expressed by the quantum no-cloning theorem [24]. As it is a very relevant and, at the same time, succinct result, we shall reproduce it here. Assume we have a quantum system in a normalized state $|\psi\rangle \in \mathcal{H}_1$ in a Hilbert space $\mathcal{H}_1$, which we want to copy into an ancillary system in a (normalized) state $|a\rangle \in \mathcal{H}_2$. The quantum no-cloning theorem proofs that there is no unitary transformation U acting on $\mathcal{H}_1 \otimes \mathcal{H}_2$ capable of the following operation $U(|\psi\rangle|a\rangle) = e^{i\alpha}|\psi\rangle|\psi\rangle$, where some phase α, in principle depending on ψ and a, is allowed. The proof of the theorem follows from contradiction. Consider now the overlap between $|\psi\rangle$ with $|\phi\rangle$, where $|\phi\rangle$ is some state of $\mathcal{H}_1$. We have $\langle\psi|\phi\rangle = \langle\psi|\phi\rangle\langle a|a\rangle = \langle\psi|\langle a|\phi\rangle|a\rangle$. Now we introduce $U^\dagger U = 1$ in between. We have $\langle\psi|\langle a|\phi\rangle|a\rangle = (\langle\psi|\langle a|U^\dagger)(U|\phi\rangle|a\rangle) = e^{-i\alpha}\langle\psi|\langle\psi|e^{i\alpha'}|\phi\rangle|\phi\rangle = e^{i(\alpha'-\alpha)}\langle\psi|\phi\rangle^2$. Now, this condition only holds for the *special* cases: either $|\phi\rangle = e^{i\gamma}|\psi\rangle$ or $|\phi\rangle \perp |\psi\rangle$. However, the states were arbitrary (we did not impose any condition on them). So, an unitary cloning operation U such as defined above cannot exist. Note that not only pure states cannot be cloned, but also mixed ones [25].

Although one cannot copy a quantum state imperfect copies (or in a non-deterministic way) can still be made [26]. However, such imperfections can be detected. Measurements on quantum states necessarily disturb unknown states being measured (if we know the state of a quantum system, we can perform a quantum nondemolition (QND) measurement, minimally disturbing the system [27]). That means that if we encode information in quantum states, that information cannot be obtained in the same way classical information can. If we encode a key into quantum states, it is not possible for a spy to obtain a copy of it to later decipher secret messages without leaving any trace. In other words, eavesdropping can be *fundamentally* detected. Thus, we can think of a way of encoding, transmitting

and recovering the key in a quantum fashion, so that in the case of an adversary tampering with our communication, results in a measurable disturbance. In that case, we can either abort the transmission, or if the disturbance is not to big, as we will see, narrow very precisely how much information the spy gained, and transmit key safely, in what is known as QKD. Note that even though such key can be kept secret, provided the laws of QM are correct, that does not by itself authenticate the parties sharing secrets. That has to be still realised, as said, by classical means.

At this point, we shall not go too deep into details of actual QKD implementations, as we will address so in Chapter 3, starting by the milestone that was the Bennet-Brassard 1984 protocol (BB84) protocol [28]. For now, it will be sufficient to highlight how information is encoded in quantum states, giving some basic ideas regarding QKD, and advance what will come in the next section. Classicaly, we have bits, and a bit can be either in the state 0 or 1, thus encoding two possibilities, like a coin (one bit of information). In QM, we have qubits which in the so-called *computational basis*[3] may read

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{1.1}$$

In the expression above, one can make the correspondence between the classical bit with value 0 with the state $|0\rangle$, and the classical bit value 1 with the state $|1\rangle$. Crucially, the quantum state above is a superposition of said states, thus the bit information is encoded simultaneously. As such, it can be processed simultaneously. Such property endows quantum computers with great *parallellization* capabilities. Other encodings are possible; for instance, we may prefer to encode bit 0 as $2^{-1/2}(|0\rangle + |1\rangle$ and bit 1 as $2^{-1/2}(|0\rangle - |1\rangle)$. If one alternates between the two choices, any eavesdropper, as she cannot clone the states, will be forced to measure. Sometimes, she will make a mistake and will be discovered afterwards. This is the intuition behind the BB84 protocol, which shall be addressed in finer detail in Chapter 3.

1.2 Photonic implementations

QKD is not a mathematical device but rather the realization of a quantum channel that enables for keying material to be generated and securely exchanged. DiVincenzo's criteria [29] includes a couple of requirements for quantum communications, which argue for the need for *flying qubits* that can be both reliably sent and recovered across distances, and converted back-and-forth into *stationary qubits* (those the quantum computer uses for operations) by the appropriate interfaces [30]. As it is, *the photon is the natural implementation of a flying qubit.*

[3]Throughout this Thesis we will use various notations, but as more than one photon will sometimes be in a given state, and since those situations and many others are best treated with absorption and emission operators, we will mostly employ the occupation number, Fock state notation. This means that one should avoid confusing the computational 0 and 1 with the vacuum and the one-photon state.

The photon travels at the speed of light and does not easily decohere, so, while it is not, perhaps, the best candidate for performing operations inside a quantum computer [31], it is so for transmitting information. As optical communications are a mature field [32], this implies that QKD inherits (or may inherit) the bulk of this technology. Additionally, the language of QKD becomes that of quantum optics.

One can broadly distinguish here two kinds of optical communications, those which work in free space and those which are fiber based. The characteristics of the quantum channel are influenced by this fact. The intensive information needs of the present day make the existing optical fiber infrastructure crucial. From the data bandwidth perspective, there exists the need for both researching and deploying new kinds of fibers that can increase the amount of information that can be transmitted. One of such candidates is spatial division multiplexing (SDM). On the other hand, many of that information is confidential, thus the possibility of QKD in such fibers gains attraction. In an optical fiber, light is confined and only certain solutions of the Maxwell equations are allowed, defining *optical modes*. This notion is to be retained when dealing with the quantum aspects and thus, with QKD. It is a well-known fact that real fibers have imperfections that may perturb those optical modes in undesired ways. This is a source of problems: if optical modes are disturbed during propagation, encoded information gets *noisy*. Thus, the fiber link needs to be properly characterized, with the noise properly modelled while, if found to be big enough to obstruct QKD, some kind of perturbation palliation.

One of the advantages of working in this setting is, as said, that we already have a toolbox for good use, in terms of available lightwave technologies. QKD in fiber sytems (and free-space too) requires from photon production, detection and processing at various stages. In particular, fibers are highly compatible with *integrated photonic devices*, which are known to be fast, robust and stable [33, 34], allowing for miniaturization of certain stages of QKD protocols, and with many applications indeed in the broad field of quantum technologies, in contrast with the space consuming and reduced practicality and portability of bulk-optic components. Monolithic optical integration in glass substrates has been shown to be feasible, with applications in QKD for various purposes, aiding in the generation and detection of quantum states [138].

1.3 Towards real-life QKD

Although the ideas behind QKD are very promising, even urgent, given the foreseeable advent of quantum computers, there are still difficulties in order to *bridge the gap between theory and practice*. The following conundrum arises: if one wants to increase security, then the rate of exchanged information (the secret key rate) goes down. Thus, the more secure the protocol, the less practical it is [14].

QKD can be thought of as a physical layer for symmetric (one-time pad, AES) cryptography. The crucial aspect of this cryptosystem is that the adversary's information about the key needs to be arbitrarily close to zero. In other words, no information about the secret key can be leaked. In particular, this clearly affects the key distribution step, when the key is established between users at distant loca-

tions. The physical process of key distribution, *i.e* QKD cannot leak information. For this to happen, all the devices, including sources, detectors, phase modulators and a huge etc, the fiber links... need to be properly characterised so no sensible information is inadvertently disclosed to the eavesdropper.

Now, all such hardware elements are described in terms of physical models, which often introduce assumptions and simplifications. This has the risk that some of the physics is not accounted for in the model, and precisely that may translate into a vulnerability. Examples of this can be found in the literature, where QKD systems were *hacked* exploiting failures of the models use, because they did not account for more realistic physical behaviour of the hardware components [35].

Thus, there is work to do in order to ensure that QKD protocols, although safe in theory [36], are safe in reality. Effort can go (at least) in two directions. The first one is to be more and more accurate with the physical descriptions, model imperfections and play the devils' advocate, looking for ways of hacking the systems, thus countermeasures (albeit specific) can be implemented. On the other, try to design QKD protocols so their security does not rely on the knowledge of the devices, which is never full. These two approaches complement each other, because where reliance on the devices is unavoidable, it is better to have them well characterized. However the second approach is more robust, as the security is built-in the protocol and not model dependent. In this sense, progress is being made. Protocols that do nor rely on active elements for information encoding are being developed [37, 38], along with QKD schemes that do not require the measurement devices to be trusted (Measurement-Device-Independent (MDI)-QKD) [15]. The main drawback these have is the comparatively lower key rate. Twin-field QKD [39] provides a significant upgrade in this aspect, retaining MDI characteristics while reaching longer distances, surpassing the PLOB bound [40] providing an scaling of the key rate as if the link made use of a single quantum repeater, and being the basis for current fiber-optic QKD distance records [41]. Other improvements are stronger in the sense of less dependence on the devices [42], but they are much more challenging, in the practical sense. Protocols that make use of entangled sources [43, 44] are also more robust regarding attacks on the source, but production and transmission of entangled photons is not easy, also affecting practicality. Note that even though distance is a limitation, and lots of efforts are directed to upgrade QKD performance in this aspect, improvements in QKD in more modest distances, like those of a metropolitan network, are (and had been) taking place, the challenge here being the integration of the quantum protocols within the classical infrastructure [45, 46, 47].

1.4 Objectives and methodology

To sum up, QKD has seen fruitful development, but there is still a big room for improvement. In this Thesis we have focused on a small patch where to conduct our efforts. As we already laid out, one of the problems of real-life QKD, with real-life devices, is the drop on the key rate, compared to more theoretical, ideal protocols. The feasibility of QKD is often the center of its problematic: QKD is recognized as a method to provide with very strong security, but its application to realistic

telecommunication networks is a huge challenge. To argue thus for feasibility, we want, with this Thesis, to design schemes that improve QKD's practicality, in terms of rate of information that can be exchanged while at the same time retaining or improving security.

In particular, we wanted to design protocols that can be implemented with the current and/or foreseeable fiber-optic infrastructure. *Current infrastructure* on the one hand because of cost-effectivenes, but *foreseeable infrastructure* because, as society needs from vast circulation of information, and thus improved optical communications, deployments of fibers with bigger information capacities are and will happen in the near term. Being able to perform QKD over these fibers is hence an opportunity that want to exploit in this Thesis.

In order to do so, we have analysed the state of the art and found where QKD protocols[4] allowed for a plug and play-like version. We have centred our efforts in MDI-QKD and entanglement-based QKD. We have described light circulation and hardware specifics for implementation of such protocols in multicore (multicore fiber (MCF)) and few-mode (few-mode fiber (FMF)) fibers, as well as in the more familiar polarization encoding in single-mode fibers (SMFs). All that endowing the protocols with passive systems to undo information scrambling due to fiber perturbations.

To stablish that opportunity of improvement, we have quantitatively modelled errors due to fiber perturbations along two alternative routes: heuristically and from a probabilistic noise model approach, by assuming perturbations can be described by unitary matrices with random coefficients. To show the advantages of the autocompensation methods, we carried out security analysis, showing an increase of the overall key rate and achievable distance when autocompensation is implemented. This aimed to address, we insist, and in a realistic manner, one of the most acute problems of QKD, which is the low rate of secret communication.

At the same time, we have put through microfabrication of devices that are oriented for future QKD purposes, performing basic operations. In particular, building on previous work on directional couplers in glass [48], we have studied phase shifters. Those, in combination with the aforementioned structures, can be used to perform any single-qubit operation. The line of reasoning for this is the following: as seen, optical integration arises as a cost-effective, fast and stable method to process information encoded in photons. Thus, our objective was to contribute, albeit modestly, in this aspect, by exploiting the application of photonics to QKD, given its notable compatibility with optical fibers, and clear advantage over bulky, optical table experiments, therefore advancing future scalability and robustness of QKD implementations, hence feasibility. On a smaller scale, and in purely theoretical terms, with the objective of refining the quality of integrated optical devices for optical information processing in the QKD sense, we proposed photonic elements in order to generate topological phase gates in one qubit as well.

For the experimental part, the methodology consisted on surveying the literature, in order to find the most suitable way of matching the phase shifters with the rest of the waveguide, by means of adiabatic tapers. Then, integrated structures

[4]Some specific, albeit general, classes of QKD protocols, as the diversity of approaches is huge.

of the Mach-Zehnder interferometer (MZI) where devised, sampling various phase-shifting lengths. The optical chip those fabricated, by means of already established photolithography and ionic exchange. The resulting waveguides were subject to two stages of characterization: phase retrieval with an optical microscope and laser characterization by a prism-coupling setup made ad-hoc for the samples.

1.5 Thesis outline

This Thesis is organized in six segments. The first one is almost entirely introductory, motivating the research conducted for this Thesis, explaining the methodology of said research, and laying out the field's state-of-the art relevant to the Thesis. The second part (Chapter 2) contains a basic description of important pieces of optical hardware we will require for the rest of the Thesis, and outlines the theoretical framework we will work on. This is supplemented with some research results obtained in this area. Mainly, we show some schemes for photon generation adapted to our needs, as well as results on a integrated device we developed for generating geometric phases of possible use in quantum information processing and in particular QKD. In Chapter 3, we show results obtained in the context of autocompensating measurement-device-QKD. After a preliminary introduction containing some relevant notions on QKD, we describe the protocols in detail, making full use of the hardware devices from Chapter 2, and discussing their performance. in Chapter 4 we present results on microfabrication of proof-of-principle devices that are intended for their future use in QKD. In particular, we fabricated phase-shifters to be used in conjunction with directional couplers (DCs). We show in detail the steps of the process, involving design, photolithography and ion-exchange (Ionex), as well as the characterization results, plus an ad-hoc prism-coupling setup we developed. In Chapter 5, following a similar path than in Chapter 3, we study autocompensation in entanglement-based QKD. We give an alternate model of the perturbations effects than in Chapter 3, and propose a protocol that inherently solves problems associated with entanglement-based QKD when fiber perturbations are present. We conclude the Thesis by giving a summary of the results obtained and outlining possible future improvements.

Chapter 2

Optical hardware for QKD

This Chapter is related to the following articles the author has contributed to (found at the end of this document, in Appendix D): a) it cites extensively [49]; and b) it includes significant content based from results in [50].

QKD in optical fibers is an intricate communication process involving various (coordinated) tasks. One has to generate photons send them through fibers, with some alterations in their journey, like the action of optical gates for autocompensation, for instance to be finally detected. This requires from appropriate detectors, and often from certain preprocessing, like for example Bell state discrimination.

On top of that, there is a number of ways of encoding information in such photons, as there are various accessible d.o.f. Each of them has its advantages and disadvantages. Throughout this Thesis, various encodings will be considered. The most studied and common one is polarization. Both free-space and guided photons have two possible polarizations, constituting a Hilbert space of dimension two optimal for quantum endeavours. In the case of guided light, one ordinarily refers to this as transverse electric (TE) and transverse magnetic (TM) polarizations. We also have the time-bin encoding, where bit values are assigned depending on the pulses time-of-arrival. We will not use it in this Thesis. We may mention that while it is robust against polarization drift and fiber undesired birefringence, it comes with its own set of disadvantages [51]. It is still of widespread use.

New kinds of fibers, designed to avoid the so-called *capacity crunch* of single-mode fibers [52], offer the possibility of exploiting additional d.o.fs. In particular, FMFs allow for encoding in spatial Hermite-Gauss (HG) modes. On the other side, MCFs allow for dual-rail encoding, which assigns different bit values to the different paths (fiber cores) travelled by the photons.

All of the above means that we have a diversity of implementations of QKD in optical fibers, and that diversity translates directly to hardware specifics. In this chapter, we shall lay out the subset of such hardware that is relevant to us, and also

describe some results obtained on the matter.

2.1 Bulk optic elements for QKD. Quantum optics and devices.

In this Section we give a short catalogue of some basic discrete optical devices that are necessary to perform various tasks in the QKD protocols we will later consider. All of them are treated in the realm of non-relativistic QM, and, in particular, within the framework of non-relativistic quantum optics.

2.1.1 The Beam-Splitter

The first one is the ubiquitous *beam-splitter (BS)*, which is a basic building block used for many purposes, not only at the quantum state generation level or quantum state detection (for instance, Bell state analysers) but also for other intermediate quantum optic processing tasks.

To understand how a BS works, we first need to start by briefly outlining the quantization of the electromagnetic (EM) field [53]. The standard procedure consists on, first, obtaining the classical Hamiltonian of the EM field. Then canonical variables ("position" and "momentum") are introduced, and the Hamiltonian becomes that of the harmonic oscillator (or a set of harmonic oscillators). The canonical variables are promoted to operators and then annihilation and creation operators are introduced, which in the quantum optics field are called *emission* and *absorption* operators. These operators describe optical modes and photons are interpreted as excitations of these modes [53]. An emission operator $a^\dagger$ representing a given mode creates a photon in such mode, thus a photon is emitted in that mode. An absorption operator a, representing a given mode, annihilates/absorb a photon in such mode. The EM field is described in terms of modes and the interactions (transforms) between them. This means we can formulate such interactions in the Heisenberg picture. Different devices imply different transforms between modes, which are normally obtained from the classical theory by application of the correspondence principle.

For the case of the BS, if we represent the input modes by a and b, then the corresponding unitary, photon number preserving transform is [54]

$$U_{BS} = e^{i\xi(a^\dagger b - b^\dagger a)}, \tag{2.1}$$

where the value of ξ depends on the specific physical characteristics of the BS. Introducing Eq.(2.1) into the Heisenberg equations gives a discrete transform between the input modes (a, b) and the output modes (let's call them c, d) [53, 55]

$$\begin{pmatrix} c \\ d \end{pmatrix} = U_{BS}^\dagger \begin{pmatrix} a \\ b \end{pmatrix} U_{BS}, \tag{2.2}$$

which can be easily written in matrix form as [53]

$$\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} t' & r \\ r' & t \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \tag{2.3}$$

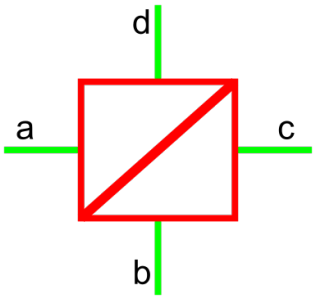


Figure 2.1: *Beam-splitter basics. Two incoming modes get transformed into two output modes. If only one beam impinges on it, the other input port* must *be put to a vacuum. Not doing so implies that the quantum treatment of the device would be incorrect (the canonical commutation relations between absorption operators would not hold).*

where the coefficients t, r, r', t' need to verify the appropriate conditions so as the commutation relations between emission and absorption operators are maintained [53].

The concrete values of the matrix entries depend, again, on the specifics of the BS. Throughout this Thesis, we shall use various types of BS for different purposes, we shall write the concrete form of the transformations in each case.

2.1.2 Polarization encoding

A popular encoding in the field of quantum information and, in particular, QKD, is the polarization encoding. The polarization degree of freedom of a photon means that we have a two-level system isomorphic to spin-$\frac{1}{2}$, which is also a usual platform for quantum applications. A particular case of BS is then of use: the *polarizing beam-splitter (PBS)*, which acts like a BS but now the coefficients in Eq. (2.3) exhibit polarization dependence. A typical PBS, which is the one we shall use, blocks a particular polarization on each direction. That means that we have now a device that can sort polarization modes. For instance, an incoming H-polarized photon will emerge in one port, while a V-polarized photon would emerge in the other. If each port is redirected to a different detector then the combined device is able to identify the polarization of a photon. Evidently, if the photon is in a superposition, the result will be random, with the probabilities given by the correspondent square amplitudes. However, other devices, which we shall describe soon, can map polarization states into the canonical pair H, V, thus we will be able to sort those polarization states.

In order to (passively –if actively, we would have Pockels cells [56]) map polarization states into polarization states, which is something required for various tasks, like detection or autocompensation, the next important bulk optic device is the *waveplate*. Specifically, it will be enough to single out the half-wave plate (HWP). It implements the following transform [57]

$$\begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}, \tag{2.4}$$

where θ is the angle between the waveplate fast axis and the horizontal direction

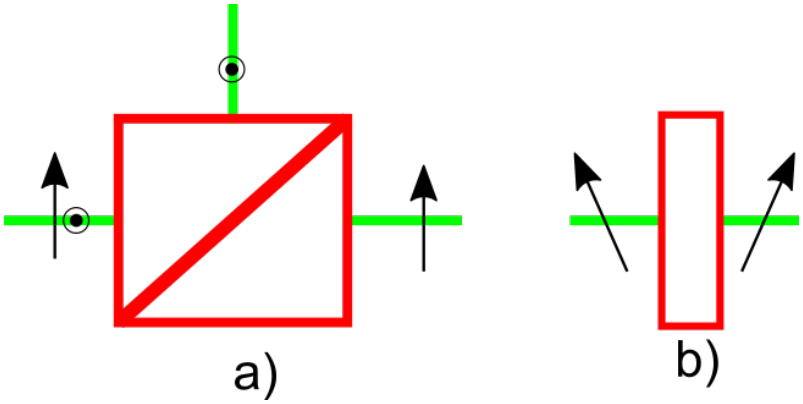


Figure 2.2: *Schematic representation of bulk devices for polarization encoding. a) polarizing-beam splitter and b) half-wave plate. The first can be used to sort polarization modes, while the latter to manipulate the polarization.*

(the convention is a right handed coordinate system of reference with the light propagating on the z-direction).

2.1.3 Spatial mode encoding

The three devices we have just described are canonical ones. The BS is perhaps the more versatile and relevant, the other two being used for polarization specific applications. Now, we move to a couple of bulk devices that can manipulate spatial *mode functions* of photons, which are the *Dove prism (DP)* and the *cylindrical lens converter (CLC)*.

By mode functions we refer to the transverse (with respect to the direction of propagation) amplitude shapes of the EM field, which photons inherit in the quantization process [58]. In fact, we saw that a emission/absorption operator is associated to a given mode. The operators are also associated to a certain mode shape [58]. The mode functions are relevant for quantum phenomena [59], and can be used for information encoding, being related to the orbital angular momentum d.o.f [58]. Indeed, a photon in a superposition of horizontal and vertical HG modes (with the same polarization) can be used as a proper qubit [58]. In particular, the following identification between the so-called computational basis and such encoding holds:

$$\begin{aligned} |0\rangle &\leftrightarrow |1_X\rangle \text{ Horizontal X HG mode} \\ |1\rangle &\leftrightarrow |1_Y\rangle \text{ Vertical Y HG mode} \end{aligned} \tag{2.5}$$

Is this encoding we will use when we investigate Autocompensating Measurement-Device-Independent Quantum Key Distribution (A-MDI-QKD) and entanglement-based QKD in FMFs in Chapters 3 and 5. The notions of horizontal and vertical refer to physical space and, in particular, to the positioning of the blobs in the intensity profiles of the HG modes.

A CLC consists on a couple of identical cylindrical lenses facing each other. A cylindrical lens focuses light only on one of the transverse directions, while on the

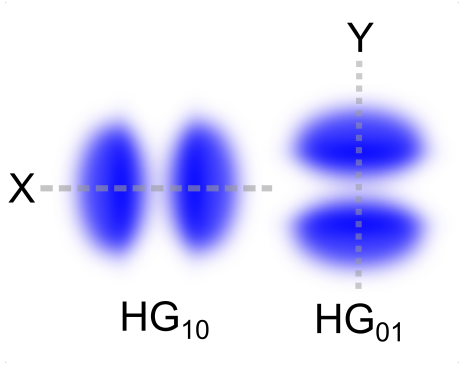


Figure 2.3: *Simplified illustration of the two order 1 HG modes. They have their intensity blobs in orthogonal orientations, and they are orthogonal themselves, thus they span a 2D vector space.*

other the propagation is free. If the lenses are situated a distance equal to $\sqrt{2}f$ (and rotated $\pi/4$), being f their focal length, then the corresponding transform is a $\pi/2$ phase gate

$$\begin{pmatrix} 1 & 0 \\ 0 & \pm i \end{pmatrix}, \tag{2.6}$$

where the sign depends on if the converter is rotated $\pi/4$ or $-\pi/4$. As such, this is know as a $\pi/2$-CLC. This rotation is along an axis perpendicular to the propagation direction, with X and Y coordinates defined by the symmetry axis of HG modes of order one (see Figure 2.3).

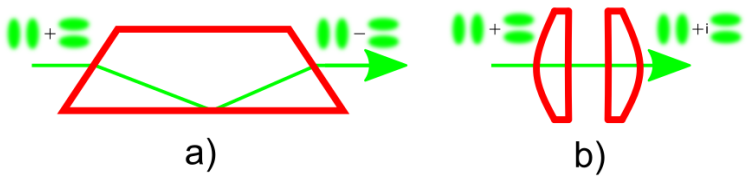


Figure 2.4: *Schematic representation of bulk devices for spatial mode encoding in few-mode fibers. a) Dove prism and b) $\pi/2$-cylindrical lens converter. To illustrate them, a definite transformation between input and output is chosen.*

Arrangements involving various, sometimes rotated, $\pi/2$-CLC can be used to implement other operations along π-converters [58] and DPs. This device is a prism which is cut in such a way that its input and exit faces (with respect to the direction of propagation) form an angle relative to the vertical direction. When working with the HG modes we have seen, a DP implements the following rotation

$$\begin{pmatrix} \cos 2\Omega & \sin 2\Omega \\ \sin 2\Omega & -\cos 2\Omega \end{pmatrix}, \tag{2.7}$$

where the angle Ω corresponds to the angle of rotation of the prism's normal. The DP has the inconvenience of altering the the polarization of the incoming beam [60]. As a consequence, polarization sensitive applications may require from additional devices to restore back the polarization state. The polarization transformation is

deterministic, so it is only a matter of hardware to bring it back to the original state. An alternative route is to use other combinations of CLCs could be used instead of a DP, or even combinations of DP are enough, without any CLC involvement, as shown in Chapter 5. We may mention that in specific applications where the DP intervenes, like a MZI for mode-sorting, the whole system can be also substituted by a Michelson-like interferometric arrangement [61], though we will not make use of this here.

2.2 Integrated photonics for QKD. Quantum optics and devices.

We have seen bulk devices and how to model their interaction with photons. Now it is the turn of integrated components which have some nice properties that justify their use, as we have seen.

The intuition behind integrated optics or even photonics, making an emphasis on applications dealing with the particle nature of light, is confinement by total internal reflection (TIR). An integrated structure consists on a region of given index (core, film if it is planar) which is greater than its surroundings (cladding, substrate). By TIR, light launched with the appropriate range of angles into the core gets trapped, travelling along the core forever. Thus, a waveguide has been formed. This behaviour is easily understood within a geometric-optic zig-zag model [62]. The refractive index distribution of the structure may be arbitrarily complicated. This, together with the values of the indexes will determine the properties of the structure.

For most cases, however, the zig-zag model is not enough to capture the physics of waveguides. In fact, EM theory is required. Solving Maxwell equations, taking into account the material properties of the structure and the restrictions it introduces, one can obtain a set of allowed solutions for the EM field called *modes*. By computing the modes, one can describe any state of light propagation in the waveguide. If the structure is simple, they can be obtained analytically, but in most cases this is not possible, and has to be done numerically. Depending on the structure dimensions and index values, the number of propagating modes is different. Often, one is interested in designing the waveguide in such a way that only a mode propagates (single-mode behaviour).

So far, we have briefly described integrated optics in the classic realm. However, we need to understand how the quantum particles of light, the photons, propagate along such structures. We shall work in a non relativistic quantum optics framework, as we did with bulk optic devices. Now, the problem is best suited to work not with the quantized Hamiltonian of the EM field, but its (quantized) *Momentum Operator M* [63, 64]. This will not give the time evolution of the modes, which will be promoted to emission and absorption operators, but rather the *spatial* evolution along the structure. In other words, along the direction of propagation, which is conventionally chosen to be the $z-$direction.

The spatial evolution of the field operators $\hat{a}_n$ is given by the appropriate Heisen-

berg equations, where in this case the Hamiltonian has been properly substituted by the Momentum operator

$$-i\hbar\frac{\partial\hat{a}_n}{\partial z} = [\hat{a}_n, \hat{M}]. \tag{2.8}$$

The Momentum operator contains all the relevant information to understand light propagation. For instance, interactions (couplings) between modes. When they are small, which is a realistic condition, one would classically apply coupled mode equations. In virtue of this approximation, one takes the unperturbed modes and expands the actual modes in terms of them, with amplitudes depending on the propagation distance (usually the z-coordinate). The coupling is then described as a set of coupled ordinary differential equations involving such amplitudes. If only two modes are present then there are two of these amplitudes or coefficients.

Expanding this equation we end up with [62]

$$-i\hbar\frac{\partial\hat{a}_n(z)}{\partial z} = \hbar\tilde{\beta}_n\hat{a}_n(z) + \hbar\sum_{n\neq m}^{N}\kappa_{nm}\hat{a}_{mq}(z), \tag{2.9}$$

where the sum involves N modes. Also, although we typically omit the hat, we retain it here to emphasize that they are operators.

Now we explain the quantities involved in the equation above. The function κ_{nm} is the linear coupling coefficient between modes n and m, and its given by a overlap integral involving the mode electric field distributions and the perturbation, expressed as a function of x and y coordinates:

$$\kappa_{nm} = \int P(x,y)e_n(x,y)e_m(x,y)dxdy, \tag{2.10}$$

implying that we are considering modes confined in both x and y directions, as in the case of a channel waveguide (or an optical fiber), which is the main wave-guiding configuration throughout this Thesis. Importantly, when writing the coupling coefficient like this, we are considering here a small interval z where the perturbation *does not depend* on z. Note that the quantity $\tilde{\beta}_n = \beta_n + \kappa_{nn}$ contains already the self-coupling term κ_{nn} of the mode n with itself, apart from the free propagation constant β_n.

With this theory laid out, we can now describe one of the most basic and relevant devices, which we shall use extensively along this Thesis: the *dc*. In essence, a DC consists on two (single-mode) waveguides that are initially far apart, so no modal coupling between exists, but they are then brought close to each other. In such situation, the evanescent tails of the modal fields overlap, and there is power transfer between the waveguides or, in other words, mode coupling. In quantum terms, we have a linear momentum operator involving the free modes and a coupling term [48]

$$M = \hbar\beta_1 a_1^\dagger a_1 + \hbar\beta_2 a_2^\dagger a_2 + \hbar\kappa_{12} a_1^\dagger a_2^\dagger a_1 a_2. \tag{2.11}$$

From here, solving the Heisenberg equations, we end up with a nice 2x2 matrix representing the action of the DC

$$\begin{pmatrix} \cos\kappa d & i\sin\kappa d \\ i\sin\kappa d & \cos\kappa d \end{pmatrix}, \tag{2.12}$$

where κ is the coupling strength, which involves both the coupling coefficient κ_{12} and the different between the modal propagation constants, and d is the coupling length, *i.e* the effective distance where the waveguides are close together.

The DC is a basic building block for linear quantum information processing with photons. It can be thought of as an integrated version of the BS beam-splitter, and thus, it inherits the versatility of this bulk optic counterpart. DCs can be used at state generation (combined with a source), for autocompensation or for detection (as a preprocessing device). DCs can be arranged in a cascaded manner, enabling, for instance, to aid in projective measurements for Bell state detection, and also high-dimensional QKD [48] or applied in the context of reference-frame-independent QKD [65].

2.2.1 Phases and DCs as universal gates for single-qubit operation

The DC is not the only integrated device we need. Often, we need to introduce phase differences, for various motives. If we want to encode information this way, normally we need an active element, such as a phase modulator (PM). This is because the phase needs to be adjusted at will, randomly indeed, if we want to generate the various states of a given basis. However, sometimes we are required to introduce a fixed phase. For instance, we shall see autocompensating circuits where we need phases for producing the desired transforms, specifically, matrices like

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{2.13}$$

which requires a π phase difference between the corresponding vector components (for instance, two fiber modes). To sum up, we need *phase gates*.

Moreover, what is important is that such phase gates, together with the operation a DC performs, are enough to achieve single-qubit universal quantum computation [66, 67]. Specifically, the Hadamard gate (which can be achieved with a DC and phases) and phase gates are a universal set of single-qubit gates. Thus, we rephrase and particularize: with DCs and phase gates we can build any integrated-optic implemented operation on a fiber mode.

Note that the devices we have been describing above were aimed at this very objective. With DPs and CLCs we can operate at will with mode function encoded qubits. And with HWPs and quarter-wave plates (QWPs) (that we have not mentioned, but because will not directly use them in what follows), one can achieve universal computation for polarization qubits.

The question now is how to practically obtain phase gates. The straightforward answer to this question is to induce a controlled change in the optical path of the

mode. Such quantity is given by

$$\phi = n_{eff}\Delta z, \tag{2.14}$$

where n_{eff} is the effective refractive index of the wave-guiding structure, and Δz is the propagation length along which the mode sees a refractive index equal to n_{eff}.

Hence, there are, at least, two ways of introducing a phase change. First, modifying Δz, however we are aiming for miniaturization, so we want everything as small as possible. Another option is to change n_{eff}, which is quite feasible. It is enough to change the width of a waveguide, in a controlled manner, to modify the effective refractive index. This is the route we will take in Chapter 4 when we design and probe our glass-integrated phase shifters.

2.2.2 Some preliminary results on geometric phases in integrated structures as phase gates.

In addition to this, there is a third possibility that profits on the fact that we can also generate *geometric* phases with photonic structures. Note that controlling Δz, as in the Eq. (2.2.1) above, is very complicated, in the sense of doing it precisely. Controlling the change of the refractive index is more predictable (depending on the method to do it, in our case, ion exchange is very reproducible), but is not without complication. This suggests the need for more robust phase-shifting. Geometric phases arise thus as a very good option to this matter, albeit challenging, as we will see.

The geometric phase, re-discovered by Berry [68] and further generalized by Aharonov and Anandan [69], is a phase that is not acquired over mere temporal or spatial evolution, like the *dynamical* phase. Given some (in our case, quantum) system, the overall accumulated phase during evolution can be factorized a sum of a dynamical contribution and a geometric contribution. The dynamical one we are more used to: for instance, in a MZI the phase difference because of a different path length is dynamical. The geometric phase however, arises from aspects related to the overall structure, say, or *topology* of the system evolution. For instance, in the usual formulation of the Berry phase [68], it comes from a slow (adiabatic), cyclical variation of the Hamiltonians parameters. Meanwhile, the generalization of Aharonov-Anandan implies that the geometric phase does not require the evolution adiabatic. The corresponding geometric phase is usually called Aharonov-Anandan phase (AA-phase).

The best known example of a system exhibiting AA-phases is a spin-$\frac{1}{2}$ particle interacting with a magnetic field [70]. We shall use this fact to obtain analogous AA-phases in integrated structures, by imitating such mechanical system. This means, in general, as we have shown [50], that the photonic structure is an *analog simulator* of the spin-magnetic system (note, for the sake of completeness, that it also simulates the interaction of an atom with a classical electric field).

We shall focus here on the particular application of achieving geometric phases, which then may be used for QKD purposes. The reason why this would be desirable lays in the properties of the geometric phase itself. Although the device we will

propose its somewhat complicated involving a two-mode planar waveguide and an integrated grating with sinusoidal period, the nature of the AA-phase protects it against disturbances. Computation with geometric phases has already been investigated in spin-magnetic systems [67], even achieving two-qubit gates. We want to work in this direction (albeit up to one qubit), by precisely exploiting this analogy between the photonic device and the spin-magnetic system.

The photonic device consists in a two-mode slab waveguide with a grating on it. Although channel waveguides could be used, the slab waveguide is enough. The latter is a well-known integrated device, easy to fabricate and characterise, compared to the former. The index profile of the structure is not specified, but it is given by a function $n(x)$ of the depth coordinate x (it could be gradient refractive index (GRIN) or step-index), while the lateral direction lays along the y direction. The grating, on the other side, is situated along the direction of propagation (z, as usual), according to Figure 2.5.

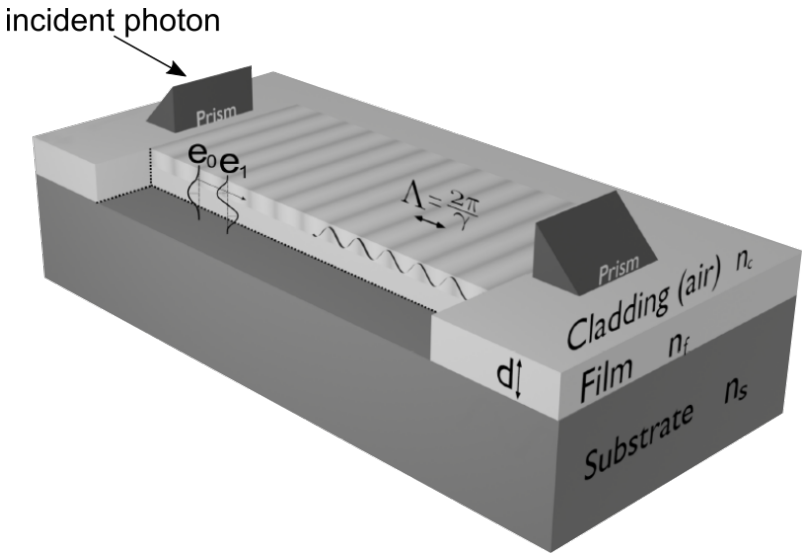


Figure 2.5: *Scheme of the integrated structure for geometric phase generation. It consists on a two-mode slab waveguide with a periodic grating on it. Prisms at the input and outputs provide for coupling with the exterior, although fibers could be employed also. Reproduced from own contribution [50].*

The two modes (call them 0 and 1) are coupled by the grating, which consists on a periodic modulation of the refractive index. This will be analysed in the context of coupled mode theory, as we have seen, where the free modes are assumed to be perturbed by some variation of the electric permittivity. In this case, we model this effect as

$$\Delta\epsilon(x, z) = \Delta\epsilon(x)\cos(\gamma z), \tag{2.15}$$

expressing the periodicity on the propagation direction, modulating a fixed variation of the index in depth. In the expression above, γ is the period of the grating. Some initial phase could be taken into account also, but it can be put to zero by proper fabrication adjustments.

We can directly apply Eq. (2.9). The coupling coefficients of Eq.(2.10) become

$$C_{ij}(z) = \frac{\omega}{2} \int \Delta(x,z) e_i(x) e_j^*(x) dx \tag{2.16}$$

where ω is the temporal frequency of the modes. In this particular case, we may factorize the z-dependence

$$C_{ij}(z) = \cos(\gamma z) \bar{C}_{ij}, \tag{2.17}$$

where $\bar{C}_{ij} = \int \Delta\epsilon(x) e_i(x) e_j^*(x) dx$.

As said, we have two coupled modes. Each mode is represented by the corresponding operator (emission and absorption). This enables for building the various quantum states, like usual.

For reasons that will become apparent later, we make the following transformation on the operators

$$A_j = a_j \exp(-i\beta_j z), \tag{2.18}$$

where b_j is the free propagation constant of the mode j.

With all the ingredients above we arrive at the following pair of coupled equations

$$\begin{aligned} -i\frac{dA_0}{dz} &= \bar{C}_{00} \cos\gamma z A_0 + \bar{C}_{01} e^{-i(\beta_0-\beta_1)z} \cos\gamma z A_1, \\ -i\frac{dA_1}{dz} &= \bar{C}_{11} \cos\gamma z A_1 + \bar{C}_{10} e^{i(\beta_0-\beta_1)z} \cos\gamma z A_0. \end{aligned} \tag{2.19}$$

Now, we assume that γ is big enough so the cosine term is rapidly oscillating. In other words, it averages to zero. That automatically kills the self-coupling terms, and the cross terms become

$$\begin{aligned} \bar{C}_{01} e^{-i(\beta_0-\beta_1)z} \cos\gamma z &\to \frac{1}{2} \bar{C}_{01} e^{-i(\Delta\beta-\gamma)z}, \\ \bar{C}_{10} e^{i(\beta_0-\beta_1)z} \cos\gamma z &\to \frac{1}{2} \bar{C}_{10} e^{i(\Delta\beta-\gamma)z}, \end{aligned} \tag{2.20}$$

where we have defined $\Delta\beta = \beta_0 - \beta_1$, which we assume to be of the same order as γ, and it is positive as the fundamental mode has a bigger value of the effective refractive, and by definition $\beta = k_0 n_{eff}$. Note that $\Delta\beta$ being bigger is a valid assumption. Even a slight difference (say, order of 10^{-3}) on the effective refractive index leads to considerable values of $\Delta\beta$, due to k_0 being inversely proportional to the wavelength, which is a really small number. Moreover, noting that the coupling coefficients are symmetric, then we have $\bar{C}_{01} = \bar{C}_{10} = C$.

Thus, from Eq. (2.19) we get to the intermediate expression

$$\begin{aligned} -i\frac{dA_0}{dz} &= \frac{\bar{C}}{2} e^{-i(\Delta\beta-\gamma)z} A_1, \\ -i\frac{dA_1}{dz} &= \frac{\bar{C}}{2} e^{i(\Delta\beta-\gamma)z} A_0. \end{aligned} \tag{2.21}$$

We make yet another transformation of the operators, so we separate back γ from the propagation constants. We define

$$\begin{aligned} A_0 &= b_0 e^{-i\Delta\beta z/2}, \\ A_1 &= b_1 e^{i\Delta\beta z/2}. \end{aligned} \tag{2.22}$$

Introducing this into Eq. (2.21) we arrive at

$$\begin{aligned} i\frac{db_0}{dz} &= -\frac{\Delta\beta}{2}b_0 - \frac{C}{2}b_1 e^{i\gamma z}, \\ i\frac{db_1}{dz} &= \frac{\Delta\beta}{2}b_1 - \frac{C}{2}b_0 e^{-i\gamma z}. \end{aligned} \tag{2.23}$$

Recall that these are the Heisenberg equations for the mode operators B_0 and B_1. If the operators are the ones that evolve, it is useful to put them into a two-row vector $[b_0, b_1]^t$. Then the Heisenberg equations can be written in matrix terms as

$$i\frac{d}{dz}\begin{pmatrix} b_0 \\ b_1 \end{pmatrix} = -\frac{1}{2}\begin{pmatrix} \Delta\beta & Ce^{i\gamma z} \\ Ce^{-i\gamma z} & -\Delta\beta \end{pmatrix}\begin{pmatrix} b_0 \\ b_1 \end{pmatrix}. \tag{2.24}$$

Now, note two things. First, that the original mode operators a and b are related by a global phase $a_j = b_j \exp i(\beta_0 + \beta_1)z$ $(j = 0, 1)$. Second, that when dealing with single-photon states mode operator evolution can be directly translated to state evolution. For the sake of the argument, consider the free evolution case: $a(z)|0\rangle = a(0)e^{i\beta z}|0\rangle = e^{i\beta z}|1\rangle$. Hence Eq. (2.24) can be written as

$$i\frac{d}{dz}|L(z)\rangle = -\frac{1}{2}\begin{pmatrix} \Delta\beta & Ce^{i\gamma z} \\ Ce^{-i\gamma z} & -\Delta\beta \end{pmatrix}|L(z)\rangle, \tag{2.25}$$

where $|L(z)\rangle$ (L for light) is the superposition $L(z) = b_0(z)|1_0\rangle + b_1(z)|1_1\rangle$, with the former operators b now demoted to z-dependent coefficients, as now the states are the ones evolving in space.

If we multiply on both sides by $\hbar$ we can write Eq. (2.25) in terms of the momentum operator in a very compact form

$$-i\hbar\frac{d}{dz}|L(z)\rangle = -M(z)|L(z)\rangle, \tag{2.26}$$

with $M(z)$ the momentum operator.

Eq. (2.25) is greatly simplified if we move to a rotating reference frame at a speed γz, *i.e* use the transform $U(\gamma, z) = e^{-i\sigma_3\gamma z/2}$, where σ_3 is the third Pauli matrix. Under such circumstance, the momentum operator, acting on the 'static' state $|l(z)\rangle = U(z, \gamma)|L(z)\rangle$ becomes

$$M' = -\frac{\hbar}{2}\begin{pmatrix} \Delta\beta - \gamma & C \\ C & -\Delta\beta + \gamma \end{pmatrix}. \tag{2.27}$$

Now the spatial evolution of state $|l(z)\rangle$ is simple, as the momentum operator is a constant

$$|l(z)\rangle = e^{\frac{i}{\hbar}pz}|l(0)\rangle, \tag{2.28}$$

where p will be the momentum eigenvalue. We end up with the eigen-problem $p|l(0)\rangle = -M'|l(0)\rangle$. Computing the eigenvalues gives

$$\pm p = \pm\frac{\hbar}{2}\sqrt{(\Delta\beta-\gamma)^2+C^2}, \tag{2.29}$$

and the corresponding eigenvectors

$$\begin{aligned} |l_+(0)\rangle &= \cos\frac{\alpha}{2}|1_0\rangle + \sin\frac{\alpha}{2}|1_1\rangle, \\ |l_-(0)\rangle &= \sin\frac{\alpha}{2}|1_0\rangle - \cos\frac{\alpha}{2}|1_1\rangle, \end{aligned} \tag{2.30}$$

where α is an angular variable given by

$$\alpha = \sin^{-1}\left(\frac{C}{\sqrt{(\Delta\beta-\gamma)^2+C^2}}\right). \tag{2.31}$$

Now we have the necessary ingredients to see how geometric phases are generated. First, recall, from what we have seeing, that the full evolution of the original states $|L(z)\rangle$ is given by

$$|L_\pm(z)\rangle = e^{i\sigma_3\gamma z/2}e^{\pm\frac{i}{\hbar}pz}|l_\pm(0)\rangle. \tag{2.32}$$

The two exponential operators commute, so we can move the rotation next to the state and compute. Letting the resulting state evolve for n grating periods $\Lambda = \frac{2\pi}{\gamma}$ we obtain

$$\begin{aligned} |L_+(n\Lambda)\rangle &= e^{\frac{i}{\hbar}pn\Lambda}\left(e^{in\pi}\cos\frac{\alpha}{2}|1_0\rangle + e^{-in\pi}\sin\frac{\alpha}{2}|1_1\rangle\right), \\ |L_-(n\Lambda)\rangle &= e^{\frac{-i}{\hbar}pn\Lambda}\left(e^{in\pi}\sin\frac{\alpha}{2}|1_0\rangle - e^{-in\pi}\cos\frac{\alpha}{2}|1_1\rangle\right). \end{aligned} \tag{2.33}$$

We can write, after a bit of manipulation

$$|L_\pm(n\Lambda)\rangle = e^{\pm\frac{i}{\hbar}pn\Lambda}e^{\pm in\pi}|l_\pm(0)\rangle. \tag{2.34}$$

What we have here is a cyclic evolution over n grating periods. After it, the input state has acquired a phase

$$\phi = \pm\frac{1}{\hbar}pn\Lambda \pm n\pi. \tag{2.35}$$

This phase will have a *dynamic* component and a *geometric* component $\phi = \phi_d + \phi_g$. To obtain the geometric phase we have to subtract the dynamic part from the total phase. The dynamic phase is given by [67]

$$\begin{aligned} \phi_d = \frac{1}{\hbar}\int_0^{n\Lambda}\langle L_\pm(z)|M(z)|L_\pm(z)\rangle dz &= \frac{1}{\hbar}\int_0^{n\Lambda}\langle l_\pm(0)|M|l_\pm(0)\rangle dz \\ &= \frac{1}{\hbar}\int_0^{n\Lambda}[\langle l_\pm(0)|M'|l_\pm(0)\rangle - \frac{\gamma}{2}\langle l_\pm(0)|\sigma_3|l_\pm(0)\rangle]dz \\ &= \pm\frac{1}{\hbar}pn\Lambda \pm n\pi\cos\alpha. \end{aligned} \tag{2.36}$$

From here, the geometric phase is

$$\phi_g = \phi - \phi_d = \pm n\pi(1 - \cos\alpha). \tag{2.37}$$

Thus, we have generated geometric phases with our integrated device. Now, we would be left with the important task of finding the way to eliminate the dynamical part of the phase while maintaining the geometric one. What happens is that Equation (2.37) is not useful by itself, as the full phase is still 'contaminated' by the dynamical phase. In other words, one would want to generate a phase that is purely geometric and therefore more robust, *i.e* $\phi = \phi_g$.

2.3 Optical fiber technology

We have seen how a waveguide works; the optical fiber is a special (and perhaps the most important) case of waveguide. In its basic form, a optical fiber is a cylindrical[1] piece of dielectric material of refractive index n_{co} (core) surrounded by another material of index $n_{cl} < n_{co}$ (cladding). If light is appropriately launched into the fiber[2] [32], it gets confined in the core. One can compute the modes of propagation, including linearly polarized (LP) modes in the weakly-guiding approximation [71]; and also coupling between modes of the same or different fibers, either artificial, by means of other devices, or due to imperfections, such as fabrication defects, twists and torsions etc. in the fiber.

As the modes of propagation are the allowed solutions for EM fields propagating in the fiber (Maxwell equations + boundary conditions), by tuning the design parameters of the fiber we can modify the number of modes that propagate, as we did with general waveguides. Typically, given some material properties, a small core will only allow the propagation of one mode, the fiber being a SMF. Actually, there are two modes, since there is one for each polarization, that can couple between themselves. If we make the core bigger, more modes are allowed, the fiber being a FMF.

The reason to introduce more modes is bigger capacity for information transmission, which is, ultimately, one of the main goals of optical fibers. Another option for bigger information carrying capabilities is to stack multiple cores into the same cladding. In that case we have a MCF. Ideally, a fiber may be designed so that there is little *cross-talk* (coupling) between the modes. Still, in general, under realistic conditions, we cannot rule out cross-talk. That, if appreciable, can scramble the information that is being transmitted. In the case of QM, as the photonic modes get coupled, being the encoding dependent on which core the photon is to be detected, cross-talk leads to noise (errors) in the communication. This, together with the phases acquired along each core, which may be different for each one of them (*phase drift*), are problems that we will tackle with the appropriate autocompensating methods.

[1] In general it is, in other case it is not. It may be elliptic, for instance.

[2] The input light angle needs to lie within the cone of acceptance of the fiber. When coupling into a single-mode fiber, the fiber mode needs to be matched to the input light's field distribution...

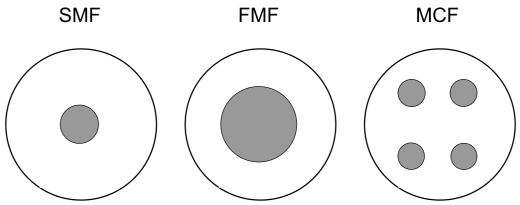


Figure 2.6: *Three types of fiber topology: SMFs, which only guide one mode. FMFs which have a larger core that can guide more modes, and MCFs, with multiple single-mode cores, thus increasing bandwidth. The core is the darker region.*

When propagating along a fiber, polarization modes may couple between them, and a photon that is initially H-polarized may become V-polarized at the end of its journey (for instance, at a detector). In quantitative terms, given a fiber with coupling coefficient κ and whose two fundamental modes propagation constants are given by β_H and β_V (the difference in the propagation constants is induced by birefringence); then coupling happens whenever $\Delta\beta = \beta_H - \beta_V < \kappa$. On the other side, this also means that there will be a phase difference (or phase drift) between polarization modes [72].

If we encode information in polarization, then such coupling amounts to noise in the communication protocol, as cross-talk in MCFs did. At this point, two solutions come to mind: the first one, use of polarization-maintaining fibers (PMFs), which have such a strong, built-in birefringence that the H-polarized mode and the V-polarized mode have such different propagation constants that coupling between them is very low [73]. If we purposely increase (by design) the value of $\Delta\beta$, then coupling is greatly reduced, thus polarization is conserved as long light is polarized along the required direction (principal axis). For other inputs, polarization does get scrambled along propagation. This solution requires the replacement of the existing fiber (if it is not PMF, which is very likely) with a PMF one. Other option, which we will favour here in this Thesis, is to introduce autocompensating devices in the already existing fiber architecture in order to mitigate such undesired effects. As said, for each spatial mode in the fiber there are two-polarizations. As they all can get coupled, we actually have four modes into consideration. In order to reduce this to two-dimensional problems, some assumptions need to be made, which amount to use fibers that need to be more specific (fibers that are at the same time MCF and PMF, for instance.)

The optical fiber is a classical device, but photons as quantum. Is the conjunction of an optical fiber with photons propagating in it that we term as a quantum channel. All this perturbation effects we have been mentioning translate directly to the quantum domain, as unitary transformations affecting emission and absorption operators and, as a consequence, quantum states. We shall consider two effects with regard to an otherwise free (albeit guided) propagation of the photon: attenuation and perturbations.

2.3.1 Model of fiber losses by means of a fictitious beamsplitter

In the case of attenuation, what is ordinarily done is to model the losses in the fiber as a fictitious BS located somewhere in the fiber, that sends a fraction of the photons out of the fiber to the environment [74]. Assume that we call $a_0^\dagger$ the emission operator of a photon on the fiber, i.e, the creation operator of a photon in a mode represented by a_0. This mode impinges on one port of the BS. In the other input port of the BS, we have the environment mode e_0, which starts in a vacuum. The transformation between the input ($a_0^\dagger$ and $e_0^\dagger$) and exit modes ($a^\dagger$ and $e^\dagger$) is the following

$$\begin{pmatrix} a_0^\dagger \\ e_0^\dagger \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ -\sqrt{1-\eta} & \sqrt{\eta} \end{pmatrix} \begin{pmatrix} a^\dagger \\ e^\dagger \end{pmatrix}, \tag{2.38}$$

where η represents the transmittance (additive inverse of the losses) of the fiber, which obeys the following law $\eta = 10^{-\frac{\alpha_{att} L}{10}}$, where α_{att} is the attenuation of the fiber, usually measured in dBs/km [decibels/km] and L is the fiber length.

This simple but useful model can be applied to any input state. Consider for instance that a single photon is travelling along the fiber. The input state is $a_0^\dagger|0\rangle = |1_{a0}0_{e0}\rangle = |10\rangle$. By the BS modal transformation, we have $a_0^\dagger \to \sqrt{\eta}a^\dagger + \sqrt{1-\eta}e^\dagger$. Thus, we have that the single-photon state becomes $|10\rangle \to \sqrt{\eta}|10\rangle + \sqrt{1-\eta}|01\rangle$, where now $|10\rangle$ means $|1_a 0_e\rangle$ and so on. Thus, a photon escapes to the environment with probability $1-\eta$. Now, in the density matrix formalism we have $\rho_{ae} = \eta|10\rangle\langle 10| + \sqrt{\eta(1-\eta)}|10\rangle\langle 01| + \sqrt{\eta(1-\eta)}|01\rangle\langle 10| + (1-\eta)|01\rangle\langle 01|$. Since we are interested only in the fiber, and not on the outside, we trace out the environment, producing the following mixed state

$$\rho_a = \eta|1\rangle\langle 1| + (1-\eta)|0\rangle\langle 0|. \tag{2.39}$$

This means that we are in a statistical mixture of a photon in the fiber with probability η and none with probability $1-\eta$. What happens if we launch a Fock state? (assuming independence between the n photons [75]). Proceeding in a totally analogous manner, taking into account that $|n_{a0}0_{e0}\rangle = (a_0^\dagger)^n|0_{a0}0_{e0}\rangle$, using Newton's binomial theorem and the fact that the partial trace kills the off-diagonal terms of ρ_{ae}, we obtain a n-photon Fock state transmittance $\eta_n = 1-(1-\eta)^n$. Indeed,

$$\begin{aligned} |n0\rangle &\to \frac{1}{\sqrt{n!}}(\sqrt{\eta}a^\dagger + \sqrt{1-\eta}e^\dagger)^n|00\rangle \\ &= \frac{1}{\sqrt{n!}}\sum_s^n \frac{n!}{s!(n-s)!}\sqrt{\eta}^{n-s}(a^\dagger)^{n-s}\sqrt{1-\eta}^s(e^\dagger)^s|00\rangle \\ &= \sum_s^n \sqrt{\frac{n!}{s!(n-s)!}}\sqrt{\eta}^{n-s}\sqrt{1-\eta}^s|n-s,s\rangle. \end{aligned} \tag{2.40}$$

Now,

$$\rho_{ae} = \sum_s^n \sum_t^n \sqrt{\frac{n!}{s!(n-s)!}} \sqrt{\frac{n!}{t!(n-t)!}} \sqrt{\eta}^{n-s} \sqrt{1-\eta}^{s} \sqrt{\eta}^{n-t} \sqrt{1-\eta}^{t} |n-s,s\rangle\langle n-t,t|. \tag{2.41}$$

Tracing over the environment means a Dirac delta δ_{sm} is to be introduced

$$\begin{aligned} \mathrm{Tr}_e(\rho_{ae}) = \rho_a = \\ \sum_s^n \sum_t^n \sqrt{\frac{n!}{s!(n-s)!}} \sqrt{\frac{n!}{t!(n-t)!}} \sqrt{\eta}^{n-s} \sqrt{1-\eta}^{s} \sqrt{\eta}^{n-t} \sqrt{1-\eta}^{t} |n-s\rangle\langle n-t|\delta_{st} \\ = \sum_s^n \frac{n!}{s!(n-s)!} \eta^{n-s}(1-\eta)^s |n-s\rangle\langle n-s|. \end{aligned} \tag{2.42}$$

The trace of this density operator is the unity, as it should: $\mathrm{Tr}(\rho_a) = (1-\eta)+\eta = 1$, as what we can readily obtain from the binomial expansion above. We can use this to compute what we are searching for. First, we make some rearrangements

$$\rho_a = (1-\eta)^n |0\rangle\langle 0| + \sum_s^{n-1} \frac{n!}{s!(n-s)!} \eta^{n-s}(1-\eta)^s |n-s\rangle\langle n-s|. \tag{2.43}$$

The trace of the second term is actually the n-photon state transmittance. So,

$$\eta_n = \sum_s^{n-1} \frac{n!}{s!(n-s)!} \eta^{n-s}(1-\eta)^s = \mathrm{Tr}(\rho_a) - (1-\eta)^n = 1-(1-\eta)^n, \tag{2.44}$$

which is what we wanted [75]. Note that if we set $n = 1$ in that equation, we recover the previous result.

If we ask about an input coherent state, we obtain a quasi-classical answer. The result is more easily obtained by means of the displacement operator. We know that we can write the input state as

$$D(\alpha)|0\rangle = \exp(\alpha a_0^\dagger - \alpha^* a_0)|0\rangle = |\alpha\rangle. \tag{2.45}$$

Now, putting the BS transformation here

$$\begin{aligned} |\alpha\rangle \to \exp\left[\alpha(\sqrt{\eta}a^\dagger + \sqrt{1-\eta}e^\dagger) - \alpha^*(\sqrt{\eta}a + \sqrt{1-\eta}e)\right]|0\rangle \\ = \exp(\alpha\sqrt{\eta}a^\dagger - \alpha^*\sqrt{\eta}a) \times \exp(\alpha\sqrt{1-\eta}e^\dagger - \alpha^*\sqrt{1-\eta}e)|0\rangle = |\alpha\sqrt{\eta}\rangle|\alpha\sqrt{1-\eta}\rangle, \end{aligned} \tag{2.46}$$

which can be done since a and e commute.

The corresponding density operator is

$$\rho_{ae} = |\alpha\sqrt{\eta}\rangle|\alpha\sqrt{1-\eta}\rangle\langle\alpha\sqrt{\eta}|\langle\alpha\sqrt{1-\eta}|. \tag{2.47}$$

Tracing over the environment, noting that $\mathrm{Tr}(|\alpha\sqrt{1-\eta}\rangle\langle\alpha\sqrt{1-\eta}|) = 1$, we end up with

$$\mathrm{Tr}(\rho_{\mathrm{ae}}) = \rho_a = |\alpha\sqrt{\eta}\rangle\langle\alpha\sqrt{\eta}|. \tag{2.48}$$

The mean photon number of a coherent state is the square of its amplitude. Thus, the initial state had $\bar{n} = |\alpha|^2 = \mu$, while the final state now has $|\alpha|^2\eta = \eta\mu$. This is, in average, a fraction η of the photons have been transmitted by the fiber, which is almost a classical result. Note that we have already introduced the usual notation in the QKD literature of calling μ to the mean photon number of a pulse. With this notation, one usually writes $\alpha = \sqrt{\mu}e^{i\phi}$.

2.3.2 Model of fiber perturbations

How perturbations affect information travelling optic fibers is a more difficult aspect to model than attenuation. In the case of phases, like in a perturbation resulting in phase drift (or different phases along different cores, something that may be consider not as a perturbation), it is an straightforward task. In the case of coupling, it requires a more complex mathematical treatment. Specifically, we will treat this within the coupled mode formalism we described in the previous section. We shall consider pairs of modes (we only need qubits), and we shall assume apply the conditions of perturbation theory.

The question now is how to formulate this in more tractable terms for quantum states propagating along an optical fiber. We may take the linear system of equations in Eq. (2.9) and write it in matrix form, as

$$-i\frac{d}{dz}a = Ca, \tag{2.49}$$

where a is a column vector of absorption operators.

The solution of this equation is

$$a(z) = e^{iCz}a(0), \tag{2.50}$$

where the perturbation C acts on the input operators $a(0)$ yielding operators $a(z)$. Before we go any forward, note that, as the coupling coefficients verify $k_{nm} = k_{mn}$, then C is symmetric. Moreover, $e^{iCz} = S$ is a unitary matrix.

Real fiber perturbations are random, and may vary with z. As said, in this previous analysis, we were actually considering segments where the perturbations remained z-invariant. This means that Eq.(2.50) is a discrete transformation, valid for a given segment s of the fiber. The full perturbation is given by a sequence of k perturbations encompassing the whole length of the fiber, in such a way that the output operators (i.e. fiber exit) are given as a function of the input operators (i.e. fiber entrance) as

$$a_{out} = S_k S_{k-1} ... S_2 S_1 a_{in} = T a_{in}. \tag{2.51}$$

Please bear in mind that, even though the matrices $S_k, S_{k-1}...$ are individually symmetric, the full matrix product T *is not*.

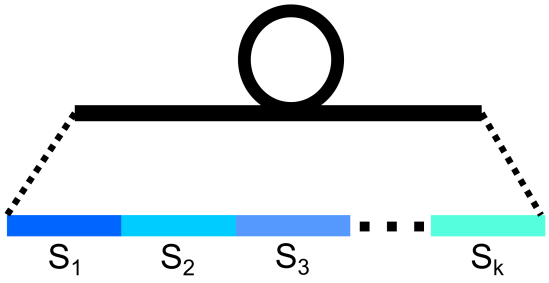


Figure 2.7: *The full perturbations on the fiber are expressed as the product of k perturbations. On each of the k small segments, the k-th perturbation is assumed to be independent from the propagation coordinate z.*

Normally, we will be dealing with qubits, so only two modes need to be considered ($N = 2$), which considerably simplifies the equations. This means that a is a two row column vector, and T is a 2x2 matrix. In particular, by solving Eq. (2.8), we find that each S_k is equivalent to an asynchronous coupling matrix [76]

$$S_k = \begin{pmatrix} s_{11} & is_{12} \\ is_{12} & \bar{s}_{11} \end{pmatrix}_k , \tag{2.52}$$

which has $\det(S_k) = 1 \; \forall k$. So, T is actually a SU(2) matrix, given by

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}_{out} = \begin{pmatrix} t_{11} & -\bar{t}_{12} \\ t_{12} & \bar{t}_{11} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}_{in} . \tag{2.53}$$

As the perturbation is random, parameters on the matrix are actually random variables (RVs).

Finally, note that another way of seeing that T needs to be indeed SU(2) (that is, unitary with determinant equal to one), is that it is a product of k unitary matrices. The determinant of a product of matrices is the product of determinants, so, if the individual matrices had a determinant other than 1 (that is, -1), then the value of $\det T$ would be either 1 or -1. As that cannot possibly be, because k is arbitrary (coming from the formal argument), and the value of the determinant needs to be fixed, then $\det(S_k) = 1 \; \forall k$ and thus $\det(T) = 1$.

As we saw, we can consider this perturbation as a map between quantum states, that is, a transform acting on single-photon quantum states. In particular, we can understand it as a rotation in the Bloch sphere [77]. This rotation is given by an SU(2) matrix, hence with three d.o.f. Given an initial state on the Bloch sphere, randomly chosen according to some basis, the perturbation rotates the vector (spinor) on the 2-sphere. We shall go over this in greater detail in Chapter 5.

This (unfinished) perturbation analysis will prompt us to describe the working principle of autocompensation in Section 2.4.

2.3.3 A brief word on optical fiber interconnects

We know how to guide and manipulate light, but in addition to this we need a series of auxiliary devices that allow us to build optic fiber networks. There are many components involved in such a task [32], but it will be enough for the purposes of this Thesis to briefly mention a couple of them: *circulators* and *photonic lanterns*. We will make an extensive use of the former in the A-MDI-QKD protocols we shall present in the following chapter, and also in the final chapter.

An *optical circulator (OC)* is a device that is used for suitably routing light. In particular, it routes light unidirectional, allowing flow in one sense but not in the other.

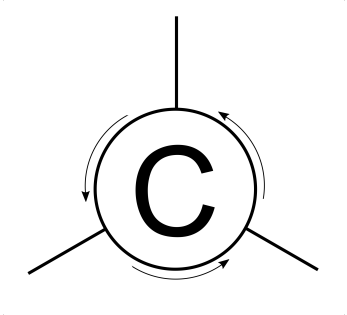


Figure 2.8: *Example of a three-port optical circulator. Light can enter and exit on any of the connected ports, but can only exit from the one at its left (anti-clockwise).*

OCs allow us, for instance, to couple light in and out, in a coordinated manner, from the main fiber channel into Alice's and Bob's stations, where regularly, as we will see, smaller fiber circuits are located for various purposes (phase coding and autocompensation). OCs are a basic tool for tidy light circulation along the fiber infrastructure of the QKD protocols. Internally, they are rather complicated, and they are based, in part, in the Faraday effect [32], which we will describe later in the context of autocompensation.

On the other side, another interconnecting element we shall make use of are *photonic lanterns*. These are elements that allow to join the cores of an MCF with individual SMFs [78]. This is useful as it allows for individualized processing of pulses travelling different cores, as for instance delaying a pulse propagating along a core with respect to another.

2.4 Autocompensation for fiber systems. Theory and results.

The essence of *autocompensation* (from *automatic compensation*) boils down to the following trick: get the light to travel from point A to point B (A and B do not necessarily mean Alice and Bob here), operate on the quantum state by some determinate transformation M, and then propagate the light back to point A so that the overall effect $T_{B\to A}MT_{A\to B}$ is a predictable transformation [79]. This can be applied

to an already existing fiber network without not too much cost, thus allowing for Plug and Play (P&P) operation [80]. Perturbation's effects can be removed provided the former do not change on the light's way back. This is a reasonable assumption. Given the speed of light, many realistic situations can be modelled by perturbations that are slowly varying or stable enough.

For instance, if we put a Pauli-Y gate-like operation

$$M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{2.54}$$

sandwiched between matrices of the type

$$S_k = \begin{pmatrix} s_{11} & is_{12} \\ is_{12} & \bar{s}_{11} \end{pmatrix}_k \tag{2.55}$$

we obtain

$$S_k^{\leftarrow} M S_k^{\rightarrow} = M \tag{2.56}$$

While this case is applicable for perturbations giving rise to spatial coupling between modes, either in FMF or MCFs (though the physics are different), things need to be made slightly different for polarization. This is because the polarization couplings are not insensitive to the change of propagation direction when light goes back (backpropagation). The assumption of stable perturbations is also made, but some modifications (affecting signs) need to be made to take backpropagation into account.

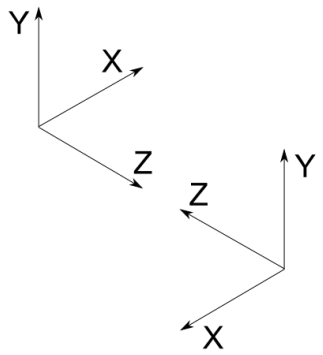


Figure 2.9: *When treating backpropagation ($z \to -z$), taking into account the system of coordinates convention, we require that $x \to -x$, while the y-direction remains unchanged.*

We consider (see Figure 2.9) a coordinate system with light propagating along the z-direction, as customary. At the endpoint of the line, where the sense of propagation gets reversed, z becomes $-z$. As a consequence, to maintain the right-handedness of the coordinate system (it is a convention), we need to invert also x [79]. Thus, as polarization coupling coefficients can be written as [49], in a similar way we formulated spatial couplings

$$\kappa_{nHmV} = \int P_{pol}(x,y) e_{nH} e_{mV} dxdy, \tag{2.57}$$

where we are here describing the coupling, due to P_{pol} being nonzero, between an H-polarized mode with index n and a V-polarized mode with index m.

Now, given the coordinate system above, we identify the x direction with H-polarization and the y direction with the V-polarization. When back-propagating, now the horizontally polarized mode will change sign (not magnitude), thus the coupling coefficient will too, while the vertically polarized mode will remain the same.

In order to translate this into a more tractable matrix form, given the polarization encoding (the well-known polarization qubit), like we did for spatial coupling, something similar needs to be done [49]. In particular, the forward propagation form of the polarization perturbation is

$$S_k^{pol,fwd} = \begin{pmatrix} s_{11} & is_{12} \\ is_{12} & \bar{s}_{11} \end{pmatrix}_k , \tag{2.58}$$

now the backpropagation version of this matrix is

$$S_k^{pol,bwd} = \begin{pmatrix} s_{11} & -is_{12} \\ -is_{12} & \bar{s}_{11} \end{pmatrix}_k . \tag{2.59}$$

Mathematically, to autocompensate for this kind of polarization perturbations is enough to sandwich a Pauli-Y gate (with a phase) between the perturbation matrices.

$$\begin{pmatrix} s_{11} & -is_{12} \\ -is_{12} & \bar{s}_{11} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} s_{11} & is_{12} \\ is_{12} & \bar{s}_{11} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} , \tag{2.60}$$

which can be achieved, according to Equation 2.4, by rotating a HWP an angle $\theta = \pi/4$.

Other possibility to achieve polarization autocompensation, and perhaps the mostly known, is by means of a *Faraday mirror (FM)*. It consists on a regular mirror plus a Faraday rotator. The Faraday rotator is a piece of material that, when subject to a magnetic field, allows for changing the polarization vector of the light traversing it [32]. For the case of linear polarization, we have an actual rotation of the polarization vector. Quantitatively, the amount the polarization is rotated is proportional to the value of the applied magnetic field. Indeed, the phase introduced between the two circular polarization components any polarization vector may be decomposed in is given by [79] $\phi = V\beta_0 Bd$. Here, V is the so-called Verdet constant; β_0 is the propagation constant in vacuum; B is the magnetic field along β_0's direction and d is the length light traverses under the magnetic field's influence. Importantly, the FM is a non-reciprocal component (polarization perturbations are non-reciprocal either), meaning that its effect is not the same for light propagating in one sense or the opposite. If forward-propagating light acquires is rotated by an angle ϕ, then backpropagating light is rotated by $-\phi$. In terms of matrices, with the a choice $\phi = \pi/4$, the combination of a Faraday rotator (thus a Hadarmard gate) and a mirror produces the following [79]

$$\frac{1}{2} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} , \tag{2.61}$$

which is a Pauli Y-gate operation (albeit a global π phase). From here we see that the passive autocompensating devices we have been working with can be thought as *effective* FMs, not only for polarization (like the HWP) but for other (spatial mode) encodings too.

2.5 Sources

The first step of any QKD protocol is the actual production of photons within some given parameters. We shall then start by describing the *sources*. We will reduce our attention to two of them: attenuated lasers for independent weak coherent pulse (WCP) production and SPDC sources, both type-I and type-II, for production of entangled states.

Ideally, QKD needs single photon sources. We shall see it in detail in the following chapter, but for the moment it will suffice to state that the use of single photon signals is required, in principle (there are workarounds, like use of decoy states), to obtain full secure QKD.

The search for an efficient single-photon source, that emits single photon signals on demand is still an ongoing issue [81, 82, 83]. For now, we shall conform ourselves with approximations to such ideal single photon character. In this sense, the sources we shall describe are non-deterministic. They emit empty pulses with an appreciable probability, single photon sources with a small probability, and multiphoton pulses with a smaller probability.

A relevant parameter for the kind of pulsed sources for QKD use is the *repetition rate* (or equivalently, the clock rate). The repetition rate is the amount of pulses produced by the source per unit time, normally per second [84]. When dealing with key rates, a number of bits (typically less than one) are generated per pulse. This quantity times the repetition rate gives the key rate in bits per unit time. As it is just a multiplying factor on the key rate, as we will see in greater detail, we will tend to normalize the bit rate by the repetition rate (as is customary in the field).

2.5.1 Attenuated laser pulses: WCPs

The first approximation to the single-photon source is the attenuated laser pulse. It consists on a laser, used for pulse generation, plus an attenuator. While passively, neutral filters or waveplates and polarizators could be used, we shall assume we can have access to variable optical attenuators (VOAs).

The attenuated laser source produces coherent states. Recall that the mathematical expression of a coherent state [53] in terms of Fock states is the following

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{2.62}$$

From this expression, one can readily obtain the probability of measuring n photons

in the pulse as (substituting the parameter α by $\sqrt{\mu}e^{i\phi}$)

$$P(n,\mu) = e^{-\mu}\frac{\mu^n}{n!}. \tag{2.63}$$

which is a Poisson distribution.

The phase of the coherent state can provide Eve with information [85]. Thus, what one does is to phase-randomize the coherent states [75]. Under that circumstances, the coherent state becomes a mixture of Fock states [75] with probability coefficients given by the Poisson distribution above.

$$\rho = \frac{1}{2\pi}\int_0^{2\pi} d\phi |\sqrt{\mu}e^{i\phi}\rangle\langle\sqrt{\mu}e^{i\phi}| = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n\rangle\langle n|. \tag{2.64}$$

By tuning the attenuation so μ is small (around 0.1 [86]) we can greatly reduce the probability of multiphoton pulses and try to achieve single-photon behaviour. However, we also increase the probability of emission of photon pulses with zero photons. Indeed, most of the pulses are now empty [86], which means that the signal will be weak and the key rate small. Even more crucial is the issue of *dark counts* [86] (dark count: detector firing up even when there is no signal i.e the signal is empty), which adds a lot of noise to the detection process, obfuscating accurate communication. In the next chapter we will see how to overcome some of this difficulties, apart from providing a workaround for the so-called Photon Number Splitting (PNS) attack, by using decoy states. We will give more detail on the dark count issue in this chapter also, in the section dedicated to detectors.

2.5.2 Spontaneous parametric down-conversion

The process of spontaneous parametric down-conversion (SPDC) is a well-known way to obtain entangled photons from a laser source [53]. It is used to produce photons in entangled states however not (and crucially) on-demand, but with a small probability. This is one of its disadvantages, because it reduces the key rate.

SPDC is a non-linear optical process [87]. It consists in a strong laser beam (the pump) impinging a crystal (typical materials are BBO, KDP...) with a nonzero second-order susceptibility. The crystal is transparent to most of the light coming in, but a tiny fraction of the pump (or parent) photons is converted into two photons (the idler photon and the signal photon —daughter photons), satisfying energy and momentum conservation (*phase condition*). If the two photons have different energies, then we are in the nondegenerate case; if they have the same (central) frequency, we are in the degenerate case. In the latter, the photons emerge symmetrically in opposite sides of the same cone. In the former, they emerge in opposite sides of concentric ones.

Depending in the polarization of the outcoming photons between themselves and that of the pump, SPDC comes in two flavours: type-I and type-II. In the case of type-I SPDC, the polarization of the outgoing photons (idler and signal) is opposite to that of the pump. For type-II SPDC, the polarization between the idler and signal is the opposite.

The way this two types of SPDC generate entanglement is through indistinguishability. We shall describe how. First, we will show how to do it in the polarization encoding, as is the direct and most usual one.

We may begin by entanglement generation in the case of type-II SPDC, as is simpler than for type-I. In type-II SPDC, the outgoing photons emerge in two cones that intersect in some region. One of the cones corresponds to the idler photon and the other to the signal photon. In the sections that this cones overlap, we have an ambiguity, whether one photon coming from that region is an idler photon or a signal photon. Moreover, as said, idler and signal photons have orthogonal polarizations. We can discriminate this using PBS. Thus, if we detect a couple of photons coming from the overlapping regions, which can be singled out by means of pinholes, what happens is this: say we detect a horizontally polarized photon coming from one of the pinholes. We do not know if it came from the idler cone or the signal cone. A photon coming from the other pinhole will be vertically polarized, and we will have the same ambiguity whether it is a signal or an idler photon. Hence, the quantum state corresponding to this observations is no other than

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|1_{Hi}1_{Vs}\rangle + |1_{Vi}1_{Hs}\rangle). \tag{2.65}$$

A phase $e^{i\theta}$ may be introduced between the two terms of the expression above, thus being able to generate also the singlet (Bell) state $|\psi^-\rangle$.

Note that such narrow region for ambiguity reduces the generation rate of entangled pairs. In the following mechanism for achieving entanglement in a type-I configuration, this inconvenient is avoided by extending the ambiguity over a much bigger region.

Entanglement generation with type-I SPDC is a bit more trickier. To obtain the necessary ambiguity we need a second nonlinear crystal. An efficient configuration [88] consists on using two BBO crystals, the optical axis of one of them rotated 90^{o} respect to the other. We are required to pump the BBO crystals with photons in the state

$$\frac{1}{\sqrt{2}}(|1_H\rangle + e^{i\theta}|1_V\rangle), \tag{2.66}$$

where we already have introduced a phase difference between the two polarization components, which will enable later for generation of other Bell states ($|\phi^+\rangle$ or $|\phi^-\rangle$ —or also compensate for undesired phases introduced in the process). This can be realized, passively, by means of a waveplate or, actively, by means of a Pockels cell, as mentioned.

The crystals are put very close to each other. They are cut and oriented with respect to the pump beam in such a way that only a vertically polarized pump photon can be downconverted at the first crystal, and the horizontally polarized one at the second crystal. The result is that, after the crystals, photons emerge in a superimposed H-polarized cone with a V-polarized cone. In other words, the precise crystal from which the signal and idler photons came out cannot be possibly known. A coincidence measurement of the idler and signal photons could yield two different results: either both photons are horizontally polarized or vertically polarized. This

means that after the crystals the photons are in the following entangled state

$$|\phi(\theta)\rangle = \frac{1}{\sqrt{2}}(|1_{Hi}1_{Hs}\rangle + e^{i\theta}|1_{Vi}1_{Vs}\rangle). \tag{2.67}$$

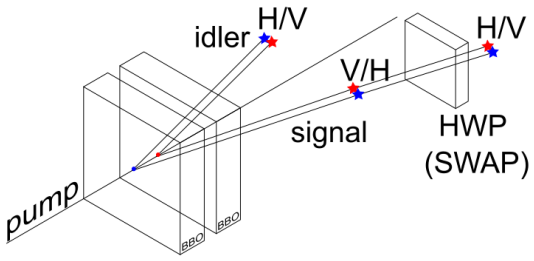


Figure 2.10: *Schematic example of an efficient arrangement to produce any of the four Bell states by means of type-I SPDC, following [88]. State preparation of the pump not shown. The HWP is rotated $\pi/4$, thus interchanges polarization states.*

Even though this source produces two-photon states, which will be extensively used in this Thesis, it can also be used to achieve a single-photon source for detection of one photon (called *heralding photon*) of the pair guarantees that a single photon (called *heralded photon*) is travelling on the other (corresponding) direction. That single photon can then be used for quantum information/computation etc purposes. Because of this, SPDC is also called an *heralded* single-photon source [89].

So far, we have outlined this well known technique to generate entanglement in the canonical, so to speak, polarization encoding. However, in this Thesis, we will be interested in other encodings also, like for instance the dual-rail encoding in multicore fibers. Imagine that we have such two cores of an MCF; such encoding works according to the rule (we show how this fits with the computational -$|0\rangle$, $|1\rangle$ basis, although most of the time we will not use such notation)

$$\begin{aligned} |0\rangle &\rightarrow 1 \text{ photon in core 1 and none in core 2,} \\ |1\rangle &\rightarrow 1 \text{ photon in core 2 and none in core 1.} \end{aligned} \tag{2.68}$$

In a typical setting, we shall have two cores for Alice to launch her photons, and two cores for Bob. To identify the cores we may opt for the following notation

$$\begin{aligned} |1_{j1}\rangle &\rightarrow 1 \text{ photon in core 1 and none in core 2,} \\ |1_{j2}\rangle &\rightarrow 1 \text{ photon in core 2 and none in core 1,} \end{aligned}$$

where j can take the values $j = \{a, b\}$. With this notation, an in this degrees of freedom, an entangled state (2.67) would look like

$$|\phi(\theta)\rangle = \frac{1}{\sqrt{2}}(|1_{a1}1_{b1}\rangle + e^{i\theta}|1_{a2}1_{b2}\rangle). \tag{2.69}$$

Now, how do we achieve this by physical means? We can use the SPDC type-I configuration we have just described. Only, at the end, given a pair of points in the

overlapping cones, we need a system to redirect the entangled photons to the fiber cores, either directly or by coupling to single-mode fibers and then to cores. A way to do it directly involves the use of PBSs. A given photon of one side of the cone can be either H-polarized or V-polarized. Thus, a PBS would (spatially) split these two possibilities, each one redirected to one core of (Alice's) MCF (*demultiplex*). Likewise, in the opposite operation can (selectively) redirect Bob's photon to Bob's MCF cores.

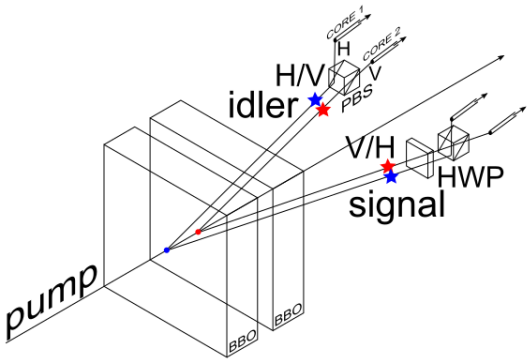


Figure 2.11: *Schematic SPDC type-I setup for entanglement generation in MCFs, which will be useful for the section on entanglement-based QKD. Again, the HWP interchanges the polarization states.*

For spatial mode encoding in FMFs we can proceed similarly. The essence is that polarization needs to be translated into HG modes. In such case, we would need devices binary phase plates together with refractive phase shifters [90] to multiplex right after the PBSs.

In the case of SPDC the photon number statistics are, a priori, different from the Poissonian distribution characteristic of coherent states of light. In fact, the photon number follows a *super-Poissonian* or *thermal* distribution [86]. For instance, for type-II SPDC the probability for obtaining n photons is given by [91]

$$P(n) = \frac{(n+1)(\mu/2)^n}{(1+\mu/2)^{n+2}}, \tag{2.70}$$

where μ is again the mean photon number. But recall we said, however, *a priori*. The state coming out a SPDC crystal is closely related to two-mode squeezed states [92, 91, 93]. In fact, it involves many two-mode squeezed states. Each of them obeys a super-Poissionian distribution, nonetheless the combination of all them renders a Poissonian distribution on the detected number of photons [92, 94].

2.6 Detectors

The endpoint of the quantum communication process are the detectors. In an ideal scenario, they would register every incoming signal with perfect efficiency and without introducing any errors, apart from those due to the degradation of the signal along the fiber. In real life setting, this is not the case. Detectors have some problems

associated with them. The central issue is that no perfect single photon detector exists, at present date; although there has been huge progress on the matter [81, 95], this is still an open problem which, if solved, would greatly enhance QKD performance, among a myriad of quantum technological applications [96]. The standard detector throughout the main body of QKD literature are avalanche photodiodes or APDs. There are other technologies, like superconducting single-photon detectors (SSPDs) [97], which are currently employed in state-of-the-art QKD implementations like [41] but to be consistent with the off-the-shelf nature of APDs, and mainly given that the focus of this Thesis is in fibers, rather than sources or detectors, we shall remain in the standard.

APDs come with a series of practical inconveniences. First of all, they have a range of wavelengths they operate with good efficiency, while they may be almost transparent to others. On the other side, fibers also have a certain bandwidth (corresponding to typical telecom wavelengths) where attenuation is quite low, while for other wavelengths it unacceptably high for practical communication. The problem is that the optimal detection bandwidth (maximum efficiency) does not need to actually match the optimal fiber bandwidth (minimal attenuation). Therefore, a compromise must be achieved between the two bandwidths, which will likely determine the technology to be used. If telecom fibers are to be used, this will favour some detector platforms (InGaASs/InP based, germanium based...) above others [86]. In any case, in our simplified scenario, we shall rather treat detectors as black boxes and focus only on two relevant parameters when characterizing their performance: the efficiency η_d and the dark count rate p_d.

These two essential parameters express two facts: a) that not all the optical signals arriving at the detectors from the fiber are registered; b) that sometimes no photon arrives but still the detector registers a count randomly, contributing to noise. Both aspects can contribute to a reduction of the key rate. The effect of the efficiency is perhaps more straightforward, as it does not contribute to noise, thus does not generate errors. Most of the times, the efficiency term can be included into the more general transmittance term, that also includes fiber attenuation and internal transmittances of the involved devices (optical hardware at Alice and Bob's stations). In the second case, the dark counts can dominate true counts when only a weak signal (because of the fiber attenuation) remains. In such cases, there is a distance where errors are to big for a secret key rate to be distilled, marking thus the maximum achievable distance of the protocol.

Other relevant factor is the detector's dead time. This parameter expresses the minimum temporal separation between signals to be recorded as two different signals. This clearly affects key rate, specially in relation with repetition rate because, no matter how many pulses we send per unit time, if detectors cannot resolve them, we will gain nothing. The dead time won't enter our equations, but is worthwhile to mention that is a critical limiting factor for protocols implementing a time-bin encoding. Indeed, this can be considered as one of the reasons to not use a time-bin encoding, while it has some very good advantages as being immune to, for instance, polarization perturbations. This is because only the time pulses arrive matters for key generation; the information is not encoded in the polarization degree of freedom.

Let us now compute the probability of detection of a given signal state, *considering that signal and dark counts can occur independently*. First we absorb the efficiency η_d in the overall transmittance of the quantum channel. Note that this cannot be so simply done if each of the detectors (in Alice's or Bob's stations, within the same station) has a different efficiency, but such symmetry is something that we will, in good approximation (they are standard detectors, with supposedly identical specifications and fabrication procedures), assume. In that case, the projector P modelling a negative measurement of the detector, that is, the detector registering no photons (*no click*), is given by

$$P_{no} = (1 - p_d)|0\rangle\langle 0|. \tag{2.71}$$

This means that, whenever the pulse is empty, i.e contains zero photons $\rho = |0\rangle\langle 0|$ (it is photon number encoding, not the computational basis), and no dark count click happens (with probability p_d), we have a negative result. The positive result, meanwhile, is written down, by complementarity, as

$$P_{yes} = \mathbb{1} - (1 - p_d)|0\rangle\langle 0|, \tag{2.72}$$

where the identity is given by $\mathbb{1} = \sum_n |n\rangle\langle n|$.

The probability of obtaining a click on the detector will be given by the usual rules of QM, as [74]

$$p_{yes} = \mathrm{Tr}(\rho P_{yes}). \tag{2.73}$$

Note that the process of absorbing the detection efficiency into the overall transmittance can be done prior to detection or at the the detection stage. In the first case, we have to modify the state coming from the source. In the second case, we compute detection probabilities altogether. The results are the same, evidently.

Consider for instance that a photon is being sent, $\rho = |1\rangle\langle 1|$. Due to the transmittance of the fiber (considering detection efficiency too), the state arriving at the APD is, from Eq. (2.38)

$$\rho = (1 - \eta)|0\rangle\langle 0| + \eta|1\rangle\langle 1|, \tag{2.74}$$

with $\eta = \eta_d \eta_{\mathrm{int}} e^{-\alpha_{att} L/10}$, where η_{int} refers to the optical hardware other than the fibers internal transmittance.

Now, introducing this in Eq. (2.73) we have

$$p_{yes} = (1 - \eta)p_d + \eta, \tag{2.75}$$

which is often approximated to $\eta + p_d$ as p_d and η are quite small [75]. For an $n-$photon state the expression for p_{yes} becomes

$$p_{yes} = 1 - \mathrm{Tr}(\rho P_{no}) = (1 - \eta_n)p_d + \eta_n, \tag{2.76}$$

with η_n given by Eq. (2.44). Finally, if we do the same computation for a coherent state $\rho = |\alpha\rangle\langle\alpha|$, which after passing through the system with overall transmittance η has become $\rho = |\sqrt{\eta}\alpha\rangle\langle\sqrt{\eta}\alpha|$ we find that

$$p_{yes} = 1 - (1 - p_d)e^{-|\sqrt{\eta}\alpha|^2} = 1 - (1 - p_d)e^{-\eta\mu}. \tag{2.77}$$

Chapter 3

Autocompensating Measurement-Device-Independent QKD

This Chapter is related to the following articles the author has contributed to (found at the end of this document, in Appendix D): a) it is fundamentally based on results published in [76], adding a figure adapted from [98]; and b) it includes small contributions based on results from [99].

A typical QKD setting consists on two agents, Alice and Bob, that wish to *share* a random string of bits called the *key*. This key must be kept secret, ideally, away from the knowledge of an eavesdropper, Eve. Then, such key will be used by Alice and Bob to cipher/decipher a message using a *symmetric key* cryptosystem like the one-time pad protocol, which is *absolutely secure* [86, 17]. The exchange of key between Alice and Bob can still be subject to a man-in-the-middle attack, but classical authentication protocols, which require a key of $O(\log(n))$ bits, with respect to a secret key –or message– of length $O(n)$, adequately fulfil such need [11].

QKD is not a substitute to classical cryptography in the sense that it can be thought of as a technique that helps classical cryptography, or physical layer on top of regular classical communication, to achieve unconditional security by distributing key safely (or *grow* key safely, since Alice and Bob start with a pre-shared short key for authentication [11]). Quantum signals are generated, sent and measured along a quantum channel. The quantum channel may be monitored by Eve. Then, Alice and Bob communicate, publicly, along an authenticated and unjammable classical channel (meaning that messages keep their authenticity and integrity). The raw data from the measurements is classically post-processed and a secure key is distilled. This key, in turn, is used as a one-time pad to encrypt the message by means of a Vernam-like cipher.

The quantum channel may have different implementations. In this Thesis, we are interested in optic fiber links, where information is encoded in photon states travelling an optical fiber and processed with photonic hardware, both passive and with the aid of optoelectronic elements. Some of the hardware will be preferably be integrated, while for some cases bulk optics may me used. Some results we obtained are also applicable to free-space links, but for all of this Section and throughout the whole Thesis, an optical fiber setting is assumed. As in any communication channel, both loss and noise will be present, and will diminish the performance of QKD protocols. Being conservative in the cryptographer's sense means that it must be assumed that the eavesdropper Eve is solely the responsible for loss and noise (primarily, *noise*), since it may be possible that she substitutes the quantum channel for an ideal one, without loss and without noise[17]. Given some noise level, which we must try to reduce, the achievable secret key rate will give the performance of the QKD protocol [86, 17].

3.1 The BB84 protocol

To explain how QKD works we may carry it out, as it is commonly and most illustratively done, in the context of the pioneering BB84 protocol [28]. Later, when we move onto other protocols, we will explain their particularities on the fly. It is important to note at this point that, conceptually, all QKD works under the same premises than BB84. This goes for this specific Section as well as for the following ones.

The security of the protocol relies in the fact that, in QM, observables associated to non-commuting operators are incompatible. Or, in other words, the Uncertainty Principle. Information is encoded in quantum states belonging to two mutually unbiased bases (MUBs). For instance, one can use the Z basis and the X basis. In the computational notation, the elements of the Z basis are $|0\rangle$ and $|1\rangle$. There are many physical realizations of such encoding. One of the most popular is polarization encoding[1], where the aforementioned computational states are identified with $|1_H\rangle$ or $|V\rangle$. The basis X consists of the elements $|+\rangle = 2^{-1/2}(|0\rangle + |1\rangle)$ and $|-\rangle = 2^{-1/2}(|0\rangle - |1\rangle)$. Classical bits are encoded in the following way: 0 corresponds to either $|0\rangle$ or $|+\rangle$ and 1 corresponds to either $|1\rangle$ or $|-\rangle$. Thus, if Alice sends to Bob states, say $|0\rangle$ and $|-\rangle$ she will be encoding the string 01.

The Z and X bases are mutually unbiased as $|\langle u_i^Z||u_j^X\rangle|^2 = 1/2$, where $|u_i^Z\rangle$ and $|u_j^Z\rangle$ are any element of the Z and X bases, respectively. In general, given a Hilbert space with $\dim(\mathcal{H}) = N$, and two bases P and Q, this condition is expressed as $|\langle u_i^P||u_j^Q\rangle|^2 = 1/N$, for any pair of elements of the bases. The elements of the Z basis are eigenstates of the Pauli operator σ_z and the elements of the X are the eigenstates of the Pauli operator σ_x. The eigenstates of one operator are non-orthogonal with respect to the eigenstates of the other. The Pauli operators verify

[1]In free-space links, polarization is the popular choice [100, 101], as it does not get scrambled by propagation on atmospheric channels or space (some adjustments need to be made, nonetheless). For the case of fibers, the time-bin encoding is more common. However, with autocompensation techniques we can still perform QKD with polarization-encoded qubits.

$[\sigma_z, \sigma_z] = 2i\sigma_y$, thus they correspond to incompatible observables. All of this means that a measurement in the X basis of a quantum state encoded in the Z basis will not reveal any information about it and vice versa. To measure in the Z (X) basis is to project the quantum state into an eigenstate of such basis.

The BB84 protocol operates in the following way: Alice chooses randomly a basis for encoding information. For instance, one uses a Quantum Random Number Generator (QRNG) [86, 17] for the choice of basis. Alice then sends the state to Bob, who chooses also randomly the measurement basis, and then measures the state sent by Alice. Now, if the encoding basis and the measurement basis are not the same, the outcome of Bob's measurement is totally random, thus Bob gains no information about what Alice's has sent. Suppose for the moment there is no Eve. Transmission of information across the quantum channel goes as follows: Alice randomly encodes and sends to Bob, who randomly measures. If they bases agree, the state Alice sends is the state Bob measures: *then they share the bit associated to that state.* Repeating this process lefts Alice and Bob with a shared string of bits, the *sifted* key, which is the key after the events where Alice and Bob do not agree on their choice of bases, are discarded. To reach such agreement, Alice publicly announces her choice of basis over the classical channel, and then she and Bob discuss which events to keep.

Now, it may happen that unbeknownst to Alice an Bob, Eve is trying to tamper with the channel. Eve may use a number of strategies, or *attacks* to extract private information. The most basic attack is to directly measure the state Alice sends. But, Eve does not know what precise basis Eve used for encoding. She may guess right, or she may guess *wrong*. In that last case, imagine Alice sends the state $|0\rangle$, then if Eve measures in the X basis, the state after the measurement will be $|+\rangle$. When Bob measures it, and he does it in the same basis that Alice used (if not, it is discarded), he will measure the state $|1\rangle$ with a 50% probability. But, how did that state get there in the first place? Alice sent a 0 and Bob measured 1! If he and Alice reserve some of their shared bits and compare them, they will find errors, and those errors will point to Eve (or to experimental errors, which in a cryptographic sense must be attributed to Eve). Explicitly, Eve measures in the wrong basis 50% of the time. From that half, Bob may measure the correct state. Then, Eve's strategy of measuring what Alice sends and then send it along the line (*intercept-resend attack*), will contribute to a 25% of errors in the sifted key, assuming the number of signals sent is infinite.

Table 3.1: *Small sample (not all possible outcomes are considered) of a typical QKD signal exchange in the BB84 protocol with polarization encoding. We assume an H-pol (V-pol) photon represents the bit 0 (1).*

Alice (basis/pol)	Bob (basis/pol)	Bit
Z/H	Z/H	0
X/-	X/+	Error (Eve!?)
Z/V	X/+	Discard (sift)
Z/V	Z/V	1

3.2 Eve's interference

Eve's attacks on the quantum channel induce noise, as measurement imperfections and errors do. It is mandatory to accurately model the separate influence of Eve's and experimental imperfections contributions to errors. For instance, if, for instance, in the ideal BB84 case (no experimental errors), and under a intercept-resend attack, Alice and Bob detect a quantum bit error rate (QBER) greater than the 25% threshold, they must abort the protocol. If we now move to a realistic setting, we will have also to consider the influence of practical imperfections of the devices. If our quantum channel is so imperfect that, even if Eve were not watching, the QBER is greater than 25%, the protocol will be useless. Thus we have to control (model) for experimental errors and reduce them as much as we can, within practical limitations.

Moreover, even if the QBER is below the threshold, we cannot discard Eve's interference. Experimental errors mask Eve's presence. As said, from the cryptographic standpoint, we need to assume that Eve may be able to swap the noisy channel for an ideal one of her own [17], thus all noise will be caused by Eve. We might naively think that the communication is safe, because QBER is under the limit, but information is indeed leaking. In the other hand, a certain level of noise will be always present. A zero noise QKD protocol is not possible (it may be for Eve, who we assume is infinitely powerful, but we are not). Thus, we cannot halt the protocol every time noise is detected. We cannot discard Eve's presence either, no matter how low the noise level is. To deal with this problem, we need to *bound* Eve's information given some noise level [86, 17].

To achieve this we first need to measure information. Fortunately, we know how to do this. Information theory [102] provides with the right tools. Then we need to stablish secure bounds on it. One assumes [86] that Alice and Bob and *Eve* share some information. Then, the aim is to reduce, to an arbitrarily small amount, the information that Eve has, while Alice and Bob retain part of their shared information. The process by which this is done is called *privacy amplification*. Importantly, the information shared between Alice and Bob must agree, so *error correction* is needed. The application of these two processes *distils* a sifted key, with possible information leaking to Eve, into an *secret (symmetric) secure key*.

This embodies one of the key aspects of QKD. Eavesdropping, we insist, leads to errors (or noise), which we can detect. In other words, those errors constitute a proxy of an spy's information on otherwise confidential data. So, we may actually *use* such errors, by means of privacy amplification, to reduce the information the adversary has down to a negligible amount.

If, by means of a QKD protocol, it is possible to exchange an amount of secret information greater than zero, for some noise level, then the protocol is said to be secure. Formal proofs of the unconditional security for BB84 (which can be extended to other protocols) have been provided [103, 104]. They are rather mathematically involved, relaying on quantum information-theoretic arguments. Intuitively, they are based in formulating the BB84 protocol as an entanglement protocol, and then use quantum error correction codes (in particular, CSS codes [105]) to show that

one can safely distil key for a given error rate. They give an expression for a lower bound of the key rate per pulse R in terms of the binary Shannon entropy function $H(x)$ and the bit and phase error rates e_b and e_p

$$R \geq 1 - H(e_b) - H(e_p), \tag{3.1}$$

where

$$H = -x \log_2 x - (1-x) \log_2 (1-x). \tag{3.2}$$

The errors just above are respectively related to the fact that if a bit is supposed to be a 0 and changes to a 1, that is an error, and if a bit is encoded in the X basis as $2^{-1/2}(|0\rangle + |1\rangle)$ and due to de-phasing becomes $2^{1/2}(|0\rangle - |1\rangle)$ that is also an error. A randomly applied Hadamard transform, that randomly exchanges between the Z and X bases, converts a phase error in a bit error and vice-versa. Thus, in an actual BB84 experiment, the measured error rate becomes, simultaneously, an estimate of both e_b and e_p [104], then $e_b = e_p = e = QBER$ and

$$R \geq 1 - 2H(e). \tag{3.3}$$

Importantly, whenever $e \geq 11\%$ one cannot distil a secret key rate. Such value corresponds to Eve launching the most general type of attack in a single-photon setting, the *coherent attack*. In this type of attack [17], Eve is assumed to perform a joint measurement on the qubits Alice and Bob send, coupled with ancillary states of hers, and using a quantum memory. Thus, this key rate formula is valid under such attack, and also under other less general attacks like the *collective* or *individual* attacks [86, 17]. There are other types of attacks, motivated by practical imperfections in realistic settings, that have a relevant influence in deciding whether a given protocol is secure or not. Although one can prove that key can be safely extracted even though Eve may launch a coherent attack, that attack does not include practical imperfections that are not taken into account when proving security. Attacks exploiting these vulnerabilities fall under the denomination of *quantum hacking* [106], and usually specific measures are needed to counter them.

It is also important to know that Eq. (3.1) and Eq. (3.3) are valid under the assumption that an infinite number of signals have been sent by Alice, so these formulae describe *asymptotic* key rates [104]. In a real-life experiment with actual data, one will need to make a finite-key analysis to take into account statistical fluctuations [17].

Regarding attacks, Eve may attack each (or all of them, simultaneously) of the aforementioned three hardware parts. Eve can, in principle, launch attacks on the sources, on the fiber link and on the detectors. In this Thesis, however, we will mostly ignore attacks on the sources. We will only consider the PNS attack, that may be considered in some sense an attack on the source. Source attacks normally require tailored solutions. In this case, it can be solved by means of the *decoy state method*. By attacks on the communication link we mean spying strategies consisting in taking some qubits from the channel and measuring them, for instance in the most general way of coherent interaction. Such attacks are unavoidable, but can be identified by the errors the introduce in the key rate, and their influence thereby

reduced (at the expense of a lower key rate, but perfectly secret). Attacks on the devices ought to be handled in a general way, by means of full *device independence*, which is impractical at the present time, or, in the case of attacks on the *detectors*, by means of the less-stringent (in terms of technological requirements) *measurement-device-independence*.

3.2.1 The decoy state method

The PNS attack is a consequence of real-life behaviour of photon sources. Ideally, quantum sources are perfectly single photon, but we have seen that they actually have a non-negligible probability of emitting a multi-photon signal. This is to say, real sources essentially emit various identical signal states per pulse. For security proofs, it is assumed that Eve has full technological capabilities of manipulating quantum states; the only restriction is that she operates within the laws of QM. Therefore, Eve can do the following [17]. On the hand hand, block the true single-photon signals, which are the only ones that are really secure. On the other hand, split a n-photon state and keep $n-1$ photons to herself (in a quantum memory). The single photon is then measured (by Bob for instance, in the BB84 protocol, etc.) and after the bases are broadcast Eve makes measurements on her "copies". Alternatively, Eve can essay various measurements in his $n-1$ photon state and then select those where her basis choice matches that of the legitimate parties. in any case, Alice and Bob won't notice, but Eve has obtained a bit of key (if no other errors are present).

A way to deal with this would be to estimate what fraction of the signals are single-photon, and then only use that for estimate the key generation rate [104, 107]. However, that greatly reduces such key rate. Also, if one tries to maximize the number of single-photon states produced, one is forced to choose a low-intensity source, which means less key rate. A much improved solution consists in sending decoy states, along the actual signal state carrying the information [108]. This enables to simultaneously give much better bounds on single-photon states, increasing the key rate, and also allows for actually detecting PNS attacks and thus unmask Eve.

Before we describe how that works, we shall write down the definitions of some useful quantities. Also, this discussion will help us bring in the so-called *photon number channel model*. Indeed, let's consider the well-known case where the protocol source are phase randomized WCP's. Given the behaviour of the Poisson distribution, if the value of μ is chosen to be very low, one reduces the probability of multi-photon states, but it does not become zero, and it notably favours the production of empty pulses, which carry no signal at all. This greatly reduces the key rate. With this in hand, the following quantities are defined:

- *Yield* Y_n: it depends on the photon number n and it is defined as the *conditional probability of Bob detecting a signal subject to Alice sending a pulse containing n photons.*
- *Gain* Q_n: it is the yield times the probability of producing such pulse. For instance, the gain of a, say, three-photon state will be given by $Q_3 = \exp(-\mu)\frac{\mu^3}{3!}Y_3$.
- *Error rate* e_n: it is the QBER (recall: detections giving erroneous bits/total

detections) associated with a pulse containing n photons.

Now, for a state like (2.64), with mean photon number μ, the overall gain is denoted by Q_μ given by the sum

$$Q_\mu = \sum_{n=0}^{\infty} Q_n = \sum_{n=0}^{\infty} p_n Y_n. \tag{3.4}$$

The same goes for the error rate, and one can define the overall error rate

$$E_\mu = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} Q_n e_n = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} p_n Y_n e_n. \tag{3.5}$$

Importantly, nor the yield, nor the gain or error for a given photon number n can be measured in an actual QKD session, but it can be estimated or modelled. What can be measured are the two magnitudes above. The overall gain corresponds to the number of detections or counts and the overall error rate is the quotient between the erroneous counts (counts leading to erroneous bit assignment) and the total counts.

In the case of the PNS attack, Eve's optimal strategy is to block all single-photon pulses, which are the only safe ones. Thus in that cases the yields would be $Y_1 = 0$ and $Y_n \neq 0 \ \forall n \neq 1$. Alice and Bob, however, cannot investigate directly the yields of the pulses, as Eve keeps all but one photons of the multi-photon pulse, and Alice cannot measure them when they are emitted without destroying them. What happens, if however, Alice, along of a signal state with mean photon number μ sends many other states with different mean photon numbers ν_i? Note that in an experiment, where Bob can record the overall gains and errors, equations are linear systems of equations with infinite unknowns, the Y_n and the e_n. If there are infinite mean photon numbers, and the yields and errors depend only in the photon number, irrespective of the mean photon number, as they do, then we have infinite equations [108].

$$\begin{aligned}
Q_\mu &= \sum_{n=0}^{\infty} p_n(\mu) Y_n, \\
Q_{\nu_1} &= \sum_{n=0}^{\infty} p_n(\nu_1) Y_n, \\
Q_{\nu_2} &= \sum_{n=0}^{\infty} p_n(\nu_2) Y_n, \\
&\vdots \\
Q_{\nu_i} &= \sum_{n=0}^{\infty} p_n(\nu_i) Y_n.
\end{aligned}$$

And the same goes for the error rates:

$$E_\mu = \frac{1}{Q_\mu}\sum_{n=0}^{\infty} p_n(\mu) Y_n e_n,$$

$$E_{\nu_1} = \frac{1}{Q_{\nu_1}}\sum_{n=0}^{\infty} p_n(\nu_1) Y_n e_n,$$

$$E_{\nu_2} = \frac{1}{Q_{\nu_2}}\sum_{n=0}^{\infty} p_n(\nu_2) Y_n e_n,$$

$$\vdots$$

$$E_{\nu_i} = \frac{1}{Q_{\nu_i}}\sum_{n=0}^{\infty} p_n(\nu_i) Y_n e_n.$$

We have made apparent that the probability of emission of a certain state with n photons depends on the mean photon number: $p_n \to p_n(\mu)$ and so on. The crucial thing here is, may one insist, that the yields and error rates do not depend on the mean photon number of the distribution but on the number of photons of the state. This means that we can solve the system of equations and get the yields and errors from an actual experiment. Then, if Eve where to attack the communication, in the PNS way, the yields would be affected and Eve would be detected. This is the essence of the decoy state idea. At first sight, nonetheless, it may seem that it is actually impossible to carry it on in reality. There cannot be infinite decoy states mean photon numbers from which to choose. However, it is not necessary to have that many. Actually, a tight bound on the yields an errors can be obtained with just a few of them: even with only one weak decoy, a vacuum and a signal it is enough [109].

To sum up, the decoy state allows for the legitimate parties to detect the a PNS attack by an eavesdropper. Moreover, once they make sure there is no one using that attack (although the communication can be subject to other attacks), the decoy state method provides very good tight estimates of the single photon errors and gains, much better than the pessimistic assumption of GLLP [104]. The value of the mean photon number for the signal state needs not to be as small as without the decoy state method. In fact, it can be of the order $O(1)$ [108]. All this means that the key rate increases up to the performance of almost an ideal single photon source [107].

3.3 Evaluating protocol performance

The main parameter or figure of merit by which one may describe a given protocol's performance is the aforementioned secret key rate, meaning the amount of bits of information per pulse or per unit time, as a function of either QBER, optical loss or *distance* [17]. Note that QBER increases with distance, as attenuation on the

fiber increases the relative weight of the noisy contribution in the detected bit rate. Typically, when analysing a protocol, one must give, apart from describing its inner workings and hardware for its implementation, a graph relating the secret key rate R with the distance between Alice and Bob. This is, the communication link distance. It is a specific goal for better QKD implementations to increase both R for a given distance and to extend the achievable distance.

Evaluating the secret key rate is done in two steps. First, computation of the detection probabilities of the events used for bit generation. Any successful event, meaning a signal is measured, contributes to the raw key. If the result is not what is expected, according to the encoded bit information, they belong to the error category. This phase of the computation takes into account the characteristics of the devices in place. The more realistic the assumptions and models of the devices, the more realistic the key rate analysis. And the more prepared against attacks, regarding implemented countermeasures, the safer. As the devices are quantum, working in a QM framework (and specifically, quantum optics) is required. Two aspects of the source are, as far as this Thesis concerns, of interest: the actual state produced (encoding) and the statistics of the emitted photons. The repetition rate, which is, as said, a relevant experimental parameter, appears just as a constant factor in the key rate, so we will not dedicate time and effort to it. Normally, one normalizes the key rate by dividing by the repetition rate, so one computes the exchanged (secure) bits per pulse. To convert this in bits per unit time multiplication by the repetition rate is in order. Regarding the channel, we need to evaluate losses (attenuation) and perturbations, such as polarization and phase drift, couplings. Finally, with respect to detectors, we shall consider dark counts and efficiency.

The second step is the classical post-processing stage, consisting in error correction and privacy amplification. We may also include here the sifting procedure, consisting in Alice and Bob discarding the events corresponding to incompatible bases choices. It is a classical process in the sense that basis information has to be sent through the classical channel. In the classical post-processing phase, some of the bits are sacrificed for two purposes: first, eliminate any bit disagreement between Alice and Bob, that is, eliminate erroneous bits. This means Alice and Bob will share the same bit-string. An ideal error correcting protocol would require do discard a number N of bits. Usually, less ideal protocols are used, that need for a bigger number of bits to be disposed of. This is captured by an inefficiency coefficient f, meaning that the actual amount of bits that are lost in the process is fN. The value or f depends on the error level of the QKD experiment; the greater the error rate, the bigger the value of f [110].

The second part of this classical stage is privacy amplification, aimed at reducing to a negligible amount the information Eve may have on the key. The price to pay for this is, as said, the sacrifice of a certain number of bits. At the end of the classical stage Alice and Bob share a perfectly correlated bit-string.

When all of this factors we have been discussing enter into play, the expression of the key rate is more complicated than we have seen in Equation (3.1). Specifically, it can be obtained as the general expression [108].

$$R \geq qQ_1^Z[1 - H(e_1^X)] - Q_\mu^X f H(E_\mu^X). \tag{3.6}$$

Here, q is the base-sifting factor (=1/2), accounting for the discarding of events when Alice and Bob choose different phases (there is a efficient version, where $q = 1$ [111]). Q_μ^X and E_μ^X are the overall gains described before, and can be directly measured in a QKD experiment, while the single-photon gain and error, Q_1^Z and e_1^X, are estimated by using the decoy state method. This is, the system of equations is solved and the quantities above are bounded: a lower bound for the gain and an upper bound for the error (and thus a lower bound for the key rate).

3.4 Measurement-device independent QKD

We have been outlining how to compute key rates and how to include device's imperfections on them, through models of said devices. However, such models are intended to capture non-idealities of the devices in a most generic way. This raises the question whether we are capturing enough of the device's physics in those models; so as to not leave any loophole that could be exploited by Eve [112]. It has been shown that some characteristics of real devices, can be used by an adversary to obtain information about the secret key without being detected, leading to, for example, the phase remapping attack [113], the time-shift attack [114] or the detector blinding attack [19], which require from ad-hoc countermeasures.

Two possibilities come to mind: first, develop more accurate models of the devices, in order to fully characterize imperfections and address possible attacks. This has the inconvenience of the associated difficulty of a full characterization of devices, as they may be complicated enough that it becomes infeasible to embody the physics/technology involved in a working model. Also, one can never be sure of the robustness of the characterization, in the sense of mathematical proof. Then there is a second possibility, which consists on designing protocols in such a way that their security is *intrinsically* independent of the devices used, that can be then left uncharacterised attack-wise, apart from performance requirements. This means that the protocol becomes inherently robust against any attack on the devices.

Along this second line of thought there has been some promising progress in QKD. We may mention here two cases, the last one will be the one we shall implement within a P&P setting. The first approach is Device-Independent QKD (DI-QKD) (see, for instance, [115, 116]), in which the aim is to produce QKD protocols whose security does not depend in any of the devices involved, with Bell inequalities serving as the underlying working principle. Although this would be perhaps the best solution so far, it is very challenging, in terms of experimental feasibility [17]. Other more practical possibility is MDI-QKD [15], which protects against any type of attack on the *measurement* devices. Protocols designed this way do not have full device independence, but their implementation is far more practical. The downside of MDI-QKD with respect to ordinary implementations of, say, BB84 is the lower key rate, because it requires detection of pairs of photons simultaneously, while previous, ordinary protocols only needed to detect one photon

(per signal sent).

The essential aspect of MDI is that the measurement devices are taken out from Alice and Bob's laboratories and given to an *untrusted* relay which is normally called Charlie. It is Charlie, who might be even Eve herself, who performs the measurement. And to prove MDI security, one can simply ignore what happens in the measurement stage, as it was a black-box. The only information coming out of it its whether a successful measurement has taken place or not, and if so, what detectors did click.

The measurement the relay performs is a Bell state measurement on the joint state Alice and Bob send. In each of Alice's and Bob's stations, they generate signal states in the two usual BB84 bases, Z or rectilinear and X or diagonal. As in BB84, events where they happen to choose a different basis are discarded. In the canonical polarization basis, that means that they prepare states like $|1_H 1_V\rangle$, $|1_+ 1_+\rangle$ and so on. This joint state arrives at Charlie's station, which, again, within this particular encoding, contains, for instance, the following setup: a beam-splitter where Alice's and Bob's states are recombined, and then sent to PBS's located at each of the BS outputs, as shown in the Figure. At the respective outputs of the PBS detectors are located. This whole setup is capable of distinguishing from two (classes of) Bell states, the singlet state $|\psi^-\rangle = 2^{-1/2}(|1_H 1_V\rangle - |1_V 1_H\rangle)$ and the three others. In the case of MDI, the singlet and the state $|\psi^+\rangle = 2^{-1/2}(|1_{HV}\rangle + |1_{VH}\rangle)$ are detected, as they are the ones that are produced (we shall describe how), but such setup alone cannot be used to identify the four Bell states by themselves. Once there has been a detection (or Charlie says so) he announces the result of the measurement. From such result, if we assume that information is encoded in the same way as in BB84, Alice and Bob can deduce the bit they actually sent, but for Charlie the information he has, from the measurement, is not enough, in fact, he cannot possibly obtain any information about it. Thus, a secret key has been established.

To understand how MDI works, consider just what happens whenever Alice and Bob happen to choose the Z basis, and keep the Bell state discriminating setup of Figure 3.1 in mind.

Note that we define the Bell states in the usual way (we show them here for the polarization encoding, but the translation no any other d.o.f is straightforward):

$$\begin{aligned} |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|1_H 1_V\rangle + |1_V 1_H\rangle) \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}}(|1_H 1_V\rangle - |1_V 1_H\rangle) \\ |\phi^+\rangle &= \frac{1}{\sqrt{2}}(|1_H 1_H\rangle + |1_V 1_V\rangle) \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}}(|1_H 1_H\rangle - |1_V 1_V\rangle), \end{aligned} \tag{3.7}$$

where $|\psi^-\rangle$ will often be referred as the singlet state.

If Alice and Bob both choose the same state, either $|1_H 1_H\rangle$ or $|1_V 1_V\rangle$, we have Hong-Ou-Mandel (HOM) interference at the BS, thus photons bunch at after it and

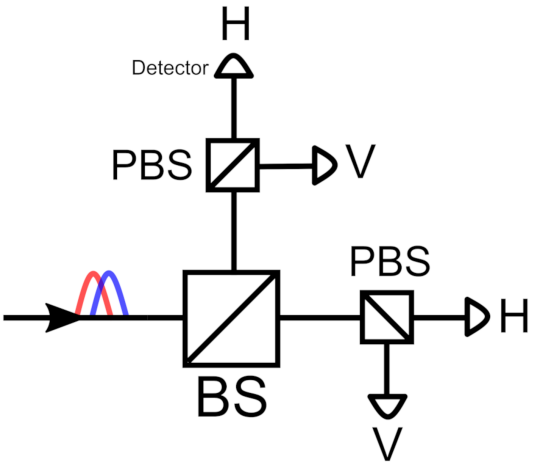


Figure 3.1: *Bell measurement arrangement (standard Innsbruck scheme) for photon polarization-encoded qubits, consisting on a BS that splits the incoming signal into two arms; each one reaches a PBS with detectors at their outputs.*

only one detector will fire, at any of the outputs of the PBSs. This events need to be discarded; if they were used, Eve would know what Alice and Bob sent. If however they choose $|1_H 1_V\rangle$ or $|1_V 1_H\rangle$, then, assuming we use a BS implementing the transform (recall Equation (2.3) and invert it)

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \tag{3.8}$$

then the output becomes

$$\begin{aligned} |1_{aH}1_{bV}\rangle \rightarrow \frac{1}{2}(|1_{cH}\rangle + i|1_{dH}\rangle(i|1_{cV}\rangle + |1_{dV}\rangle = \\ \frac{1}{2}[i|1_{cH}1_{cV}\rangle + |1_{cH}1_{dV}\rangle - |1_{dH}1_{cV}\rangle + i|1_{dH}1_{dV}\rangle] \\ = \frac{1}{\sqrt{2}}[(\frac{i}{\sqrt{2}}(|1_{cH}1_{cV}\rangle + |1_{dH}1_{dV}\rangle) + \frac{1}{\sqrt{2}}(|1_{cH}1_{dV}\rangle - |1_{cV}1_{dH}\rangle)] = \\ \frac{1}{\sqrt{2}}(i|\psi^+\rangle + |\psi^-\rangle). \end{aligned} \tag{3.9}$$

A similar output state (except from a minus sign: $|\psi^+\rangle - |\psi^-\rangle$) would be obtained if the initial state was $|1_{aV}1_{bH}\rangle$. This state has the same Bell state signature as (3.9). Note that for $|\psi^+\rangle$ both photons bunch together at the output, while for $|\psi^-\rangle$ each photon emerges in a separate port. This behaviour [55] determines the detection pattern.

Equation (3.9) constitutes a superposition of two entangled states, $|\psi^-\rangle$ and $|\psi^+\rangle$. Detection of any of them does not give any information on Alice and Bob random choice, as choices $|1_H 1_V\rangle$ and $|1_V 1_H\rangle$ give identical detection scenarios. Thus, we may assign, as usual, (classical) bit 0 to an H-polarized photon and bit 1 to a V-polarized photon. Also we agree that, for the joint state, the choice 01 corresponds to bit 0 and choice 10 to bit 1, so that Bob will perform a bit flip after

measurement has been broadcast. With such conditions, Eve, by having access or even control of the measurement cannot determine if the key-bit will 0 or 1, as any of such possibilities would yield the same output state. Alice and Bob *know*, however, as they know which state they sent and from that and the measurement announcement can deduce what the other one randomly chose.

For the case of the X basis, something similar happens, and the results follow from linearity. In this case, however, if Alice and Bob happen to send the same state, there are some events that are valid, as they do not only produce HOM interference. Say that they send the state

$$|1_+1_+\rangle = \frac{1}{2}(|1_H1_H\rangle + |1_V1_V\rangle + |1_H1_V\rangle + |1_V1_H\rangle),$$

then the terms $|1_H1_H\rangle = |2_H\rangle$ and $|1_V1_V\rangle = |2_V\rangle$ are actually HOM interference, but the sum $|1_H1_V\rangle + |1_V1_H\rangle$, from Equation (3.9) gives $|\psi^+\rangle$ (thus no bit flip is applied). An analogous result is obtained for $|1_-1_-\rangle$. For the case of $|1_+1_-\rangle$ or $|1_-1_+\rangle$, the resulting Bell state is $|\psi^-\rangle$, thus a bit-flip is required. Again, Eve cannot know the key bit, as the Bell outcomes are identical in each case. Note that we (may –other correspondences are possible) assume that $|1_+1_+\rangle$ (and $|1_+1_-\rangle$) is encoded into bit 0 and that $|1_-1_-\rangle$ (and $|1_-1_+\rangle$) corresponds to bit 1.

Table 3.2: *Small sample (not all possible outcomes are considered) of a typical QKD signal exchange in the MDI protocol with polarization encoding. Again, we assume an H-pol (V-pol) photon represents the bit 0 (1).*

Alice (basis/pol)	Bob (basis/pol)	Charlie's Outcome	Bit
Z/H	Z/H	HOM	No Bit
X/+	X/+	*if* $\|\psi^+\rangle$	0 (no bit flip)
Z/V	X/+	Irrelevant	Discard (sift)
Z/V	Z/H	*if* $\|\psi^-\rangle$	1 (Bob bit flip)

3.5 Results

We shall now describe the progress obtained in the context of this Thesis combining, in the one hand, the MDI approach of constructing QKD architectures, in order to remove detector side-channels, and autocompensation techniques in order to remove errors. The result, which we name as A-MDI-QKD, is that we obtain a significant improvement in the secret key rate with affordable means, in the sense of the extra optical hardware that autocompensation requires.

3.5.1 A-MDI-QKD in few-mode fibers

We start by describing the results for few-mode fibers. This implies, as we previously saw, that we have modes travelling in the same core.

We shall consider only modal coupling. That means that the (more precise) physical realization we have in mind may be the case of PM-FMFs [117], which, due

to the high built-in birefringence, prevents from polarization coupling but allows for cross-talk to happen, with the subsequent modal noise. These kind of fibers are relevant as they have very favourable characteristics for implementing SDM, which greatly enhances the amount of data transmission. Alternatively, we are assuming that the polarization d.o.f can be factorized from the spatial mode degree of freedom, which is reasonable if we assume polarization perturbations to be common as the core is the same [76, 98].

Light travelling this kind of fibers can be modelled as LP modes [118]. Within the same polarization, in order to have an effective qubit [58], we may encode information in a superposition of even and odd LP modes, for instance, between L^o_{11H} and L^e_{11H} or between L^o_{11V} and L^e_{11V}, with H and V indicating polarization (factorized), and e and o indicating even or odd parity of the respective mode functions. The rest of modes are considered to be very weakly coupled to those, in such a way that it can be disregarded. In addition, they may be used to regular classical data transmission, while the particular modes above are reserved for QKD purposes, *i.e*, establishing a key that can then be used for ciphering classical messages.

As the details on the perturbations and mode characteristics have been described in previous sections, we shall focus here on protocol analysis. In this line of thought, as in Chapter 2, consider that the particular modes we use for QKD are horizontal and vertical HG mode functions [58]. We label horizontal with the letter X and vertical with the letter Y, to avoid any confusion with light polarization (the polarization of the modes is the same and can be either vertical or horizontal).

Now, given these kind of modes, they will be processed by bulk optics, as seen in Chapter 2, involving characteristic devices like DPs and CLCs. This, in combination with other hardware typical of fiber-optic systems will be used to draw the optical layout of the A-MDI-QKD protocol. In particular, the collinear mode equivalents of PBSs, optical fiber delay (OFD) and FMs.

But first, let us describe the general structure of the protocol. A priori, the arrangement is analogous to that of the original MDI paper [15], with Charlie in the middle performing the measurements. However, in order to achieve autocompensation, we need back-and-forth circulation, so the source is now also situated in the middle, at Charlie's station, and not on Alice's and Bob's stations. For evident reasons, we cannot let Eve control the source, and we know that Charlie cannot be trusted, so the source at Charlie only emits blank quantum states, in the sense that they do not contain any (sensible) information. Is Alice and Bob, with respective QRNG-fed phase modulators on their well-shielded and protected stations that encode the actual bit information.

In such stations, moreover, autocompensating devices are also situated, providing the necessary transformations on the incoming photonic states so they are restored back at Charlie's. The layout of the protocol is shown in Figure 3.4.

The starting point, as said, is Charlie's station, containing an initial states generator (ISG). We use the following notation, where $|X\rangle$ represents a photon excited in the horizontal HG mode (even LP mode L^e_{11X}) and $|Y\rangle$ represents a photon excited in the vertical HG mode (odd LP mode L^o_{11Y}). Charlie then sends

the following superposition, containing no bit information at all:

$$\frac{1}{\sqrt{2}}(|1_X\rangle + |1_Y\rangle)_a \otimes \frac{1}{\sqrt{2}}(|1_X\rangle + |1_Y\rangle)_b, \tag{3.10}$$

where a stands for Alice (referring to Alice-Charlie path) and b for Bob (referring to Bob-Charlie path).

The first step now, in order to phase-modulate and autocompensate [79], is to introduce a delay τ between the $|1_X\rangle$ state and the $|1_Y\rangle$ state. As the modes are collinear, we must find a way to sort them, so separate them and then delay one with respect to the other. We shall do this with a particular implementation of a MZI. This mode-sorting MZI will be useful not only for the delay, but for the measurement device, where it will act as the equivalent of a PBS.

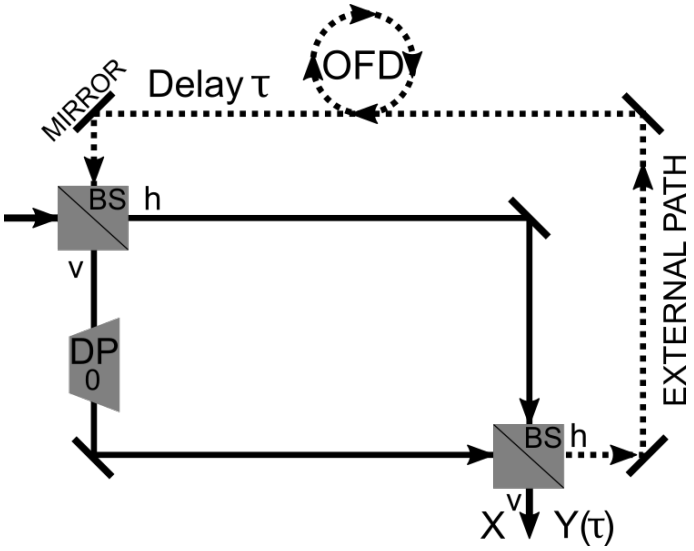


Figure 3.2: *MZI configuration for sorting HG modes. It can be used for delaying one mode with respect to another, as shown in the figure, and also later as the collinear equivalent of the PBS in the measurement device. Reproduced from own contribution [76].*

The mode-sorting MZI has the following structure (see Figure 3.2). It consists on a pair of BS, one at the input and one at the output, like a regular MZI. But, in one of its arms, a Dove prism is located. Now, a Dove prism, we have seen (see Equation(2.7)) that it may be characterized by an angular parameter Ω and used to perform rotations on spatial mode function qubits. If we set Ω to be equal to 0 (or π, global phases aside) we have a realization of the z-Pauli matrix

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The particular BS in this MZI operate the following way. For a horizontal input h (photon impinging in the horizontal input port) they produce a superposition $h+v$, while for a vertical input they produce the output $v-h$. In combination with the Dove prism in the first vertical arm of the interferometer, for an input

$$\frac{1}{\sqrt{2}}(|1_X\rangle + |1_Y\rangle)_h,$$

after the second BS the state becomes

$$\frac{1}{\sqrt{2}}(|1_X\rangle_v - |1_Y\rangle_h), \tag{3.11}$$

implying that we have been able to separate the X mode and the Y modes. For the OFD case, the Y mode is then connected back to the initial BS by a fiber loop, thus delaying one mode with respect to another $Y \to Y_\tau$.

More in detail, the sequence of transformations on the input state is as follows (it is the same for Alice and for Bob), where for simplicity we omit normalization factors in the intermediate steps

- Input: $\frac{1}{\sqrt{2}}(|1_X\rangle + |1_Y\rangle)_h$
- First BS: $(|1_X\rangle + |1_Y\rangle)_h + (|1_X\rangle + |1_Y\rangle)_v$
- Dove prism: $(|1_X\rangle + |1_Y\rangle)_h + (|1_X\rangle - |1_Y\rangle)_v$
- Mirrors (up to a global π phase): $(|1_X\rangle + |1_Y\rangle)_v + (|1_X\rangle - |1_Y\rangle)_h$
- Second BS: $(|1_X\rangle + |1_Y\rangle)_v - (|1_X\rangle + |1_Y\rangle)_h + (|1_X\rangle - |1_Y\rangle)_h + (|1_X\rangle - |1_Y\rangle)_v$
- Output: $\frac{1}{\sqrt{2}}(|1_X\rangle_v - |1_Y\rangle_h)$

Now that we have described the mode sorter, we shall focus on the autocompensation circuits. These are short loops, short enough to do not induce any appreciable coupling between modes, in the scale cross-talk happens. In these loops, which are connected to the main optical link through optical circulators, four optical hardware elements are located.

One of them is a standard element, common to the three encodings, which is a phase modulator (PM) used to encode information on the quantum state that comes from Charlie. As the two states $|1_X\rangle$ and $|1_{Y\tau}\rangle$ are delayed, the PM does not act like a phase gate, but rather in an individualized fashion on the states, that can be considered as a couple $|1_X\rangle, |1_{Y\tau}\rangle$. It is the delayed state that picks up a phase $|1_{Y\tau}\rangle \to \exp(i\theta)|1_{Y\tau}\rangle$, chosen from the set $\theta = \{-\pi/2, 0, \pi/2, \pi\}$, in order to produce any of the four states of the diagonal (or X) $2^{-1/2}(|1_X\rangle \pm |1_Y\rangle)$ and circular $2^{-1/2}(|1_X\rangle \pm i|1_Y\rangle)$ bases, which constitute two MUBs. These will be the states reaching Charlie's measurement device on their way back, as the delay is eliminated when the states travel back along the mode-sorting MZI.

The other three are a couple of CLCs and a DP which, together, are dedicated to autocompensate the mode-coupling perturbations. We have seen that the effect of these perturbations can be modelled as a sequence of k symmetric SU(2) matrices acting on the absorption/emission operators of the photonic modes or, as we are dealing with (a pair of) single-photon states, directly acting on the quantum states. In any case, we have the following transformation due to modal coupling

$$P_k = \begin{pmatrix} a_k & ib_k \\ ib_k & a_k^* \end{pmatrix}, \tag{3.12}$$

where the elements of the matrix, which satisfy $|a_k|^2 + b_k^2 = 1$, are random variables, but remain constant during the time window the light travels the fiber links back-and-forth.

We have k matrices of these acting like $P = P_k P_{k-1} P_{k-2} ... P_3 P_2 P_1$. In addition, as light circulation is a two-way path, we have two of these, meaning that the global effect of the perturbations is $P = P_{\leftarrow} P_{\rightarrow}$. In this case $P_{\leftarrow} = P_{\rightarrow}$, as modal coupling coefficients do not change when reversing the sense of propagation.

Now, the way to deal with this perturbation is sandwiching something between these two matrices. In particular, introducing the transformation (Pauli Y-gate up to a global phase)

$$M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{3.13}$$

we have that

$$P_{\leftarrow} M P_{\rightarrow} = P_1 ... P_k M P_k ... P_1 = M, \tag{3.14}$$

as $P_k M P_k = M$ for any k, so that the unpredictable transformation has been removed.

The question now is how to obtain this precise transformation. We have advanced that we can use a pair of CLCs plus a DP. The DP angular parameter is now $\pi/4$, so it implements a Pauli X-gate

$$D_{\pi/4} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{3.15}$$

exchanging horizontal and vertical modes. On the other side, the $\pi/2-$CLCs implement a $\pm\pi/2$-phase gate

$$CLC_{\pm\pi/2} = \begin{pmatrix} 1 & 0 \\ 0 & \pm i \end{pmatrix}. \tag{3.16}$$

The combined action of the three yields the desired transformation (up to a harmless global phase)

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} = -i \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{3.17}$$

The Pauli X-gate implemented by the Dove prism is also necessary to compensate for the delay introduced between the X mode and the Y mode. As it interchanges the mode type ($X \leftrightarrow Y$), when light exits the autocompensating circuit, now is the mode X which is delayed with respect to Y. Now, this latter mode is the one that gets delayed at the MZI. After it then, both modes emerge simultaneously on time, which is something necessary for the next step: the measurement process.

The measurement process happens at Charlie's station. As we have seen, the relay's goal is to project the incoming signal into a Bell state, and announce if he has been successful or not. From this announcement Alice and Bob can deduce the other's bit encoding, and, in combination with their random choice, establish a key. In the case of HG modes like we are considering here, the Bell measurement device is conceptually similar to that for polarization encoding (also for codirectional mode encoding, but things get more interesting in that case). It consists on a central BS,

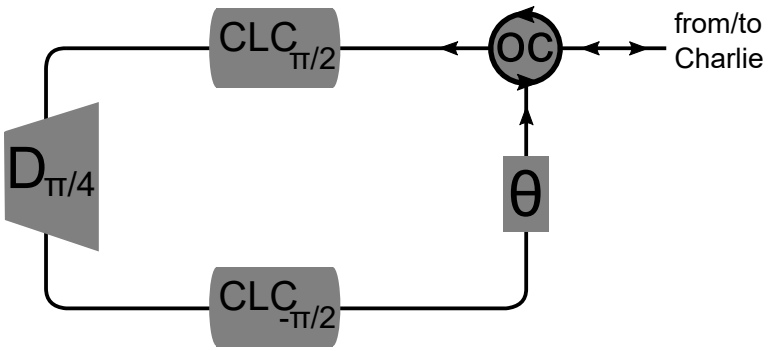


Figure 3.3: *A small fiber loop connected to the main fiber link by optical circulators provides room for autocompensating devices and phase modulators to be located. The combination of the CLCs and the DP provides the autocompensation transform. Reproduced from own contribution [76].*

where photons coming from Alice and Bob interfere plus two mode-sorting MZIs at the outputs of this BS acting like PBS (see Figure 3.4). As such, computations are identical to what we have seen in the introduction of this chapter, except from the part that we no longer use the Z basis but the Y basis. Note that this choice of basis is not trivial, as it is necessary for autocompensation. Alice and Bob are the ones encoding information, but Charlie starts the protocol. If the Z basis was used (at least directly), we would need to block some state to encode information, and autocompensation would not work (at least not so simply). Moreover, we may advance at this point that the Z basis has some practical advantages relative to key rate computations, but we will go over this for the case of MCF codirectional mode encoding.

Consider then, rather for the sake of completeness, the following input state in the circular basis, which is no conceptually different from the X basis (not to be confused with X and Y HG modes)

$$\begin{aligned} |1_{Ra}1_{Rb}\rangle &= \frac{1}{2}(|1_X\rangle + i|1_Y\rangle)_a(|1_X\rangle + i|1_Y\rangle)_b \\ \rightarrow \frac{1}{2}(&|1_{aX}1_{bX}\rangle - |1_{aY}1_{bY}\rangle + i|1_{aX}1_{bY}\rangle + i|1_{aY}1_{bX}\rangle). \end{aligned} \tag{3.18}$$

Now, the BS introduces the following transform on the modes: $|1_{aX}\rangle \rightarrow \frac{1}{\sqrt{2}}(|1_{Xc}\rangle + i|1_{Xd}\rangle)$ and so on. Therefore, we find that

$$\begin{aligned} |1_{Ra}1_{Rb}\rangle \rightarrow N(&i|1_{Xc}1_{Xc}\rangle + i|1_{Xd}1_{Xd}\rangle - i|1_{Yc}1_{Yc}\rangle \\ -i|1_{Yd}1_{Yd}\rangle &+ i|1_{Xc}1_{Yc}\rangle + i|1_{Xd}1_{Yd}\rangle + |1_{Xc}1_{Yd}\rangle - |1_{Xd}1_{Yc}\rangle \\ &+i|1_{Xc}1_{Yc}\rangle + i|1_{Xd}1_{Yd}\rangle - |1_{Xc}1_{Yd}\rangle + |1_{Xd}1_{Yc}\rangle], \end{aligned} \tag{3.19}$$

where N is a normalization factor. The first four terms in the equation above are HOM coincidences, and are not used for key generation. The other terms can be

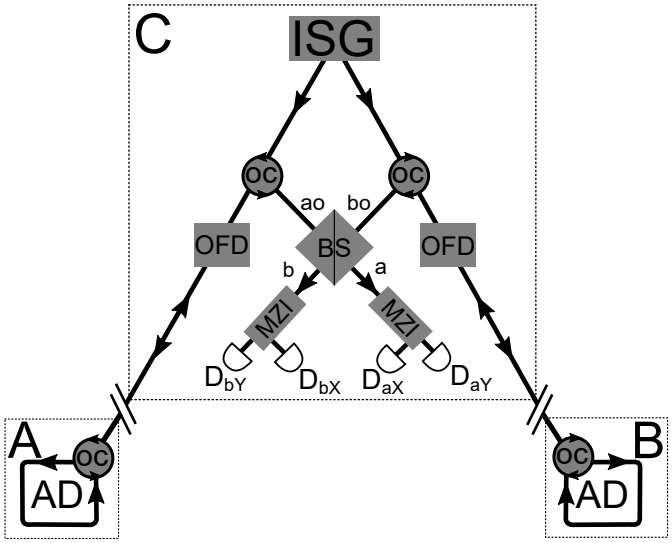


Figure 3.4: *Optical layout of the A-MDI-QKD protocol for collinear mode encoding. Reproduced from own contribution [76].*

arranged to form the state

$$\frac{1}{\sqrt{2}}(|1_{Xc}1_{Yc}\rangle + |1_{Xd}1_{Yd}\rangle), \tag{3.20}$$

which can be identified with the Bell state $|\psi^+\rangle$ on the spatial mode d.o.f. Note that the photons come out on the same port, thus they will trigger detectors $D_{aX}\&D_{aY}$ or $D_{bX}\&D_{bY}$ simultaneously.

3.5.2 A-MDI-QKD in multicore fibers

Multicore fibers are also a very good option to increase the amount of data that is transmitted through a fiber optic link. By employing different cores simultaneously, one is able to greatly increase the flux of information, while retaining single-mode propagation on each core, which may be more tractable.

Modes travelling different cores[2] can suffer from undesired modal coupling, or cross-talk, and also accumulate different phases (each photonic state can accumulate its own phase). This will scramble mode-encoded information. Recalling the dual-rail encoding, we see where the is the source of problems. For instance, if we use the X (diagonal) or Y (circular) basis, as we have defined them above, we have issues due to phase drift. Information will be encoded in the relative phase shift between the state representing a photon travelling one one core and a photon travelling on the other, as

$$\frac{1}{\sqrt{2}}(|1_{a1}\rangle + e^{i\theta}|1_{a2}\rangle), \tag{3.21}$$

[2]As patent throughout the main text body, we use this MCF modes are used interchangeably with the therm codirectional modes.

where θ may be 0 or π for the X basis or $\pi/2$ or $3\pi/2$ for the Y basis. An additional random phase ϕ along with θ may change the bit or even the basis, thus leading to errors or loose of events. For the Z basis that should not be a problem, and in this sense such basis is phase-drift protected. However, if cross-talk is present, bits encoded in such a basis are not safe, as couplings can take a state like $|a_1\rangle$ and turn it into $|a_2\rangle$ or any superposition of the type $\cos\varphi|1_{a1}\rangle + \sin\varphi|1_{a2}\rangle$, where φ would be a RV. Moreover, as we have seen, in general we have both effects combined, in a general perturbation given by an SU(2) matrix, thus scrambling information encoded in any base.

This short analysis, together with the previous theory of fiber perturbations, motivates the need for autocompensation mechanisms in this kind of setting. The protocol architecture is both conceptually (and physically) similar to that involving collinear mode encoding (see Figure 3.5). However, the hardware employed for various purposes, like mode delaying, autocompensation and measurement are quite different. As said, we focus here in optical integrated hardware.

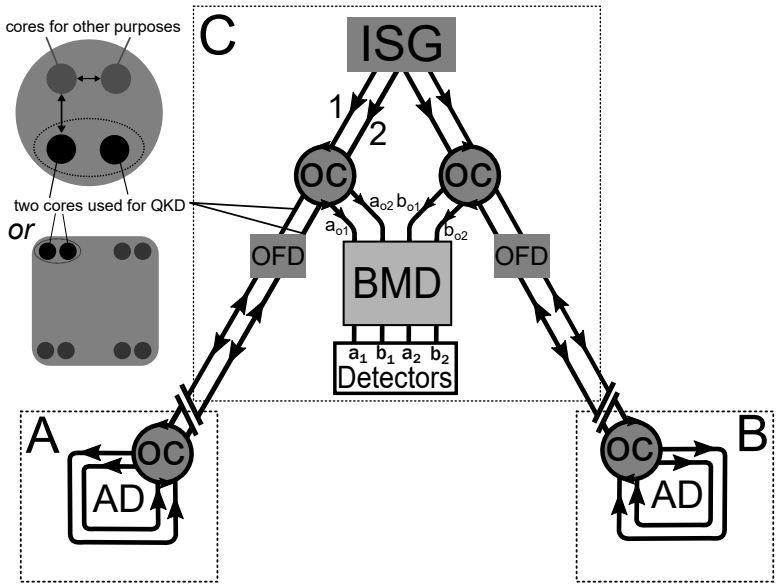


Figure 3.5: *Fiber optic architecture for performing A-MDI-QKD in multicore fibers. Inset shows an example of two-core arrangement that can be reserved for QKD, while the others would transmit ordinary classical information. Reproduced from own contribution [76].*

A remark is to be made at this point regarding the actual physical setting we are considering, with special attention to the position of the pairs of cores inside the MCF. It may be that the fiber only contains two cores, indeed [119]. We are assuming that the pairs of cores are very close between themselves, so if the starting polarization is common to both modes, it will remain so during propagation. This way, we can ignore polarization coupling and address modal coupling only. This does not mean that polarization is not an issue, as there is still the need for having Alice and Bob's photons polarized in the same way. Thus, a common reference and some autocompensation mechanism is required –HWP will be enough–, in order to

ensure that Alice's photon and Bob's photon are indistinguishable, and thus the Bell Measurement Device (BMD) performs as expected.

As in the previous case, light is launched from Charlie's station in an state containing no actual information. Indeed, the state is

$$\frac{1}{\sqrt{2}}(|1_{a1}\rangle + |1_{a2}\rangle) \otimes \frac{1}{\sqrt{2}}(|1_{b1}\rangle + |1_{b2}\rangle). \tag{3.22}$$

Now, one of the modes (for instance, 2) needs to be delayed, in order for the PM to work. The way to do it involves the following pieces of hardware: a) a fiber loop, b) two single-mode fibers and c) a photonic lantern (PL). Photonic lanterns [120] can be used to connect single-mode cores of a MCF to SMFs, in a one-to-one correspondence. This way, we can re-direct light in the cores of interest to SMFs and, in one of them, put a fiber loop which will cause a delay. Then, with another PL, we connect the SMFs back to the MCF. The layout of these devices is shown in Figure 3.6.

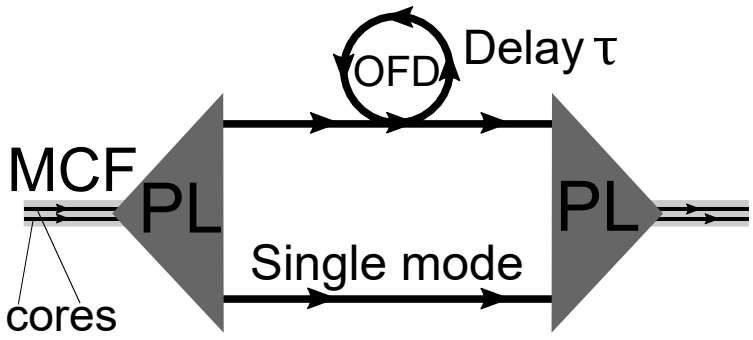


Figure 3.6: *Delay of one codirectional mode with respect to the other can be achieved by coupling into SMFs by means of a couple of PLs and then install a fiber loop in one of the SMFs. Reproduced from own contribution [76].*

Note that this delay is compensated for when the pulses reach back such device, as the autocompensation device interchanges the modes, in the same way it happened with the collinear modes.

Now it is the turn of the autocompensating circuits (Figure 3.7), where the PM is also located. For spatial perturbations (SU(2) matrix) compensation, we employ a DC with a coupling phase equal to $\pi/2$ plus a π-phase shifter. In general, given a couple of modes travelling different cores (or fibers, in the case a translation into SMFs was made), the DC implements the following transformation

$$DC(\alpha) = \begin{pmatrix} \cos\alpha & i\sin\alpha \\ i\sin\alpha & \cos\alpha \end{pmatrix}. \tag{3.23}$$

If we set up $\alpha = \pi/2$ (by tailoring, for instance, the coupling length or the distance between waveguides) the matrix above becomes

$$DC(\pi/2) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \tag{3.24}$$

which is a Pauli X-gate with a global $\pi/2$ phase that can be ignored for compensation purposes.

Now, if we put a π-phase shifter on one of the waveguides (cores or fibers) we obtain the following

$$M = i \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{3.25}$$

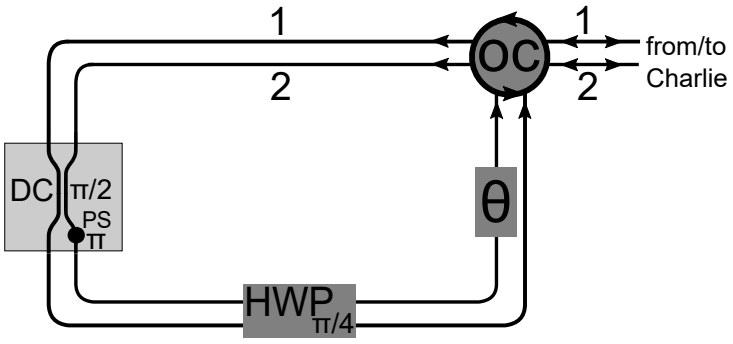


Figure 3.7: Autocompensating circuits for codirectional modes. The DC provides spatial mode perturbation compensation, while the HWP makes sure Alice and Bob's photons have the same polarization when reaching the Bell state measurement device. Reproduced from own contribution [76].

Note that this transformation is the same as Equation(3.13), albeit a common phase that has no relevance. Regarding spatial mode perturbation, the matrix is also an SU(2) matrix, and the same argument as we did for few-mode fibers, is applicable. Thus Equation(3.25) autocompensates for cross-talk in MCFs, given the conditions of the problem we are dealing with.

What is left is to compensate for possible common fluctuations of the polarization in the two pairs of codes, so as Alice and Bob's photons have identical polarization when reaching the BMD device. This can be achieved with a HWP rotated $\pi/4$ degrees, and affecting both cores at the same time. A HWP rotated an angle α with respect to the X axis implements the transform

$$HWP_\alpha = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}. \tag{3.26}$$

Giving the perturbation analysis we made in previous sections, if we set $\alpha = \pi/4$, in order to obtain a Pauli X-gate operation, we can compensate for polarization drift caused by fiber pertubations (residual birefringence).

When the state arrives back at Charlie, perturbations have been removed and information restored. The next part of the process is the Bell state measurement. In this case, it is performed by a integrated device, consisting of three cascaded DCs: one with coupling phase $\pi/2$, implementing a Pauli X-gate operation (interchanging $|a_2\rangle \leftrightarrow |b_1\rangle$), followed by two 3dBs (coupling phase $\pi/4$), implementing BS-like operations. The device is shown in Figure 3.8.

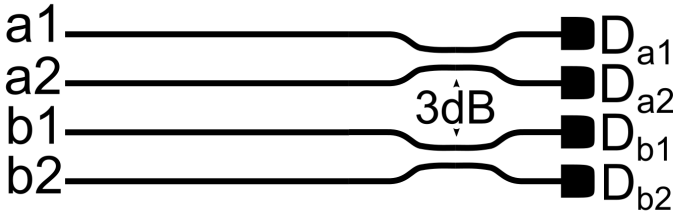


Figure 3.8: *Integrated Bell state measurement apparatus. By cascading three directional couplers in this way we are able to postselect entangled states and perform MDI-QKD. Adapted from own contribution [98].*

The integrated device is coupled to fibers coming from Alice and Bob. At each of the four outputs of the device, detectors are located. With this ingredients, we have enough information to describe how the device performs Bell state discrimination. As the calculations are similar to what we have been doing, it will be sufficient to give the computations for a given input state. The others follow from linearity and/or analogy. Imagine, for example, that Alice and Bob both happen to choose the X basis. For instance, Alice sends the state $|1_{+a}\rangle = \frac{1}{\sqrt{2}}(|1_{a1}\rangle + |1_{a2}\rangle)$ and Bob sends $|1_{-b}\rangle = \frac{1}{\sqrt{2}}(|1_{b1}\rangle - |1_{b2}\rangle)$. The input state can be written as

$$|1_{+a}1_{-b}\rangle = \frac{1}{2}(|1_{a1}1_{b1}\rangle - |1_{a1}1_{b2}\rangle + |1_{a2}1_{b1}\rangle - |1_{a2}1_{b2}\rangle) \tag{3.27}$$

Now, we have the pair of 3dBs DC each one implementing the following transform

$$\begin{aligned} |1_{a1}\rangle &\rightarrow \frac{1}{\sqrt{2}}(|1_{a1}\rangle + i|1_{a2}\rangle) \\ |1_{a2}\rangle &\rightarrow \frac{1}{\sqrt{2}}(i|1_{a1}\rangle + |1_{a2}\rangle, \end{aligned} \tag{3.28}$$

and analogously for Bob (just interchanging $a \rightarrow b$).

With this, Equation (3.27) becomes

$$|1_{+a}1_{-b}\rangle = \frac{1}{4}[i\sqrt{2}(|2_{a1}\rangle + |2_{a2}\rangle + |2_{b1}\rangle + |2_{b2}\rangle) - 2(|1_{a1}1_{b2}\rangle - |1_{a2}1_{b1}\rangle)], \tag{3.29}$$

which can be rewritten as

$$\frac{i\sqrt{2}}{4}|HOM\rangle - \frac{1}{\sqrt{2}}|\psi^-\rangle, \tag{3.30}$$

with $\langle HOM|HOM\rangle = 4$. Thus, we obtain the singlet state with probability 1/2.

Key rate analysis

So far, we have shown how to achieve autocompensation in various MDI-QKD settings, giving the light circulation analysis of the protocol and the actual implementation of the autocompensation transformations. However, we need to show how

such autocompensation is beneficial in terms of protocol performance. We need to make an analysis of the errors that fiber perturbations may cause, and how does that impact the secret key rate. We will particularize this analysis for this particular codirectional mode encoding. In the polarization basis, these has already been studied extensively. This is because we believe the use of MCFs is better suited for QKD purposes, in the sense that, on the one hand, the data rate is a priori bigger, and photonic integration is easier, thus increasing practicality. Eventually, when QKD systems are required to be portable, codirectional modes may be a good option in $SWaP$ terms (SWaP: size, weight and power).

As we know, computation of a key rate involves modelling the relevant sources of errors that may hinder the communication process. We have seen that optical hardware is imperfect, so we shall deal with errors due to multiphoton pulses and detector dark counts. We assume that Eve can perform a PNS attack. Thus, decoy states are required. That means that we have to add a VOA at Alice's and Bob's stations. The VOA acts only on the photons way back, so in the first trip Charlie can send a strong pulse and attenuation can be neglected. Finally, we shall consider that a infinite number of signals is exchanged, *i.e* the key rate will be computed in the asymptotic limit.

But before we go into the computation of the key rate, we will devote some time to discuss the error model of fiber perturbations. This time we opt for an heuristic model. This error will generalize the so-called misalignment error. On the one hand, we know that perturbations tend to accumulate as we propagate along the fiber, so it will contain some dependence with the fiber length L. On the other hand, if the fiber is of infinite length, we assume that the perturbations are strong enough to produce a totally random outcome. At a length equal to zero, only the residual misaligment error should remain. With these conditions we propose the following form for the error, which we dub as *optical error*, which is plotted in Figure 3.9.

$$E_{opt}(L) = e_{opt} + \left(\frac{1}{2} - e_{opt}\right)(1 - e^{-\alpha_{opt}L}). \tag{3.31}$$

Above, we have named the residual misalignment as e_{opt}, to also emphasize its optical origin. The coefficient appearing on the exponential, α_{opt} measures the strength of the perturbations. Typical values will be of the order of 10^{-4} km^{-1}. To justify, in an approximate manner, this order of magnitude, consider the following argument. With a codirectional mode encoding, power transfer to other modes means information scrambling. In MCFs, cross-talk can be around -40 dB/km or lower [121]. Though our results still hold for lower values, evidently if cross-talk can be neglected it does not make sense to use autocompensation. We are dealing with the case of values of cross-talk enough to make compensation a desirable feature.

Recalling that dB are defined as

$$-10 \log_{10} \frac{P_{out}}{P_{in}}, \tag{3.32}$$

that a fraction 10^{-4} of the optical power P in the initial core has coupled into the adjacent core. In that case, bear in mind the dual-rail encoding and consider, for

simplicity, the Z basis. If we had one bit of information per pulse, and ignoring every other error, we have introduced an error proportional to that power transfer, thus of order 10^{-4}.

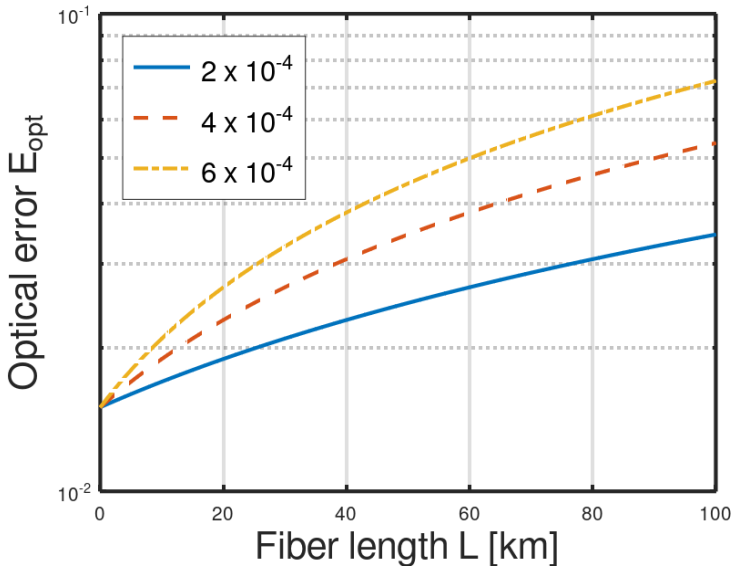


Figure 3.9: *Heuristic optical error E_{opt} ($N = 2$) for various values of the perturbation strength α_{opt} against the channel distance L. The value of e_{opt} is a typical misalignment value of 1.5% [122].*

Note that this error can be generalized for high-dimensional QKD [49], becoming

$$E_{opt}(L) = e_{opt} + \left(\frac{N-1}{N} - e_{opt}\right)(1 - e^{\alpha_{opt}L}), \tag{3.33}$$

where N is the qudit dimension (in the case of qubits –ordinary QKD, then $N = 2$).

Now, we have to introduce the expression in Equation (3.31) into the key rate. There has been extensive work regarding key rate computation in MDI-QKD [123, 124]. We shall follow such analysis and apply it for our case. Note that the Z basis is used, not the Y basis, as it introduces more errors, that can be nonetheless reduced but by complicating the post-processing step [123]. It is easier, however, that we map the Y basis into the Z basis just before detection. Note that a DC with coupling phase $\pi/4$ is enough for the task –recall Equation(2.12).

The aim is to compare the case with autocompensation, where $\alpha_{opt} = 0$ (only the residual e_{opt} remains) with various other cases with different values of α_{opt}. The expression for the lower bound of the secret key rate, under this assumptions, which are in part similar to previous work in the matter [123], is given by

$$R \geq Q_{11}^{Z}[1 - H(e_{11}^{X})] - Q_{\mu_a\mu_b}^{Z} f H(E_{\mu_a\mu_b}^{X}). \tag{3.34}$$

From the previous sections, we recognise here the single-photon *coincidence*[3] gain Q_{11}^{Z} in the Z basis; the binary Shannon entropy $H(x)$; the single-photon error

[3]We need two photons reaching two detectors at the same time in order to have signal.

in the X basis e_{11}^X; the overall gain $Q_{\mu_a\mu_b}^Z$ and error rate $E_{\mu_a\mu_b}^Z$ in the Z basis, considering WCPs of mean photon number μ_a (Alice) and μ_b (Bob); and, finally, the error inefficiency factor f.

Many of the terms of the expression in Equation (3.34) are complicated, and the parameter estimations are cumbersome, so we reserve such equations for Appendix A. Here, we will focus on the results. In Figure 3.10 we plot the secret key rate against the distance between Alice/Bob and Charlie. We call this distance L, so actually the distance between Alice and Bob would be $2L$, as the source, Charlie, is in the middle. The experimental parameters we used are shown in Table 3.3.

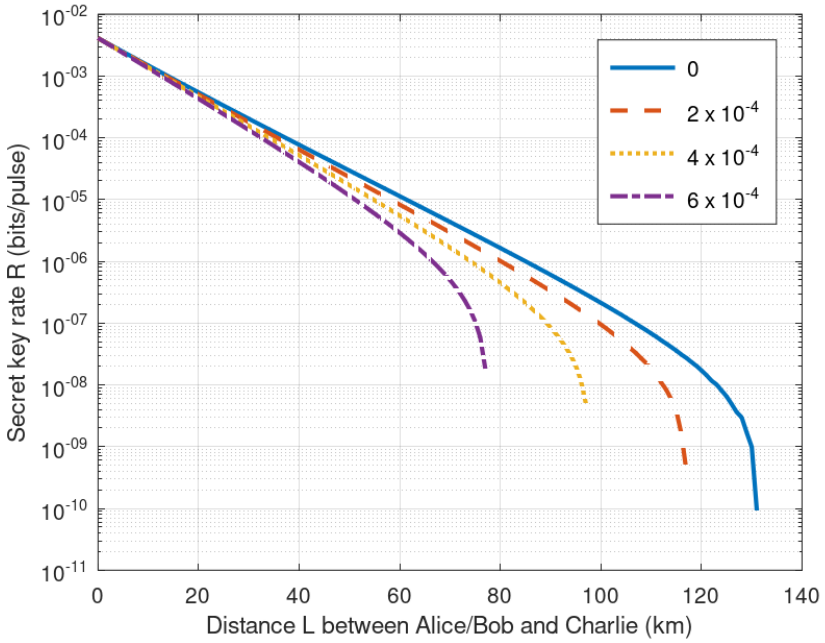


Figure 3.10: *Secret key rate vs Alice/Bob distance to Charlie for various values of α_{opt}. The autocompensated case corresponds to $\alpha_{opt} = 0$. For the other cases, we see that transmission of secret information is clearly obstructed for increasing values of α_{opt}.*

From the figure, we see that the impact of the autocompensation is clear. For increasing values of the perturbation strength, we see a progressive decay of both the key rate itself and the achievable distance. Thus, autocompensation is a good solution.

3.5.3 A-MDI-QKD in the polarization encoding

In this case, we shall describe how to perform MDI-QKD while at the same time enable polarization perturbations mitigation. As this particular encoding is not the focus of the Thesis, and we have already explained how MDI-QKD works in this encoding, we show briefly how to achieve it here.

The protocol layout is analogous to that of collinear (FMFs modes) and codirectional (MCF modes) encodings, as shown in Figure 3.11. Again, Charlie prepares

Table 3.3: *Experimental parameters for the computation of the secret key rate for A-MDI-QKD in MCFs. Note that symmetric scenario with optimal conditions* $\eta_a\mu_a = \eta_b\mu_b$ *and* $\nu_a = \nu_b$ *is assumed.*

Parameter	Value
p_d	$3.01 \cdot 10^{-6}$
f	1.16
e_{opt}	1.5%
η_d	93%
η_C	0.5%
α_{att}	0.2 dB/km
α_{opt}	$\{0.5, 1, 2\} \cdot 10^{-4}$ km^{-1}
μ_a, μ_b	0.36
ν_a, ν_b	0.001

the following input state

$$\frac{1}{2}(|1_H\rangle + |1_V\rangle)_a \otimes (|1_H\rangle + |1_V\rangle)_b. \tag{3.35}$$

The Bell state measurement is performed by the well-known scheme we already explained in the chapter's introduction. What changes now is the delay and the autocompensation (only a bit). For the former, we may employ a PBS connected to a fiber delay in one of its output ports. Then, the fiber feeds back into the PBS at the orthogonal port (see Figure 3.12).

That way, if we, say, have a PBS that reflects horizontal polarization and reflects vertical polarization, by this OFD system we can delay the V-polarized pulse with respect to the H-polarized one.

On the other hand, for autocompensation, we have seen that a HWP rotated $\pi/4$ with respect to the horizontal direction is enough. Also, as this device implements a Pauli X-gate operation, this enables for delay cancellation when the pulses go back to the delay.

3.5.4 Afterword. Multichannel A-MDI-QKD and problems associated with high dimensionality

MDI-QKD has a clear advantages, which is ruling out all the possible attacks on the measurement devices. The detection stage can be untrusted, thus the key exchange is automatically protected against detector side-channels. However, this requires from two-photon coincident detection. This means that the key rate would be lower than for single-photon protocols like BB84, for instance. Without MDI the protocol is not as safe, in the sense it lefts backdoors for adversaries to profit, but still we need the key rate to be large enough to constitute a practical way of transmitting ciphered information. Thus, one must search for opportunities to increase this quantity while maintaining MDI characteristics.

We have focused in error mitigation by passive compensation, which is one way

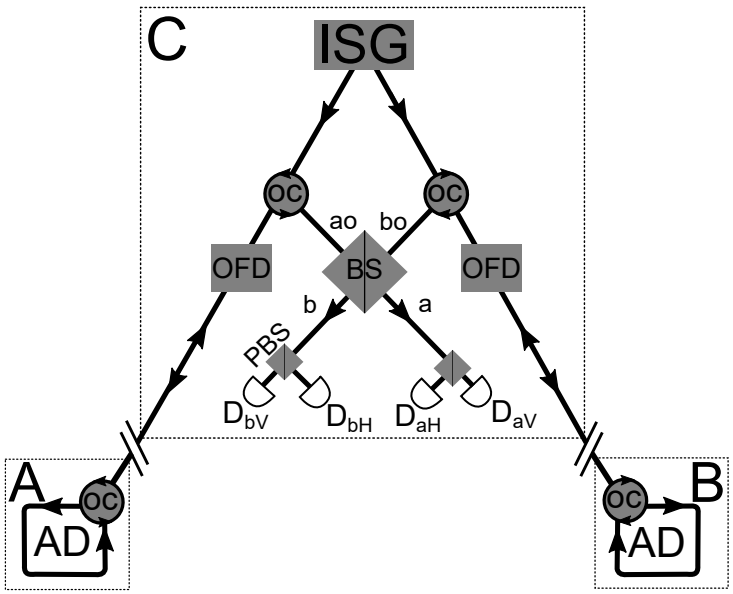


Figure 3.11: *With polarization modes we follow a similar arrangement as with other encodings. The Bell state measurement is performed by the usual Innsbruck-type scheme. Reproduced from own contribution [76].*

to increase the key rate. We have designed autocompensating systems for various encodings. In particular, focusing in such ones that favour implementations in new kinds of fibers intended for higher data rate transmission. We have shown that the benefits of autocompensation and measurement-device characteristics can be successfully merged, and we made a short key rate analysis to support this argument for the case of MCFs. Also, we have shown how to incorporate integrated optic elements into the protocols, emphasizing the advantage of compactness of quantum information processing tasks.

There still room, however, for a small improvement. We described how to perform A-MDI-QKD in a pair of selected cores of a MCF. We can extend this to many pairs of cores [99], making use of other possible core *arrangements*, given the various capabilities of MCFs. The idea is to reserve pairs of cores, that can suffer from cross-talk, or phase drift, which we are going to eliminate by means of autocompensation. To isolate them from others, we may imagine, for instance, that the difference o propagation constants of other modes is big enough so the cross-talk is negligible. Or, we may "switch of" some cores (only a few) that would disturb the QKD ones. Then, each pair of cores would be processed individually, and one would obtain some lower bound of the key rate R, as we have seen. If we have N pairs of cores, then we would have a key rate of at least $N \times R$. The arrangement follows in a straightforward manner from the two-channel systems we already described, and its shown in Figure 3.14.

This idea of multichannel suggests encoding not in qubits, but rather in *qudits*.

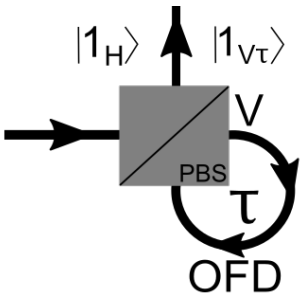


Figure 3.12: *Simple solution for achieving a delay between H-polarized and V-polarized pulses, by means of a PBS and a custom fiber loop. Reproduced from own contribution [76].*

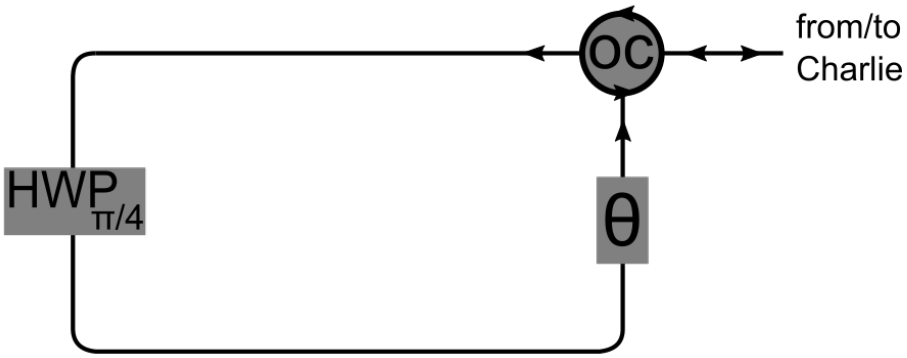


Figure 3.13: *Autocompensating circuit for polarization encoding. A half-wave plate rotated $\pi/4$ degrees is enough to implement the autocompensating transform. Reproduced from own contribution [76].*

That is, instead of two dimensional QKD, we may opt by high-dimensional A-MDI-QKD, or HD-A-MDI-QKD. The use of high-dimensional states has the advantage of greater tolerance to noise, compared to the two dimensional counterpart, which also translates into higher key rates [125].

Nonetheless, turns out that this is not possible in general by practical means [126, 127] (in any case, very far from the P&P philosophy). By using d-dimensional systems, or qudits, we are required, because of MDI to discriminate high-dimensional Bell states, which is a highly nontrivial task. This means we will not go forward at this point, and the topic of HD-A-MDI-QKD remains open. So far, there have some workarounds this problem, which are not true HD, for instance, by projecting the incoming qudits into two-dimensional subspaces [128] or using different d.o.fs simultaneously [129]. In this last case, the protocol is not really MDI, but it is more secure against side-channel attacks than BB84. On the other side, efforts in efficient Bell state discrimination for three-dimensional states has been carried out [130, 131], but still they are experimentally complicated.

Schemes like [128] share some architecture with the multichannel idea, in the sense that measurements are performed pairwise. However, the "parent" state is high-dimensional. This means that autocompensation of such scheme is more com-

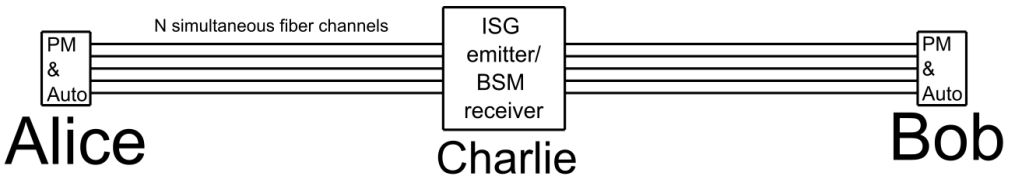


Figure 3.14: *Basic arrangement of an A-MDI-QKD multichannel scheme. It is simply an N-fold realisation of the 2D case. The processing of N simultaneous channels allows for an increase of key rate by a factor N, but no further security is added.*

plicated, as one will in general have perturbations over d dimensions, which implies that the form of the perturbations would be an SU(N) matrix, with $N = d$ ($N = 2d$ if we consider also polarization couplings) [49]. For that case, the nonlinear device proposed there (in [49]) could be an option, provided the Z basis is not used; the bases X and Y can be used. Charlie would need to send blank states which would be then phase-modulated by Alice and Bob in order to encode information.

Chapter 4

Microfabrication and characterization of proof-of-principle integrated optical components for future QKD implementations

The purpose of this Thesis is, in part, two-fold. On the one hand, it is devoted to the development of new or adapted QKD protocols embedded with autocompensation mechanisms. On the other hand, the preferred implementation for many of the required devices is integrated optics, for the various motives already explained. In particular, speed, robustness and stability. Also, high compatibility with optical fibers and very good perspectives for miniaturization of expensive and bulky optical setups (improved SWaP). All of this expectedly would mean a QKD better suited for more stringent environments, for instance those that could require from a certain degree of portability, those which are somewhat uncontrolled scenarios (for example, vibrations) or have strong size limitations etc. As such, we want to exploit this and actually fabricate devices to be intended for QKD purposes, as shown in Subsection 3.5.2 for two-photon states in spatial (path) modes, and also Bell states, as will be seen in Chapter 5 for spatial-encoded Bell states.

. Aiming for full operating devices is a long-term goal, requiring from amounts of time, effort and equipment that surpass by far the possibilities of this Thesis. Thus, we will aim for smaller components that may be, in the future, basic blocks by which to manufacture larger devices destined to tasks like Bell state measurement or autocompensation (Pauli's Y-gate, for instance). In particular, we are interested in passive devices, as their capabilities are good enough for many tasks, as we have seen in the previous chapters. Passive devices are also simpler than active ones, which makes them more robust in that sense, as there are less things that can fail. They are also cheaper and easier to handle.

There exist different platforms for integrated optics [132]. In our case, we opt

for soda-lime glass, which is a versatile and inexpensive material [133, 134]. Waveguiding is achieved by *Ionex*, where atoms of the glass are substituted for others from a different species, modifying its optical properties, and, in particular, the refractive index, in a controlled manner. In order to selectively alter the index, protective aluminium masks are required, which are previously fabricated by *photolitographic* techniques.

In terms of the actual devices, previous work in the group's laboratory led to microfabrication of DCs [48], which, as we saw, is a basic integrated optic element. As well as testing the reproducibility of this, we want to add a new element, which are phase gates. As we saw, with DCs together with phase gates we can achieve universal single qubit operation.

The microfabrication of devices involves the computerized design of masks, then the photolitographic stage, then Ionex and then characterization. Regarding the latter, some testing with the microscope, both by optical inspection and by phase retrieval methods. Then, a semiclassical characterization is due. In this case, light from a laser source needs to be coupled into the waveguide arrays and then observed at the output. This will be achieved by the *m-lines* or *prism coupling technique* [135, 136, 137]. In the following sections we shall describe in detail all this stages of fabrication and subsequent testing. We will break down the principal aspects of the microfabrication technique we employed, as well as the principles behind the mask design. A flowchart encompassing all steps can be found in Appendix B.

The testing and characterization results (last sections of this chapter) where obtained from a mask fully fabricated at the group's lab at the USC, along previous group results [48, 138]. Two photoreduction stages were required, following design and pattern printing. Note that the use of the ionic-exchange process implies that the waveguides are of the GRIN type. This means that the refractive index profile is complicated. And it is complicated enough to prevent from accurate analytical models of modes and light propagation. Also, it makes simulations like beam propagation method (BPM) difficult. Because of this reasons, we shall work under a number of approximations, which we shall describe along the process.

4.1 Mask design

The first step is to realize aluminium masks which will allow later for selective modulation of the glass refractive index. This has two stages: first, the design phase. This is done with a computer. Then the pattern is printed with an ordinary printer (albeit a good one), in black & white and a special sheet of paper. Due to this fact, we employed the graphics suite *Inkscape* for design. Although it is not a CAD software, rather a creative illustration software, focused on vector image design, it enables for good pattern production, enabling the definition of custom parametric curves that will define some of our integrated structures.

As said, we want to implement phase shifters. In Section 2.2.1 we showed that a way to achieve this is to start from a given channel waveguide and then increase its width so as to increase its effective refractive index. Such given waveguide will

operate in the single-mode regime, and will have its parameters adjusted for that matter, according to the approximations used.

The phase shifting will then be performed by waveguides with larger width than those of the rest of the integrated device. This new width may be big enough so more than one mode is allowed. In fact, in our waveguides, two modes are allowed, as the wider sections (or *phase sections*) are a bit above cut-off. In order to connect the wider portions with the rest, and still have single-mode operation, we need to make use of horn-like structures called *tapers*. In particular, these tapers need perform adiabatically. That is, the transition between waveguides needs to be done in such a way that only the original mode is guided, and no higher order modes are excited. To carry on with this, we opt for following previous work on the matter [139], where adiabatic operation is achieved by using a parabolic geometry satisfying certain conditions. Note that, were the phase sections thinner, then the tapers would have to be much bigger (in length), thus in conflict with the general objective of miniaturizing optical components. The shape of the taper is shown in Figure 4.1. We leave for later the mathematical treatment.

Figure 4.1: *Adiabatic taper geometry [139], in this case joining a thin waveguide together with a wider one. This very shape is used also to couple light in and out of the MZIs. The shape of the curve is parabolic.*

In order to have an estimate of the involved refractive indexes, ensure single-mode operation and so on, we need to have some quantitative model of our waveguides. As said, the ion-exchange process makes the guides GRIN, and that complicates the mathematical analysis. Note that even for simpler configurations, like step index, closed-form expressions are not always possible, requiring from approximations or numerical computations [140].

We have, however, some room for working. Consider first that the wavefront of the guided modes are plane waves

$$e^{-i\beta z} = e^{-i\frac{2\pi}{\lambda_0}n_{eff}z}, \tag{4.1}$$

where λ_0 is the wavelength in vacuum. The n_{eff}, for the lowest mode, is the goal parameter, and, as we said, it is in general difficult to do so. TE and TM have different propagation constant. On what follows, we shall work with TE polarization and design our devices accordingly. Note that this should limit the performance of our devices if there was any polarization change through the structure, which we know from previous results that there in fact is [48]. However, we also know it happens to be not too critical.

As we have confinement in both the x (depth) and y (width) direction (*channel waveguides*), resolution of the wave equation is not easily tractable unless we restrict

to a simpler case. It becomes easier to deal with if we assume that the index profile $n(x, y)$ is indeed separable, being only a function of depth (x) but a constant in the lateral dimension (y). This is shown in Figure 4.2 for a superficial GRIN channel waveguide.

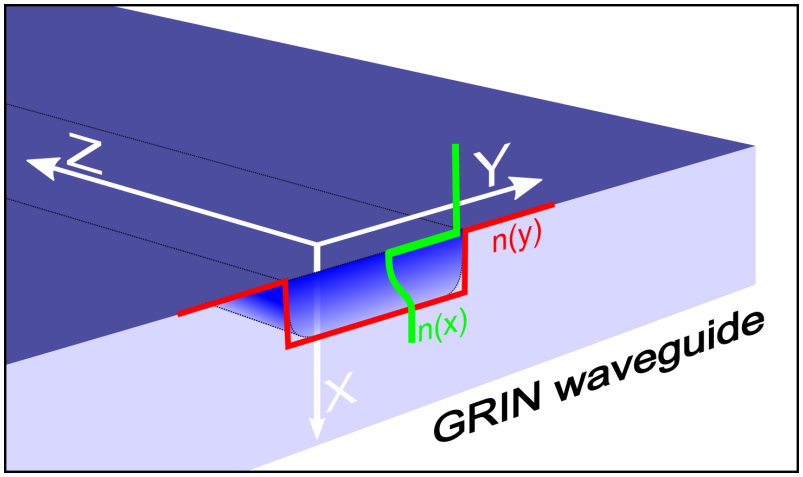


Figure 4.2: *Schematic representation of the refractive indices on a superficial GRIN channel waveguide, under the refractive index separability assumption. The profiles are to be taken as simplified qualitative illustrations, highlighting the different treatments in the x and y directions.*

What one does is actually take the two-dimensional refractive index profile $n(x, y)$ and fix a value of y, so that it becomes $n(x, y_k)$, with k a real number, and then solve for the resulting planar waveguide modes. One obtains a value of the planar effective index $n_{eff}(y_k) = n_p(y_k)$ for each slice along y. Doing this k times allows for reconstructing the index profile along y, and the modes are solved as planar waveguide modes this time assuming confinement on y direction, as shown in Figure 4.3. In particular, we assume $n_p(y_k) = n_p$ (constant), thus the reconstructed profile in the y direction is a step-index one.

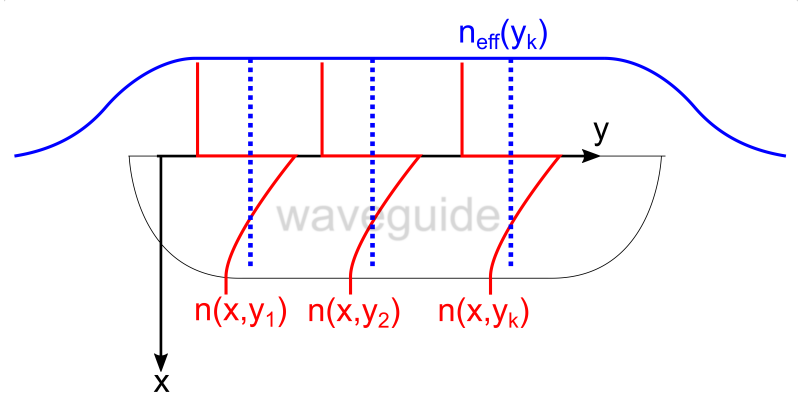


Figure 4.3: *Representation of the effective index method for a superficial waveguide. One takes a slice in the y direction and solves in x, sampling multiple slices in order to reconstruct the refractive index profile. For buried waveguides, this is totally analogous.*

In other words, under the effective index approximation, the wave equation becomes a pair of uncoupled equations, one in the x direction and one in the y. The equations we obtain are formally equivalent to the Schrödinger equation of a particle under the influence of a potential V, albeit the potential is inverted. In this case, V is a function of x and y, respectively, while for step index waveguides it would be a constant. In the integrated optic case, the role of V is played by the index profiles $n(x)$ and $n(y)$. The different discrete values of n_{eff} would correspond to the particle's energy levels. For single-mode waveguides, we have one such value. It lays between the maximum value of the refractive index profile and the bigger of the index values at the interfaces, *i.e* the substrate, as seen in Figure 4.4.

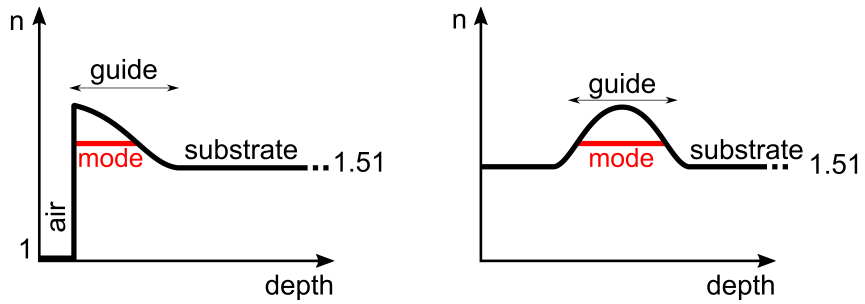


Figure 4.4: *Schematic of the refractive index structure of a single-mode superficial (left) and buried (right) GRIN waveguide, showing the analogy with the potential well in QM. The index profiles do not intend to be accurate, but illustrative.*

If one is familiar with QM, one may know that a way of dealing with non-constant potential wells is by means of the Wentzel-Kramers-Brillouin (WKB) approximation. That same equation can be used here. Special care needs to be taken when joining the solutions in the turning points, where $n_{eff} = n(x)$ (the same would go for y). Two cases need to be distinguished: whether the waveguide is superficial; in that case there is an abrupt discontinuity at the surface; or whether it is buried. In that case, the index falls softly down to the substrate index n_s. This is the case we shall consider, as we will bury our waveguides. This has the advantage of protecting them against damage in the surface due to contact with some element during sample manipulation. With these conditions, we arrive at the useful expression [141]

$$\frac{2}{\lambda_0}\int_{x_2}^{x_1}\sqrt{n^2(x)-n_p^2}dx = m_x + \frac{1}{2}, \tag{4.2}$$

where x_1 and x_2 are the turning points, $n(x)$ is the index profile in depth and m_x is the mode number in the x direction. For the fundamental *planar* mode, we have $m = 0$. This equation assumes only confinement on one direction, thus n_{eff} inside the square root is actually a planar waveguide effective index, and we call it n_p. For the case of width we proceed similarly, but in that case we assume that the index profile is a step-index one. Its value will be equal to that of the effective index of the planar waveguide index n_p (with depth index profile given by $n(x)$), as in the equation above. Thus, for the lateral dimension y, considering the turning points

situated at $-w/2$ and $w/2$ ($w \equiv$ width) the relevant equation is

$$\frac{2}{\lambda_0} w \sqrt{n_p^2 - n_{eff}^2} = m_y + \frac{1}{2}. \tag{4.3}$$

In virtue of the effective refractive index approximation, this value of n_{eff} coincides with that of Equation (4.1) (for $m_y = 0$). In Equation 4.3 above there is an interplay between two approximations: on the one hand, we assume a constant index profile, so the square root is trivially integrated, while at the same time the GRIN approximation is used to compute the phases, ending up providing an amicable and reasonable expression to work with.

The mode index m_y is independent of m_x. Note that we can have only one mode in the x direction but more than one in the y direction, if we do not control the width properly.

To measure the phases we use a Mach-Zehnder configuration (see Figure 4.5. We make use of previous results [138] to obtain 3dBs DCs with waveguides of target (or nominal) width of 2.7 microns[1]. In particular, we take the lines relating coupling phase to coupling length and we make a linear interpolation to obtain a pair of values l_c and d_c, representing, respectively, the coupling length and the distance between waveguides (from center to center), in order to achieve a coupling phase equal to $\pi/4$. The value of d_c takes already into account lateral diffusion, as it is deducted from actual experimental curves. Some error is introduced if lateral diffusions do not coincide between previous experimental results and the microfabricated samples for this Thesis. We expect this error to be small, as we will use diffusion times derived precisely from such previous results (they ended up being a bit different, for reason we soon explain).

To approach the waveguides and achieve coupling we need low loss S-bends, of the Minford type [142], which follows the relationship

$$u(t) = \frac{h}{l} t - \frac{h}{2\pi} \sin\left(2\pi \frac{t}{l}\right), \tag{4.4}$$

where t is the horizontal coordinate, u the vertical coordinate, h the maximum height of the curve and l its full length. This curve retains its shape when scaled, as can be seen by defining $u' = u/h$ and $t' = t/l$:

$$u' = t' - (2\pi)^{-1} \sin 2\pi t'. \tag{4.5}$$

The optimal length and height for the Minford curves in our samples are also obtained from previous results [138]. The final design is shown in full in Appendix C. Note that apart from the phase shifters, which is the focus of this chapter, we have included other elements, most of them for testing which were left unused due to various reasons.

[1]Other 50/50 power dividers could be used, instead, like Y-junctions or maybe multimode interference couplers (MMIs). However, as that would require for extensive additional works, specially in the case of MMIs, we opted to build on previous research group knowledge while also testing for reproducibility. Realization of MMIs can be maybe considered as an objective for the future.

Note also that, when they are close to each other, part of curved sections the Minford structures also contribute to coupling, but that is already taken into account in calibrations in [138].

We have also put tapers at the input and output of the waveguides (they are interchangeable, as the device is symmetric), to allow coupling to a prism, as will be explained later. Else, we should cut and polish the input and output faces of the chip in order to couple light and recover it. However, polishing is a very time consuming task. This exit tapers are enlarged the maximum as possible, in order to achieve maximum overlap with the incoming beam.

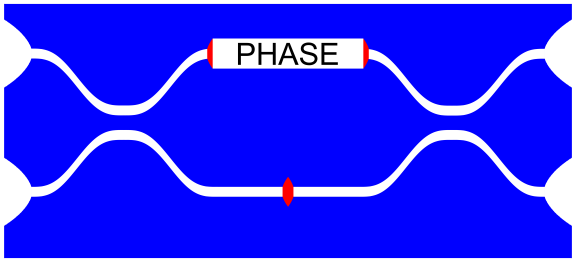


Figure 4.5: *Exaggerated representation of the designed integrated MZIs. We have tapers at the input and output. Two 3dBs couplers, consisting on Minford curves and a straight intermediate section of length l_c, at a edge-to-edge distance d_c, divide the incoming light in half for maximum visibility. Then in one arm, the widened waveguide provides phase-shifting. Finally, light is brought into interference by the second 3dBs coupler.*

Secondly we have put, in the reference waveguides, *two contiguous tapers facing each other* so the contributions of the tapers of both arms (red sections in Figure 4.5) cancel each other. The phase of the interferometer only depends on the effective index difference between the widest section in the upper arm and the channel waveguide with the same lengh of the lower arm. That is, the phase difference is only because of the change of width. The tapers do not contribute to the phase. We have done this because when designing we were working under various approximations, that we want to have the lesser impact on the potential experimental results. Thus, doing the integral corresponding to the phase introduced by the taper would likely cause an appreciable deviation from the desired behaviour. The equation that the taper's width verify is

$$w(z) = \sqrt{\frac{2\alpha\lambda_0}{n_p} z + w_0^2}, \tag{4.6}$$

with α an dimensionless parameter restricted to ≤ 1, meaning that a parabolic profile with spreading less than ($\alpha < 1$) or equal ($\alpha = 1$) to the one above will be 'slow' enough to make the coupling to higher modes minimal. In particular, the walls of the taper increase slower than the mode would diffract, so it gets gradually redirected without coupling to higher order modes. The parameter w_0 is the input width of the taper, which widens as a square root function of z ($w(z)$) until a given length. Actually, according to [139], the quantity λ_0/n_p should rather be λ_0/n_{eff}, with n_{eff} the effective refractive index of the *lowest* (local) mode. However in our case we do not know n_{eff} with precision, so we approximate it by its maximum

value (in width) n_p for this particular case. The actual value of λ_0/n_{eff} would be bigger ($n_{eff} < n_p$), but the tapers should work because have some flexibility, as we can absorb this deviation into the parameter α, which would become less than one.

To compute the phase introduced by the wide region *on the fundamental mode of the channel waveguide* we apply the WKB method in the y direction. Specifically, our working equation results from inverting Equation (4.3) and obtain the effective refractive index of the fundamental mode ($m_y = 0$) as a function of the width w

$$n_{eff}(w) = \sqrt{n_p^2 - \left(\frac{\lambda_0}{4w}\right)^2}. \tag{4.7}$$

Now, we see clearly how it changes with different widths. Thus, for the same propagation length Δz, the phase difference between the mode propagating along the ordinary waveguide (w_0) and the widened waveguide (w) is

$$\phi = k_0 \Delta z [n_{eff}(w) - n_{eff}(w_0)], \tag{4.8}$$

In the equation above, $n_{eff}(\omega_0)$ is a constant, and it is computed by applying Equation (4.7) at the width of the waveguides (thinner regions), at the nominal value of 2.7 μm *corrected* by a expected lateral diffusion of 0.8 μm on each side (1.6 μm total widening due to Ionex).

Given the special relevance of the π phase, we fix it in Equation (4.8) to obtain a relationship between the width and the propagation length, as shown in Figure 4.6-(a). We want the phase shifters as short as possible, recalling miniaturization as one of our goals. At first glance, increasing the width reduces, as expected, the length. However, this also increases the taper's length. In fact, inverting Equation (4.6) one finds that

$$z = \frac{w(z)^2 - w_0^2}{2\alpha(\lambda_0/n_p)}, \tag{4.9}$$

thus increasing with $w(z)$.

Hence, we need to also take into account the tapers length. We have to add to Δz twice the taper's length (call it z_{tap}) for a given width, and optimize accordingly. If we plot $\Delta z + 2z_{tap}$ against the width we find a minimum (see Figure 4.6-(b)) at 9.6 microns, or 8.1 microns in the mask, subtracting the lateral diffusion, imposing the condition of the printer's resolution at 0.3 microns. With this value we go back to the length v. Δz plot and find the phase shifter length, which is 879.12 μm, and we round it to 879 μm.

Then, we use this as the starting point and sample various lengths in the hope of obtaining an oscillatory behaviour when comparing the output intensities against said length. As we removed the parabolic section from the equation, the phase in the MZIs should be linear with the wider section length.

Finally, note that, in the mask (Appendix C, we have reserved some devices to check for the DCs performance, in case some variation was observed, which could

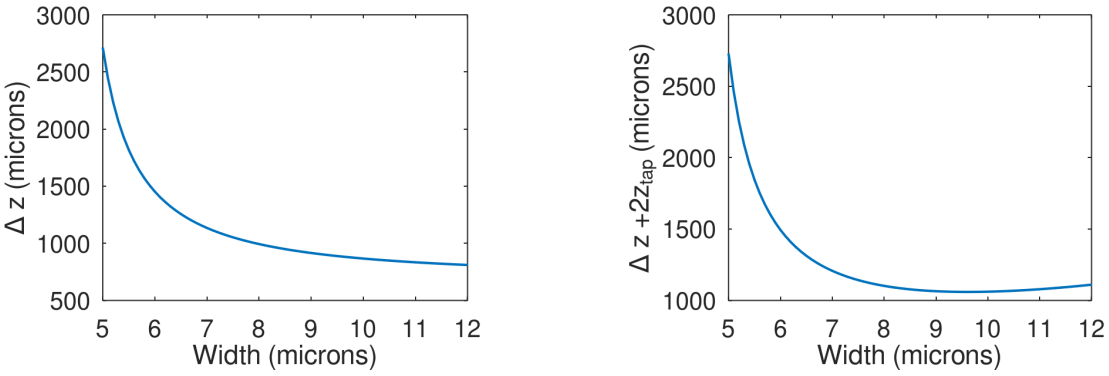


Figure 4.6: *(a) Curve representing the relationship between propagation length and width for the wider region (phase shifter) to introduce a π phase. (b) Same curva as in (a) but taking the taper length into account. The minimum indicates the optimal width for the phase shifter.*

then be corrected. Other marks in the mask are for reference and measuring purposes (ruler marks).

In Table 4.1, there is a summary of all the design values of the mask. These include the (thinner) waveguides width, the entrance/exit tapers max. width, the wider sections width and length (for a π phase), the Minford curves parameters, and the coupling length and distance of the 3dBs couplers.

Table 4.1: *Mask design parameters, including the design wavelength and the relevant refractive indices. Every length and width is given in μm. The value of n_p was obtained by previous calibrations with the Metricon apparatus [48], while the value of n_s is known.*

Design parameter	Value (μm except refractive indices)
λ_0	0.633
n_p	1.51165
n_s	1.5100
w_0 (thinner)	2.7
w (wider)	8.1
w_{max} (i/o tapers)	18
Δz (π, wider)	879
h (Minford)	15.3
l (Minford)	1520
d_c (coupling distance)	3.9
l_c (coupling length)	32.1

4.2 Photolithography and ion-exchange

In the following sections, the process of microfabrication is described, once the mask design has been validated. The process will now describe have the nice property of

a high degree of reproducibility. Though more standarization would be desirable in the future, calibration of softbaking, photoresist development and wet etching times, as well as diffusion times had been extensively done in the past, being within the research group's expertise [143, 144, 48]. We shall benefit from that knowledge to apply it to our samples, thus accelerating and better-controlling the fabrication process. It needs to be pointed out that other masks, apart from the one that gave out successful results and others produced similarly were fabricated, in a different place and with a slightly different technique. In particular, intermediate samples (the bigger ones) were produced at the International Iberian Nanotechnology (INL) facilities i.e cleanroom, by means of *direct laser writing*. Then they were photoreduced, developed, etched and ion-exchanged at USC. However, these samples turned out to be unproductive, and no signal or relevant data was obtained from them, likely due to weak guiding because of insufficient developing in the second photoreduction stage.

4.2.1 Lithography

For this process, samples need to be prepared the following way. First, a thin layer of aluminium is *vapour deposited* on the (exhaustively cleaned) glass substrate. The aluminium is resistant enough to allow Ionex only in the desired regions. The aluminium layer is then *spin-coated* with a positive photoresist.

We have two kinds of samples: a) smaller ones, which are microscope slides of area 25 x 75 mm, and 1 mm thick; and b) bigger ones, of area 50 x 75 mm, and 1 mm thick. The smaller ones are directly used as final samples, while the bigger ones are *intermediate masks*. They are intermediate because the pattern imprinted on them can be photoreduced and engraved again into a smaller sample.

The two stages of photoreduction are similar. In the first one, an intermediate mask is prepared and located on a custom optical system. Below the optics, the printed pattern is located. It is illuminated by with Hg-based general purpose lamps, containing the 436 nm line the photoresist is more sensitive to. Light is reflected in the white regions of the pattern, and then focused by the optics (a Xenon-Sapphire 4.5/95 lens from Schneider-Kreuznach) onto the sample, in the regions where we want our waveguides. This step achieves a negative magnification of -1/14.11×. The light generates a chemical reaction in the exposed regions of the photoresist that increases its solubility. After this photoreduction process, photoresist *developer* is poured into the sample while it is rapidly shaken for the right amount of time (prior calibration has been performed). This is adjusted by iteratively checking with the optical microscope, and also making use of prior knowledge accumulated by the research group. Then, the pattern emerges. The complementary regions are still covered by the photoresist. The sample is then submerged into acid and agitated, hence the aluminium gets *etched* in the regions without photoresist. The remaining photoresist is then eliminated with acetone. The final result is a glass substrate with an aluminium mask on top, the metal being absent where we want our waveguides to be.

The mask elaborated by means of the procedure above will play the role of the pattern in a second photoreduction process, by which we achieve a negative

magnification of -1/5×. The setup is similar: violet (436 nm) light traverses, in this case, the intermediate mask, getting blocked by the aluminium except where it has been etched. As before, light arriving from those regions is focused, into a smaller sample this time, sensitizing the photoresist in the regions where the waveguides are going to be. After this photoreduction is performed, the sample needs again to be developed. This requires, again, from submerging it in developer and agitate it. The next step is the wet etching of the aluminium. Finally, the mask is ready for ion-exchange. The whole process is shown in Figure 4.7.

The two stages give a combined reduction factor of 1/70.55 on the original pattern dimensions. The microfabrication resolution is limited by 1/70.55 times the printer resolution. In particular, it is capable to print at 1200 ppi. (points per inch). Thus, as 1 in=25.4 mm, the final resolution on the masks is $25.4/(70.55 \cdot 1200) = 0.3$ μm. Our thinnest structures are designed to have a width of 2.7 μm; this particular value ensures single-mode operation even after Ionex and is also a multiple of the printing resolution.

Various other factors, together with the limited resolution, influence the widths of the masks. In particular, the development and etching process are critical. Incorrect and/or inhomogeneous focusing during the photoreduction stages is also a essential factor, and a possible source of defects in the development process.

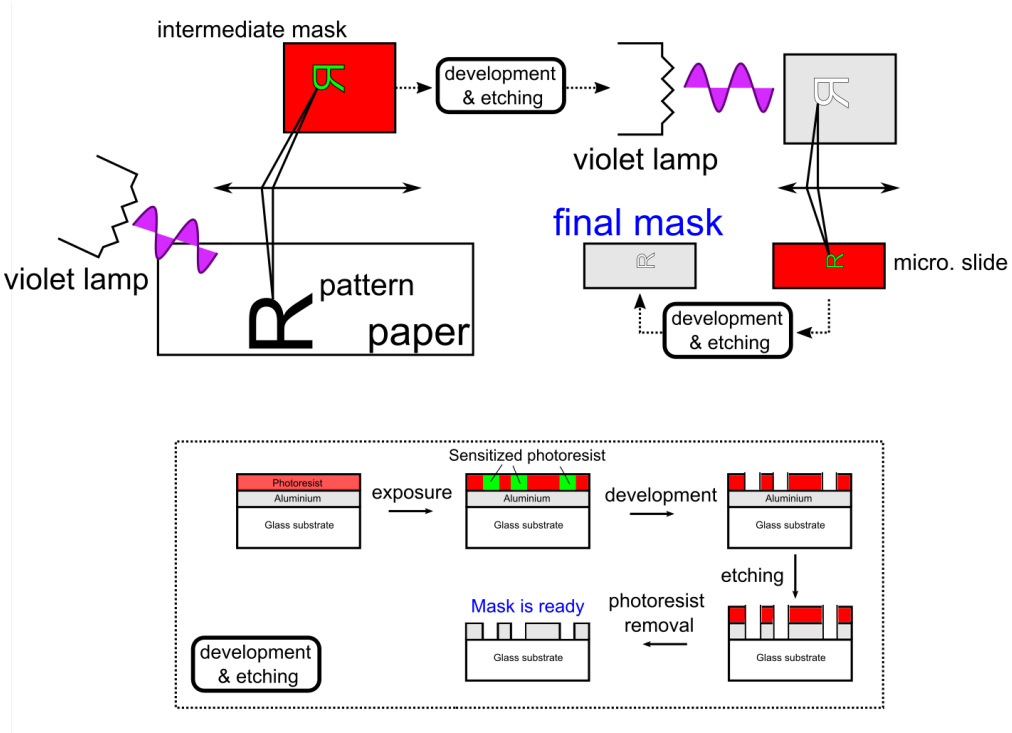


Figure 4.7: *Schematic representation of the photolithographic process. The paper-printed pattern is imaged and engraved into a previously prepared sample: a glass substrate with a layer of vapour-deposited aluminium and spin-coated photoresist on top. Then, this is developed and etched. The resulting intermediate mask serves as a pattern to image and engrave again in order to obtain a smaller, final sample.*

4.2.2 The ion-exchange process

In this technique, the sample is submerged in a fused salt at a high temperature by means of an appropriate furnace. In particular, we use a potassium salt, of composition KNO_3. The surface of the glass, unprotected by the aluminium, is in direct contact with the salt. Due to the thermal excitation, sodium ions of the glass migrate into the salt, while the potassium ions follow the opposite route. The result is that the glass is doped and the refractive index changes. Such change is sensible to factors like temperature and the time the sample is immersed (*diffusion time*). Fortunately, extensive calibration had been performed in the past [48], so we can use that knowledge to obtain the suitable index for our samples.

Note that the value of n_{eff} is not obtained; what was actually calibrated was the value of the equivalent planar guide index n_p. This can be known with great precision by fabricating different planar waveguides (just by submerging a glass substrate), and keep them for different diffusion times, for a fixed value of the temperature (the furnace is equipped with a temperature controller). Then, the effective indexes of these waveguides are measured with a commercial automated prism-coupler device (Metricon Model 2010/M). To sum up, for our samples, the variable we need to control in this process, are the diffusion time and the working temperature.

Not only because of the ionic substitution the diffusion time is critical. Also, some exchange happens under the mask (*lateral diffusion*), as we mentioned. This makes the waveguides wider, also affecting the value of n_{eff} and, importantly, we insist, may turn a single-mode waveguide into a multimode one if not properly controlled for. In general, both the waveguide depth d and the lateral diffusion, which is of the same order of magnitude as the depth [48], obey the following relationship $d \propto \sqrt{t}$, where t is the diffusion time.

The ion-exchange process we use has two steps, as the final samples are buried waveguides, which have the advantage of a more symmetrical index profile and enhanced protection against scratches and surface irregularities resulting in undesirable propagation losses. First, with the aluminium mask present, one diffusion is carried on (in a KNO_3 salt). In the case of the sample under consideration, it was submerged in the salt for 32' diffusion time (measured when the sample leaves the salt[2]), with a preheating stage of 20' duration, in order to make smoother the temperature transition. The target time was 30', but the sample fell inside the tube and we had to "rescue" it, which took approximately 2' time. Measurements of the planar index with the Metricon gave the value $n_p = 1.51260(12)$ for TE polarization.

Then, the aluminium is removed, and another diffusion happens, this time with a $NaNO_3$ salt and different diffusion time. This diffusion is intended to bury the waveguides. This diffusion causes at least two things: first, it widens the waveguides also, but it reduces the effective refractive index. Because of this, there is "interaction" between the two diffusion times, and adjustments in the first one influence the other. For this mask, the original target burying diffusion time was 10', but we left it an additional $\simeq$40" to compensate for the extra time during superficial diffusion

[2]Note that there is still some Ionex going on at this point, but rapid cooling outside the salt drastically slows down the process.

(10/30× 2'=40"). The refractive planar index measured with the Metricon yielded $n_p = 1.51173(11)$ (TE).

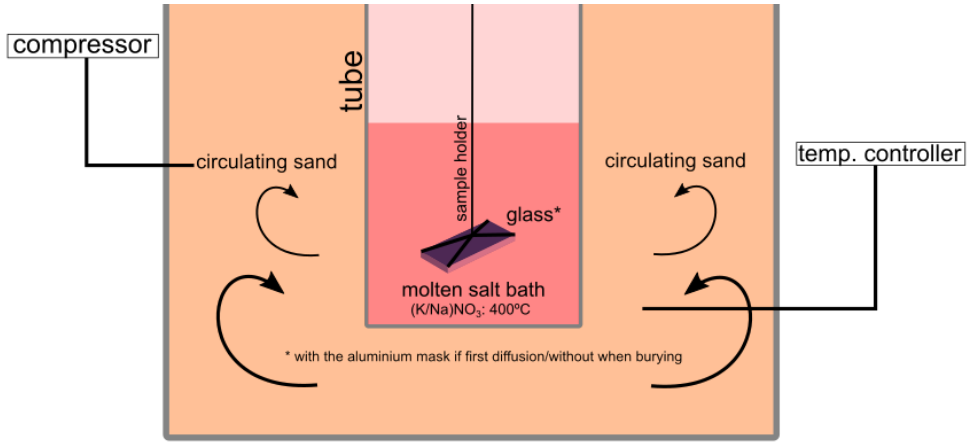


Figure 4.8: *Schematic representation of the furnace treatment for Ionex. The sample is tightened to a steel wire frame screwed to a metal stick for safe manipulation. Then, the whole apparatus is submerged for the specified amount of time in the fused salt, which is kept at a constant temperature.*

As a final remark, we may point out that the ion-exchange process is a complicated diffusion process, with its theoretical modelling and numerical resolution being far from easy [145]. It involves the analysis of various coupled non-linear partial differential equations. This all makes the prediction of the final refractive index variation a hard task. For that matter, to control this parameter, we have preferred to use an effective relationship with the diffusion time, as per previous calibrations, which take into account also particularities of the setup (furnace characteristics, sample holder characteristics...).

4.3 Fabrication testing by optical phase retrieval

To make sure the previous steps worked as expected, the samples need to be properly examined. We do it two ways. First, the sample is put under an optical microscope and is then checked by visual inspection. The pattern can be scrutinized and some measurements made (widths), by knowing just the objectives magnification and the camera's pixel pitch. If the aluminium mask is present, this is straightforward. If Ionex has already taken place, integrated structures, both superficial or buried (glass is transparent) can be still seen: a shadowy image of them appears under the microscope. However, in this case, we require for more sophisticated and precise methods to make measurements. Indeed, consider the fact that, given that we have in-depth index variations of the refractive index, the samples will act, for light traversing it perpendicularly to the surface, as a phase element or phase mask. Thus, they can be characterized with phase retrieval techniques.

Such method will allow us for checking widths also, and give an idea of waveguide

depths[3] in terms of phase. It is based on differential interference contrast (DIC) microscopy [146, 147], and, in particular, in the *de Senarmont configuration* [148]. This, in turn, is combined with the well-known four-step (4step) phase shifting algorithm (PSA) [149, 150] to retrieve the phase [151]. DIC microscopy is a method to recover information the phase of an object which could be transparent. It is based in the interference of two identical images of the object transversally displaced for an small amount s (the shear), which is lesser than the microscope resolution. So, the phase derivative along the displacement direction produces an intensity variation that is easy to detect, while the duplication of the image is not yet apparent. The double image is generated by a Nomarski prism which is similar to a Wollaston one. As each image has its own polarization, an analizer is necessary in order to they interfere. Moreover, we can control the polarization of the illumination beam with a 'de Senarmont' retarder in order to introduce an arbitrary phase difference δ between both images.

4.3.1 Optical setup and image acquisition

The full setup is shown in Figure 4.9. Light coming from the source needs to be coherent and properly collimated; for that matter, the diaphragm needs to be closed enough. This limits the amount of light. Even so, it is crucial that there are not saturated pixels, otherwise we would loose intensity information.

In the setup we use, which actually is that of a commercial DIC microscope (Nikon Eclipse Ni-U) in the de Senarmont configuration, the *bias retardation* is controlled by rotating the polarizer before the QWP. The QWP axis is kept fixed at 45^{o} respect to the displacement direction (shear) of the Nomarsky prism and aligned with the pixel array of the camera. This bias retardation is twice the angle between the polarizer and the QWP and equal to the phase introduced in the 4step algorithm. We call it α. Note that the QWP is only a true QWP for a given wavelength, which in this case lies in the green part of the spectrum, and has been calibrated to be around 500 nm ($\simeq 500 \pm 50$ nm). Thus, a green filter needs to be included in the setup (532 nm is enough for our purposes), after the light comes from the source.

In the ideal 4step PSA the phase $\varphi(u, v)$, which is a function of the spatial coordinates u and v in the image, is obtained by means of the following equation

$$\tan \varphi(u, v) = \frac{I_{3\pi/2} - I_{\pi/2}}{I_{\pi} - I_0}, \tag{4.10}$$

where $I_\delta = I_\delta(u, v)$ is the interferometric image acquired with the de Senarmont retardation adjusted to a δ phase. This equation is readily obtained from the expression of the interferometric intensity between two coherent beams of intensities I_1 and I_2

$$I = I_1 + I_2 + 2\sqrt{I_1 I_2}\cos(\varphi(u, v) + \delta), \tag{4.11}$$

[3]If required, more information could be gathered by assuming some model for the index exchange profile [48]. By applying the phase retrieval method first for superficial waveguides and then buried ones, an approximate value of the index variation can be obtained.

by setting the values of $\delta = \{0, \pi/2, \pi, 3\pi/2\}$ and operating accordingly. In our case $\delta = 2\alpha$. In addition, we need to account for a phase background introduced by the Nomarsky prism, which we shall represent by a residual phase $\epsilon(u, v)$. Then:

$$\tan[\varphi(u, v) + \epsilon(u, v)] = \frac{I_{3\pi/4} - I_{\pi/4}}{I_{\pi/2} - I_0}. \tag{4.12}$$

Then, $\epsilon(u, v)$ can be removed by moving to a region of glass without waveguides, and then applying the 4step algorithm for a set of four photographs taken there. That will provide the background phase, which can then be subtracted from the full phase. From the 4step-PSA we directly obtain $\varphi(u, v)$, which actually is a difference of the phase ϕ between two points of the object located along the shear direction:

$$\varphi(u, v) = \phi(u+s, v) - \phi(u, v) = \Delta_u \phi(u, v) = \left.\frac{I_{3\pi/4} - I_{\pi/4}}{I_{\pi/2} - I_0}\right|_u - \left.\frac{I_{3\pi/4} - I_{\pi/4}}{I_{\pi/2} - I_0}\right|_{bckg} \tag{4.13}$$

Rotating the sample 90 degrees provides a measurement of the phase difference on the perpendicular direction. Then the images are de-rotated by software. Note that care needs to be taken in order to consider the camera's pixels orientation. Thus, to sum up, we acquire twelve images: four for the phase difference in the u direction, four for the phase difference in the v direction and another four for the background (bckg).

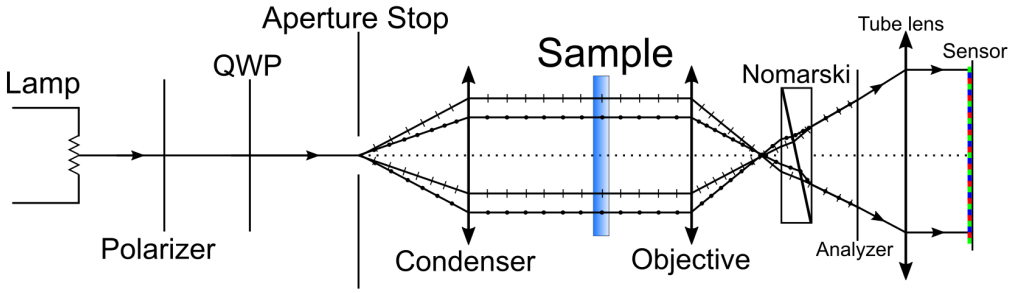


Figure 4.9: *Optical setup of the Nikon microscope in the de Senarmont configuration for DIC imaging. Light flows from left to right. Slashes/dots on the rays represent different polarizations. Light from the lamp traverses the polarizer and the quarter-wave plate, until it reaches the apertures stop, which should be almost closed to obtain a good degree of coherence in the outgoing light. Rays are made parallel by the condenser lens, and they traverse the sample. Then, he different polarizations travel without interference. The Nomarski laterally displaces each polarization in a different amount. Right afterwards, an analyzer is located. Finally, light is collected in the camera sensor.*

Photographs are stored in Nikon's raw format (.NEF files) and then converted to .pgm files with the DCRAW software. Once the images are loaded by the GNU Octave script, the "green pixels" are selected, taking into account the Bayer mosaic pattern (actually, half of them are selected). The images thus obtained are ready for further processing.

4.3.2 Image processing

The acquired images are phase differentials along the Nomarski shear s direction. This value of s in the image plane is independent of the objective since the Nomarski prism is located behind it. The particular value of s has been obtained by previous researchers working with the DIC microscope and *camera* used here (Nikon D750). It's value is approximately $s = 1.375$ pixels for the camera used, whose pixel pitch is 5.95 μm. As we use an objective with 50x magnification (Nikon TU Plan Fluor 50x/0.80), the shear becomes $1.375 \times 5.95/50 \simeq 0.12\mu$m in the object plane. In other words, the shear is small enough to justify establishing the following approximate relationship

$$\frac{\Delta\phi}{s} = \partial\phi \tag{4.14}$$

on each coordinate.

What we measure is indeed $\Delta\phi$. Rotation of the sample 90^{o} provides thus, after dividing by s, derivatives along the shear direction (u, v coordinates), i.e

$$\begin{aligned} s^{-1}[\text{Image at } 0\,\text{deg}.] &\rightarrow \partial_u\phi(u,v), \\ s^{-1}[\text{Image at } 90\,\text{deg}.] &\rightarrow \partial_v\phi(u,v). \end{aligned} \tag{4.15}$$

Now, this direction is at 45 deg. with respect to the camera pixels (x, y coordinates, and also with the straight regions of the waveguides we want to measure. Thus, to integrate the phase from the derivatives in the x and y directions, we need to compute said derivatives from the acquired images. Given that $u = 1\sqrt{2}(x - y)$ and $v = 1\sqrt{2}(x + y)$ the chain rule allows us to obtain

$$\begin{aligned} \partial_x\phi(x,y) &= \frac{1}{\sqrt{2}}(\partial_u + \partial_v)\phi(x,y), \\ \partial_y\phi(x,y) &= \frac{1}{\sqrt{2}}(\partial_u - \partial_v)\phi(x,y). \end{aligned} \tag{4.16}$$

Once one does have the derivatives, the phase ϕ of the object can be reconstructed by applying the Fourier transform F. We have that

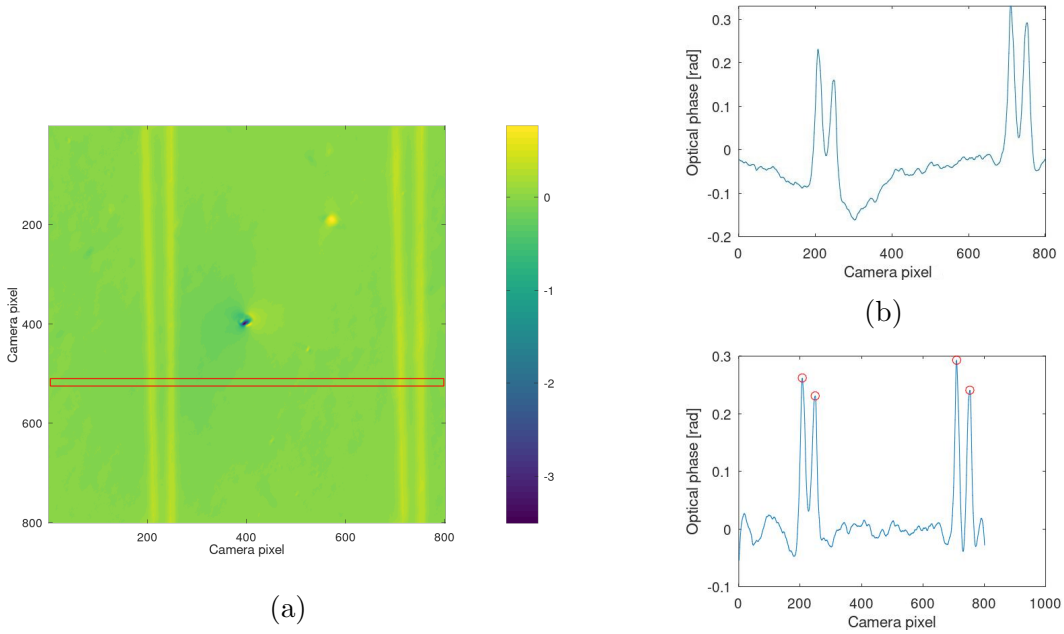
$$\begin{aligned} F(\partial_x\phi) &= ik_x F(\phi), \\ F(\partial_y\phi) &= ik_y F(\phi). \end{aligned} \tag{4.17}$$

Now, though one could obtain $F(\phi)$ from each separate variable, by inverting any of the equations above, that will amplify the noise for very low values of the Fourier variables k_x and k_y. It is more sensible [152] to weight these effects the following way

$$F(\phi) = \frac{ik_x F(\partial_x\phi) + ik_y F(\partial_y\phi)}{(ik_x)^2 + (ik_y)^2}. \tag{4.18}$$

Apart from noise reduction, we avoid singularities along $k_x = 0, \forall k_y$ and $k_y = 0, \forall k_x$, except from the origin (just a point), which we can remove at no cost. The phase is finally recovered by applying an inverse Fourier transform

$$\phi(x,y) = F^{-1}\left[\frac{ik_x F(\partial_x\phi) + ik_y F(\partial_y\phi)}{(ik_x)^2 + (ik_y)^2}\right]. \tag{4.19}$$



(a) (b) (c)

Figure 4.10: *(a) Reconstructed phase, with an example line profile selection shown (red rectangle); (b) Phase profile; (c) Baseline-corrected phase profile, with properly identified peaks.*

4.3.3 Experimental results

We show the results of this analysis for our sample. From the phase retrieval method, given the microscope magnification and (twice[4]) pixel pitch of the camera we are able to obtain & inspect some widths. This can be combined with prior measurements of the aluminium mask by direct observation with the microscope, taking into account the expected widening due to Ionex, in order to have a picture of the structure's dimensions. When analysing the images, one finds small variations of such width through the structure, as expectedly, but also some systematic deviation, probably coming from a under-development (and subsequent under-etching) of the samples.

It is difficult to give a central value on the waveguides width, as there exist fluctuations along the chip. Also, it does not make real sense to obtain a mean, precise, value, as the light will not encounter any mean value on its propagation, but rather every fluctuation will be sensed. Systematic deviations from the design parameters are far more interesting. This is more critical in the thinner regions than in the wider ones, as too thin waveguides have smaller n_{eff} and thus confine light less (it can escape easier when going trough a S-bend, for instance). For the wider regions, only systematic deviations, specially in the phase shifters, are important, but random fluctuations are expected to even out. In any case, we find, for the thinner sections, by inspecting the aluminium mask, widths around 2μm. This is quite smaller than the nominal design lengths, but we find it not that worrying, as we expect significant widening due to lateral diffusion. Also, sudden width shrinking

[4]As per our de-bayering process, we are selecting pixels two times the pixel pitch away.

or small cuts on the waveguides are not as critical as one would think, as we operate under weak-guiding conditions (the change of the refractive index with respect to the substrate is very small), thus light does not diffract strongly after a waveguide cut, so it can propagate some micrometers in a non-guiding region and then couple again to the waveguide with moderate losses.

In Figure 4.10, we show the recovered phase in a region of the sample used later in characterization, along some phase profiles. In such plots, we can see a number of peaks, that correspond to the waveguides, and whose width we can extract to give an approximate range of widths of our waveguides, and check if the devices look like expected, approximately matching the fabrication parameters with the expected deviations.

By analysing the images, and measuring the observed peaks at half-maximum we obtain values of waveguide widths between **3-5** μm (thinner regions). To do so, we trace five 15px (3.57 μm) wide line profiles for data smoothing. A moving average is also implemented for further smoothing. The curvature of the guides is low enough to provide for accurate width measurements, (also) with respect to this basic smoothing.

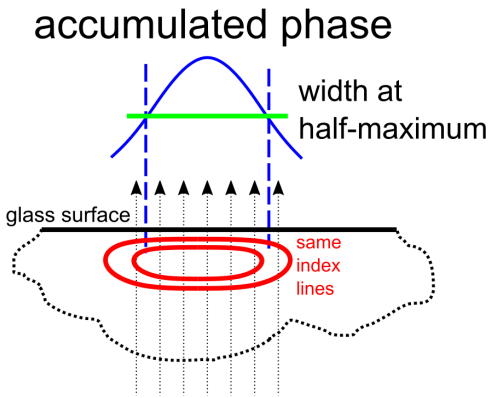


Figure 4.11: *Physical intuition behind the width at half-maximum criteria for the phase peaks.*

What we see are a series of peaks mounted on an unknown and noisy baseline curve, which acts like a background. To remove it, we clip the data corresponding to the peaks and immediate surroundings (a few data points) and then fit the resulting data to a high order polynomial (order 12 is good enough). We do not attempt to accurately model this baseline, we just want to focus on the peaks. The explanation for the curve may be found in the recovered image itself. Some low frequency blobs appear: they are likely due to stresses arising in the glass due to the Ionex process. They are not removed in background phase subtraction because in that region all the glass is uniformly subject to Ionex, while in the masked regions, this is done selectively. Such imbalance may be the origin of those stresses, which in turn affect the phase. In any case, the curve is fitted to the polynomial and then removed. In other words, we baseline-correct the signal in order to better see the peaks. Then, they are identified and its width is computed at half-height. This is a simple criteria,

but it is useful. Note that the peaks correspond to phase, thus to the integral along the depth direction of the refractive index profile. Note also that the height of those peaks is similar to that of previous results [48]. A completely analogous philosophy can be applied to other, relatively less critical width-wise, like the widened sections of the phase shifters. For that case, we find that the widths vary on the range $9-11$ μm.

If during the mask optical inspection we do not find significant variations between different regions of the chip, it is enough for this stage to take some region, if they contain various waveguides the better, sample various linear profiles, and then assume that the information we take from it is representative of the rest of the chip. The Ionex process is quite homogeneous, compared to development or etching, due to bad focusing, for instance, or incorrect development or etching, or even defects on the sample. Note that inhomogeneities in the photoresist (bubbles) or aluminium layers, specially the former, can also be relevant, but they are much finely controlled.

The values obtained for the widths are compatible with the expected lateral diffusion, but there is significant dispersion in the measurements. The algorithm, although being the only physical motivated way to probe the diffused waveguides dimensions, has its limitations. It is as precise as it is sensitive. In particular, incorrect focusing, or slight (few pixels) misalignment between the 0 deg. and 90 deg. images when rotating the sample contribute to blurring the output reconstructed phase. Focusing is difficult, special with high-magnification objectives that let a small quantity of light reach the sensor. Contrast decreases, and seeing the waveguides and focusing them becomes a nontrivial task.

4.4 Semiclassical characterization

In order to probe the microfabricated devices we need to couple laser light into them and see what happens at the output. There are various ways to do it [62]. In our case, we have equipped the entrances and exits of the waveguides with tapers to make use of a prism coupler. In previous works [48] characterization was made by means of end-fire coupling. This required from cutting and polishing the glass samples, which is a very time consuming process. In our case, we opt for the faster process of prism coupling.

The principle of this method is the following: as we know, light is confined in the waveguide by TIR. Light cannot leave the waveguide except at the output end. Endfire coupling is based on this fact. As said, for the case of glass samples, this requires for careful cutting and polishing of the exit face, as well as for the input face of the sample. An alternative is to place on top of the waveguides some media of index $n > n_{wg}$, where n_{wg} is the refractive index of the waveguide (n_{eff} is between this value and the sourroundings). In particular, this media is actually a prism, which is located on top of the waveguides entrances and terminations (see Figure 4.12). Light is launched into the prism, then it gets coupled into the guide, then it travels along the guide and the converse process happens at the end, where light exits the guiding structure through the prism.

As well as in many examples of integrated optics, there are (at least) two ways to understand this; *conjunction of the two descriptions turns out to be very useful for hands-on work on the setup.* First, we can describe the prism coupling process in terms of rays. In the geometric optic approach, we launch a ray of light into the input prism at an angle θ with respect to the prism input face. There, it is refracted twice: first, on such input face (interface air-prism), and then at the prism face *in contact* with the waveguide. By using Snell's law one can derive a relation between θ and the effective refractive index of the guide [137].

$$n_{eff}^{m} = n_{prism} \sin\left[\Omega - \sin^{-1}\left(\frac{1}{n_{prism}} \sin\theta_m\right)\right], \tag{4.20}$$

where Ω is the prism entrance face angle (see Figure 4.12) and θ_m is the custom angle, which depends on the mode m we are coupling to. In other words, *we are able to selectively excite one mode or another*[5] *by changing* θ. When the condition above is met, light is coupled into the waveguide. If the gap were too wide, total reflection would happen and no light would be coupled into the waveguide. If the prism were not present, the light would cross the waveguide without coupling and would exit through the opposite face of the substrate. Now, something similar happens at the endpoint of the guide. We can relate the output angle subtended by the emerging light with the effective refractive index. If prisms are identical, both in refractive index n_{prism}, shape and position the angles will be identical.

To complement this picture, and in order to better understand what is happening, we need an ondulatory explanation. Physically, we have that the prism mode and the waveguide mode will meet in the interface (commonly, an air gap) between prism and waveguide, where optical contact takes place. There is an overlap between the evanescent tails of both prism mode and guided mode, thus enabling for power coupling between the two, when the phase velocity of the evanescent part of the prism mode match that of the guided mode.

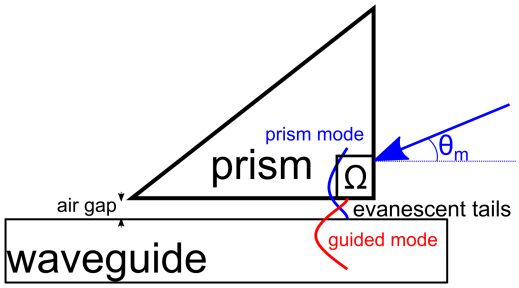


Figure 4.12: *Schematic description of the intuition behind the prism coupling technique. In this method, we launch light at a proper angle* θ_m *onto the prism, exciting a prism mode. There, the evanescent tails of such mode and the waveguide mode overlap (generally in an intermediate air gap), leading to transfer of optical power between them, i.e. mode coupling.*

[5] If more than one.

4.4.1 Optical setup

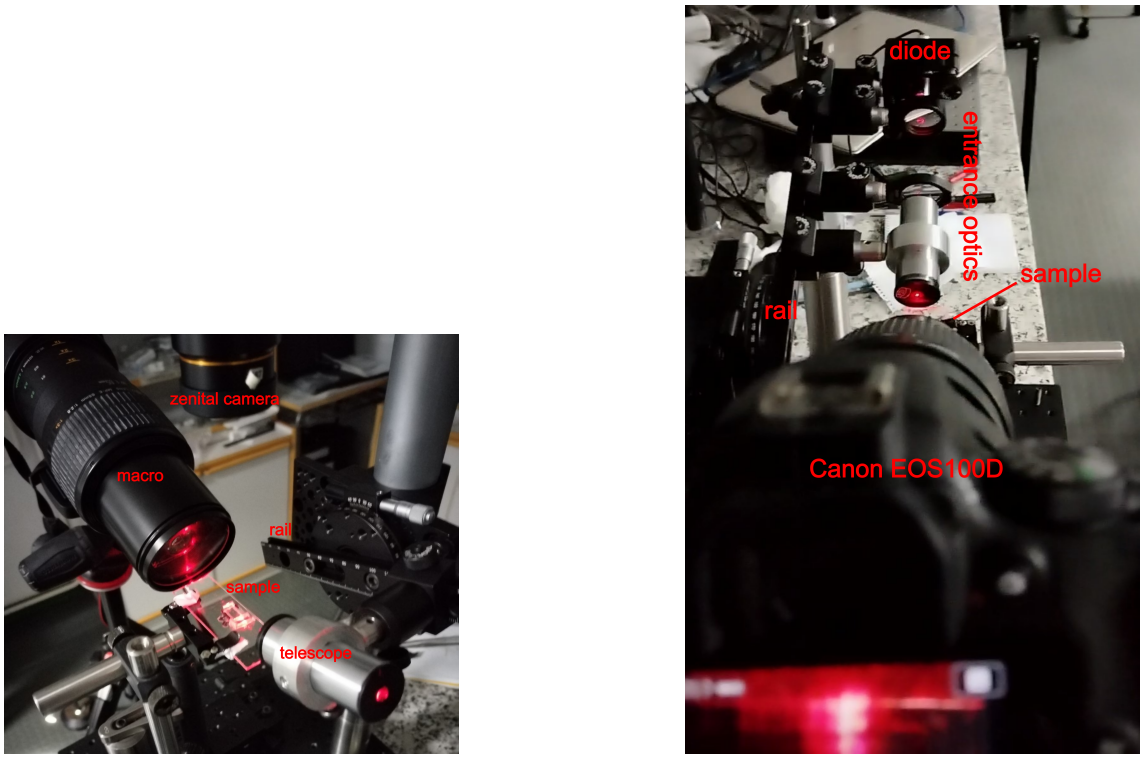
Normally, prism coupling is best suited for coupling into planar waveguides, as in the Metricon apparatus. However, we are interested in channel waveguides. That means that some modifications are due. When coupling to planar waveguides only one contact point is required, where the tails of the prism and waveguide mode meet. To achieve this, the prism is pressured against the glass with a screw. This is not valid for us, as we want to couple to *various waveguides entrances*, and selectively couple to them *by only* translating the sample. In other words, we want a bigger optical contact point.

To that matter, we have fabricated custom prisms not in glass, but in *optical polymer*. A simple glass cast is made, obtaining at least two polished glass surfaces intersecting at 90 deg. We then pour in optical polymer NOA63, which has a refractive index of $n = 1.56$. Then the polymer is cured by UV light for several minutes (depending on the lamp power), until it becomes solid *but* flexible. These plastic prisms (with approximately $\Omega = 90$) are pressured into the sample's glass, and air is mostly removed. Note that an air gap is unnecessary in our case as the waveguides are shallowly buried. That creates a contact patch between the prism and the glass big enough to encompass various waveguide entrances/exits, if not all. Is in that region that coupling between the prism mode and the waveguide mode will happen.

Once we have the prisms on the sample, it is turn for the optics. We are launching a laser into the prism. It is a diode laser emitting TE-polarized light at 635 nm and mounted on the extreme of a rotatory rail in such a way that the incidence angle can be chosen while keeping the point of incidence on the sample. Moreover, we want to match its intensity profile with that of the waveguide entrances, which consist on tapers of the type we described before. On the other hand, we want to single out just one entrance from a pair of tapers. This requires considerable confinement of the light coming out the laser. Thus, the final goal is to have a focus point of a size and shape comparable to the taper ($\simeq 15\mu$m), while being collimated enough in the perpendicular direction so as to launch light with a determinate angle of incidence (beam waist about a tenth of a millimetre). With the objective of such an astigmatic beam in mind we employ an optical system consisting on a pair of cylindrical lenses and a telescope, mounted on the rail between the laser and the prism. Photographs of the setup are shown in Figure 4.13, while a illustration of the full setup is laid out in (the simplified scheme of) Figure 4.14, while the optics after the laser are described in greater detail in Figure 4.15.

In order to introduce light into the waveguides, we first couple to the planar guide *just before*[6] the tapers. By varying the angle θ, we see a zig-zag output, in a screen, for instance, due to coupling into the substrate. Then, there is a point were the output intensity suddenly decreases, following by an also sudden increase. That means coupling into the planar region. Then, light coming from this region gets in turn coupled to the channel waveguides. We observe this from above, with the help of a zenital Thorlabs CS165MU/M Zelux camera. We also see how the light travels

[6]We want to "preserve" the beam waist within the right dimensions.



(a) (b)

Figure 4.13: *(a) Closer look into the prism-coupling setup, showing the telescope, macro lens (of the Canon EOS100D camera), zenital camera (though not in use in this particular photograph), rail and sample. (b) Look of the setup from the screen of the Canon EOS100D camera, showing the entrance optics in the rail (the sample is behind the macro lens, so it is not seen).*

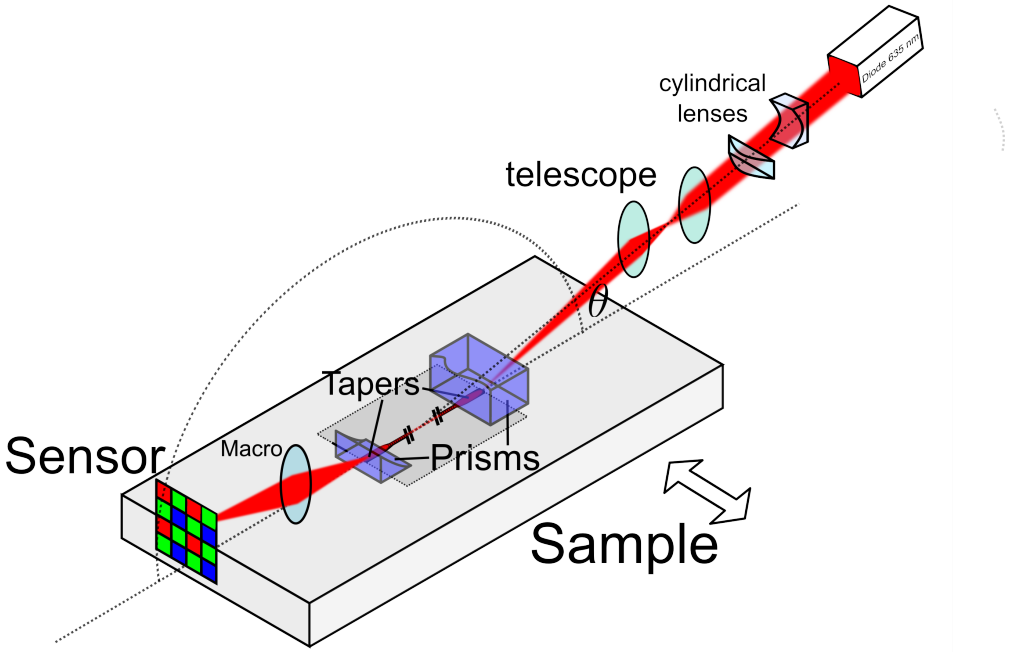


Figure 4.14: *Simplified scheme of the prism-coupling arrangement. Light coming from the 635 nm diode laser traverses a certain optics (Figure 4.15) and reaches the prism, where it gets coupled to the planar waveguide just before the tapers. Coupling into the waveguide happens only at a particular angle, which we select by rotating the laser rail (as well as the immediate optics after it) along the displayed arch trajectory. From that, light couples into the tapers and propagates along the interferometer (here heavily simplified). We choose the taper to be illuminated by transversally moving the sample. The last prism couples light out of the waveguide and the macro lens sends it towards the camera sensor.*

along the waveguides due to scattering losses. As the prisms are not so regular, coupling into the waveguides is not regular also. However, we optimize the prisms location in order to obtain a good enough coupling. In particular, the exit prism needs to be translated for best exit coupling. Still, we found difficulty in probing some structures in the middle of the mask. Fortunately, they were not as important as the phase shifters.

At the exit prism we have located a Canon EOS100D camera (pixel pitch 4.31μm), equipped with a Canon MP-E65 mm F2,8 1-5x Macro objective, which allows us to capture the light coming from the prism. This is first inspected at the naked eye. Once we identify this light matches the mode (it comes only from the exit face of the prism, it disappears when we change θ...) we focus it with the camera. We then have a second confirmation: the two clear outputs are identified. Two straight lines separated a distance on the order of 35 μm (that would depend on the precise coupling point), corresponding to the pair of tapers at each MZI exit. The intensity, read this way, will be our signal.

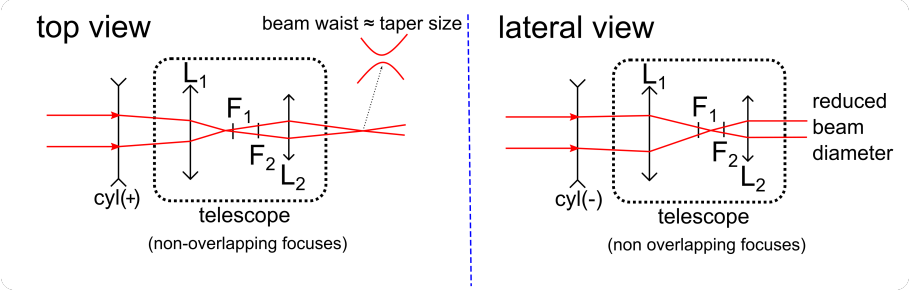


Figure 4.15: *Detail of the optics after the laser, which allow for optimal coupling into the waveguides by an astigmatic beam. In the top view (view from above in Figure 4.14), a positive cylindrical lens bends the incoming laser beam. The telescope is then used to reduce the beam spot and focus the light in a region of roughly the same dimensions of the taper's width. Specifically, we aim for the beam waist to match that width. The image focus of the objective (L1) and the object focus of the ocular (L2) do not match, so that we have that additional degree of freedom for proper focusing at a distance that is comfortable given the sample dimensions. On the other side, in the lateral view (view from the side in Figure 4.14), a negative, low-power cylindrical lens slightly expands the beam, in order to have a collimated beam at the output and thus launch light only at (almost) one given value of* θ.

4.4.2 Image acquisition and processing.

In our sample (see Appendix C), we have twelve MZIs with different lengths of the phase-shifting element (widened waveguide). Given that we have 3dBs couplers (in theory), and assuming the phase shifters work as expected, then the MZIs implement the following transform on the incoming optical fields

$$\frac{1}{2}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\begin{pmatrix}e^{i\phi} & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}e^{i\phi}-1 & i(1+e^{i\phi})\\ i(1+e^{i\phi}) & 1-e^{i\phi}\end{pmatrix}. \tag{4.21}$$

The system was aligned to the best of our efforts in order to achieve a binary input of optical power P_0, meaning $u=[\sqrt{P_0},0]^t$ (up[7]) and $d=[0,\sqrt{P_0}]^t$ (down).

The action of the transformation in Equation (4.21) on these inputs is

$$\begin{aligned}\frac{1}{2}\begin{pmatrix}e^{i\phi}-1 & i(1+e^{i\phi})\\ i(1+e^{i\phi}) & 1-e^{i\phi}\end{pmatrix}\begin{pmatrix}\sqrt{P_0}\\ 0\end{pmatrix}&=\frac{\sqrt{P_0}}{2}\begin{pmatrix}e^{i\phi}-1\\ i(1+e^{i\phi})\end{pmatrix},\\ \frac{1}{2}\begin{pmatrix}e^{i\phi}-1 & i(1+e^{i\phi})\\ i(1+e^{i\phi}) & 1-e^{i\phi}\end{pmatrix}\begin{pmatrix}0\\ \sqrt{P_0}\end{pmatrix}&=\frac{\sqrt{P_0}}{2}\begin{pmatrix}i(1+e^{i\phi})\\ 1-e^{i\phi}\end{pmatrix}.\end{aligned} \tag{4.22}$$

From these equations we can read out the output power that will be collected by the camera sensor. In the case of an input u we expect, in the upper output, a power (P_{uu}) equal to

$$P_{uu}=\frac{P_0}{4}|e^{i\phi}-1|^2=\frac{P_0}{2}(1-\cos\phi).\quad \text{In : Up; Out : Up} \tag{4.23}$$

[7]This notion of up and down is relative to a mask positioning in which the reference marks are in their natural orientation. In other words, the mask in Appendix A rotated 90 deg. anticlockwise.

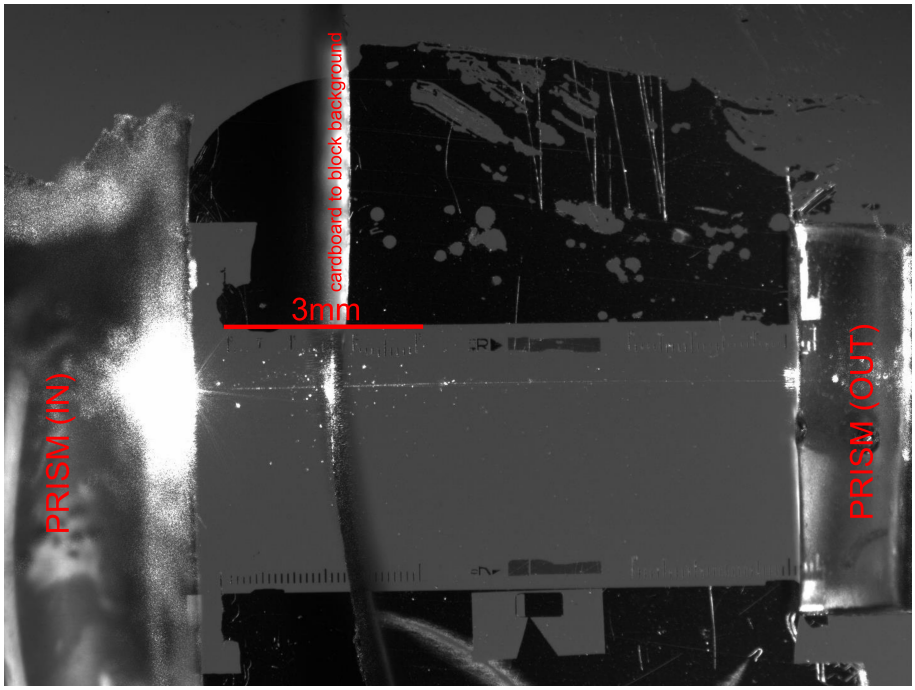


Figure 4.16: *Top view (Thorlabs camera) of the sample and the polymer prisms. The contrast has been modified for clarity. The light propagates from left to right coupled into a waveguide interferometer, after entering through its down input taper. The vertical line in the center of the image is produced by a small piece of cardboard is located after the input prism to block (part of) the background light.*

Likewise,

$$P_{ud} = \frac{P_0}{4}|1 + e^{i\phi}|^2 = \frac{P_0}{2}(1 + \cos\phi). \quad \text{In : Up; Out : Down} \tag{4.24}$$

and, for the *complementary* configurations, respectively

$$\begin{aligned} P_{du} &= \frac{P_0}{4}|1 + e^{i\phi}|^2 = \frac{P_0}{2}(1 + \cos\phi), \\ P_{dd} &= \frac{P_0}{4}|e^{i\phi} - 1|^2 = \frac{P_0}{2}(1 - \cos\phi). \end{aligned} \tag{4.25}$$

In order to eliminate the dependence on the input power it is better, when it comes to actual signal, to compute the quantity

$$\begin{aligned} r_u &= \frac{P_{uu} - P_{ud}}{P_{uu} + P_{ud}} = -\cos\phi = \cos(\pi - \phi), \\ r_d &= \frac{P_{du} - P_{dd}}{P_{du} + P_{dd}} = \cos\phi. \end{aligned} \tag{4.26}$$

Thus, our expected signal is a pair of cosine functions out of phase by a value π. We expect a linear relationship between the widened waveguide section and ϕ, as per what we saw in Section (4.1). Given the expected dimensions of the final mask,

we sample various lengths, from 0 to 2500 μm in uniform steps of approximately 250 μm, apart from the π phase.

The values of the lengths and corresponding (assumed) phases are shown in 4.2.

Table 4.2: *Values of the length of the widened waveguides and corresponding expected phases as per Section 4.1.*

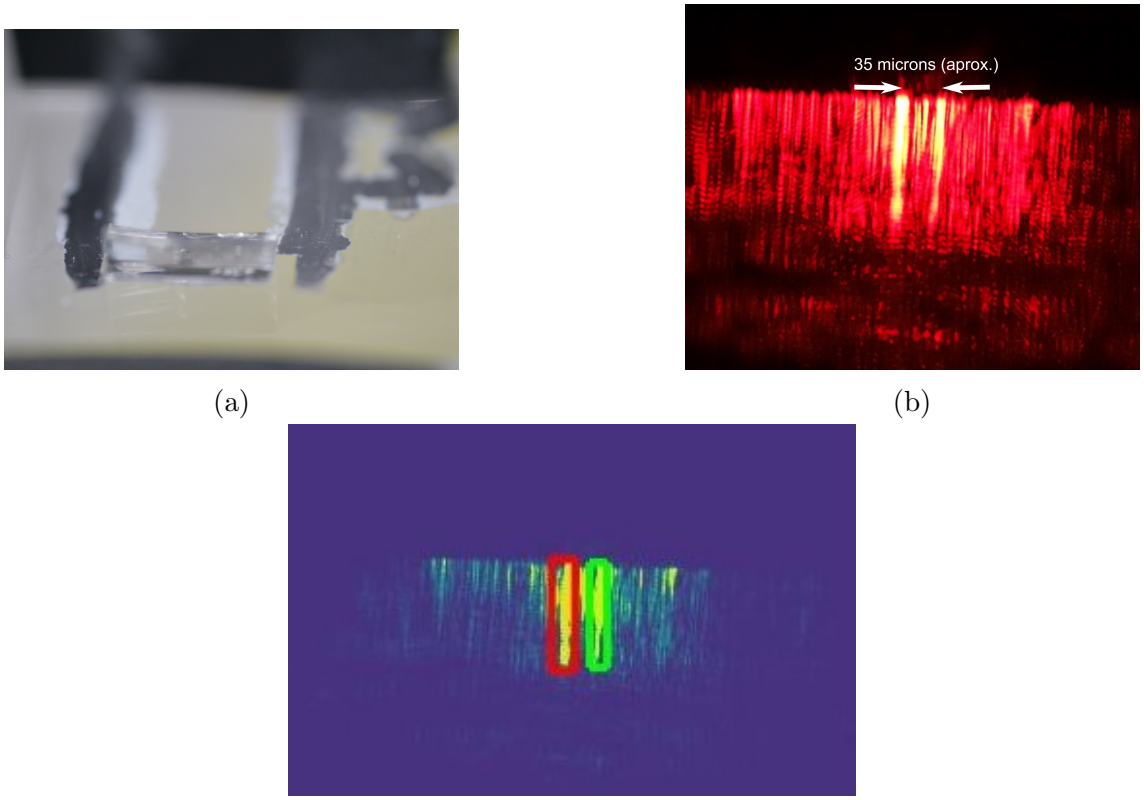
Length (μm)	Expected Phase (rad)
0	0
250.2	0.2846π
500.4	$0.5693\ \pi$
750.6	0.8539π
879	π
1008	1.1468π
1251	1.4232π
1501.2	1.7078π
1751.2	1.9925π
2001.6	2.2771π
2251.8	2.5618π
2502	2.8464π

To capture the images, as said, we use a Canon EOS100D camera with a macro lens. Such lens is almost fully extended, resulting in almost a 5x magnification. The images are stored in Canon's RAW format, .CR2, and then converted into .pgm.

The signal consists on two bright lines at a distance compatible with the waveguide separation, as shown in Figure 4.17b. As seen, there is a substantial amount of noise in the image. Light not associated to the guides forming a background which will reduce the interference visibility.

To integrate the intensity, we define a region of interest (ROI) around the line, and then sum all the pixel values. For adequate ROI selection, the red channel is used, as the pixels are brighter and the output identification is much easier. However, for the optical power measurements, the blue channel is selected, as some red pixels are saturated, thus they yield no information. Sometimes the shape of the bright lines is not very clear, so ROI selection is not obvious. There is always some uncertainty relative to the ROI selection, as the shape of the signal is sometimes confusing. To make this doable, more systematic and reduce bias we take multiple images and analyse them via computer, by means of an automatic tresholding algorithm, known as Otsu's method [153], which is used in combination with labelling algorithms. These are already implemented in GNU Octave [154]. Multiple images of the same configuration are fed to the algorithm. Then they are binarized. After that, Otsu's tresholding labelling is applied. The result is that the program is capable of automatically identify the ROI.

The process needs to be supervised, in order to ensure the program does not misidentify the waveguide's outputs. On the other side, this requires for the images to be properly focused. Nine images are taken for each configuration, and from them, the best three, which are those where the outputs are (to the best of our



(a) (b)

(c)

Figure 4.17: *(a) Exit prism as situated on the sample (b) Raw intensity output as seen through the exit prism and captured by the Canon camera. Two vertical, wide lines, representing the light coming out of the waveguides, are visible, despite the strong background; (c) Identification of the ROIs after numerical processing. Given the positioning of the camera and the sample, the green ROI is actually the upper output.*

possibilities) unambiguously identified, are selected. *Some systematic errors are expected to be introduced by the processing (they would still be there even if we did it by hand), given the sometimes fuzzy shape of the signal.* This needs to be kept in mind when analysing the results.

4.4.3 Experimental results

After the processing stage, we end up with the following set of data, which is shown in Figure 4.18. Alternatively, in 4.19 we show a scatter plot of r_u versus r_d (Eq. 4.26), manifesting the (negative) linear relationship between those two relative output power magnitudes.

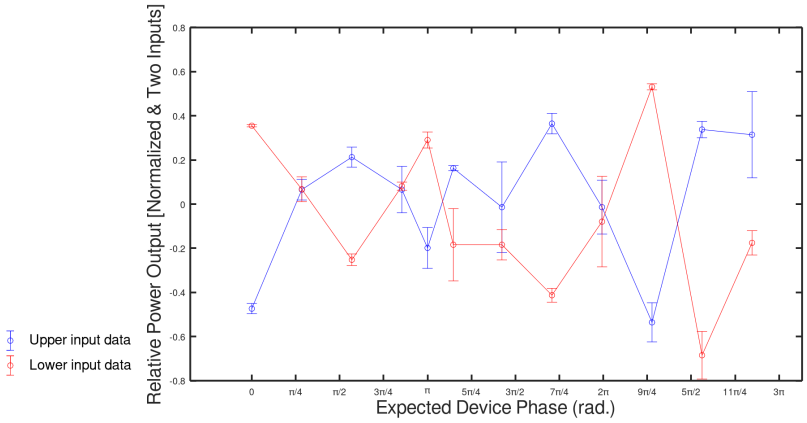


Figure 4.18: *Preliminary data obtained as a result of processing the images acquired in the prism-coupling setup. The vertical axis represents relative normalized power output and the horizontal axis the phase each element is expected to introduce, which should vary linearly with its length. Data point 10 in the red dataset was obtained by manually selecting the ROIs, and not by the automatic tresholding algorithm, as the latter did not adequately identify the outputs for this particular case.*

On the Y axis, we represent the relative normalized output optical powers of each device, according to Equation (4.26). On the X axis, we display the expected phase each device should introduce, according to Table (4.2).

From the plot we can see that the complementarity between the two configurations (upper input v. lower input) is quite consistent along the different devices. This is indicative of a good input, in the sense that we were able to couple only to a waveguide, selecting it apart from the other. In particular, one can go back to Equation (4.22) and allow for an arbitrary input $[\sqrt{P_1}, \sqrt{P_2}]$, which contains, in fact, both configurations as special cases ($P_1 = 1, P_2 = 0$ and $P_1 = 0, P_2 = 1$). If we compute the output power ratio under this conditions we arrive at

$$r = \frac{P_2 \cos\phi - P_1 \cos\phi + 2\sqrt{P_1 P_2}\sin\phi}{P_1 + P_2}. \tag{4.27}$$

Now, consider the two configurations above, but slightly off with respect to a binary input. For the sake of the argument, an imperfect upper input would be

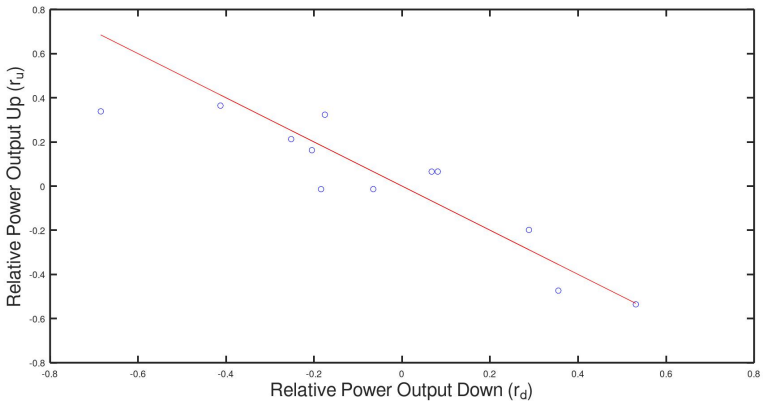


Figure 4.19: *Data obtained as a result of processing the images acquired in the prism-coupling setup, showing the relationship between the two relative power outputs, which seems to agree with the fact that said relationship should approach the line with equation $y = -x$, as per Eq. (4.26).*

P_1=0.75 and P_2=0.25 (in arbitrary power units). In that case, Equation (4.27) would become

$$r_u = 0.25\cos\phi - 0.75\cos\phi + 0.86\sin\phi. \tag{4.28}$$

Likewise, an imperfect lower input (take the same values, for simplicity)

$$r_d = 0.75\cos\phi - 0.25\cos\phi + 0.86\sin\phi. \tag{4.29}$$

Obviously, r_u is no longer $-r_d$, due to the $2\sqrt{P_1 P_2}\sin\phi$ term. This could be already read by simply exchanging P_1 and P_2 in Equation (4.27), and identifying each case with each configuration, but the numeric example makes the explanation clearer. *Thus we conclude that we are able to selectively couple to one or another waveguide of the same interferometer, with the aid of a prism and the tapers.*

What we are not able to explain with this simple model is the low visibility we obtain, lower than 0.5, and also its variation with the phase (which could be a random effect). In order to see that the measurements indeed match a sinusoidal function we combine measurements in both configurations (recall Eq. 4.26), and fit the resulting data points to a function of the form

$$f(x) = a\cos(bx).$$

Data points for the sixth device starting from the left are removed, as we believe they produce an incorrect result but we do not have any explanation for it. In any case, this is indicative of required improvement in the measurement stage. The GNU Octave `nlinfit` function is employed, which is based on the least-squares method. Combined and fitted data are displayed in Figure 4.20.

The fit yields the following values of the target function parameters: $a = -0.378(18)$ and $b = 1.799(32)$. Though the obtained values are compatible with a cosine function, we found two clear deviations to what we expected. A): The frequency of the oscillation is clearly greater than one. We had computed the phase

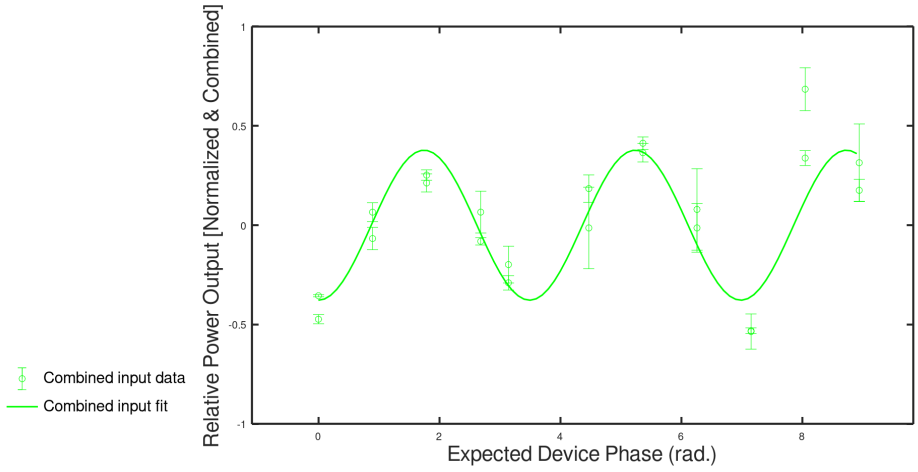


Figure 4.20: *Results on the characterization of phase shifters. Data in both upper and lower input configurations are combined and then fitted to a cosine function. We see good agreement except from the devices with larger lengths.*

acquired by the guided mode as $\phi = k_0 \Delta n_{eff} z$. We find that the relationship between ϕ and z seems to be still linear, but the proportionality constant is not what we computed. By noting that $b\phi = k_0 \Delta n_{eff} z$ one obtains that $\Delta n_{eff} = 6.58(11) \cdot 10^{-5}$ (small, in fact). Finally, as said, we observe deviation B): We have a value of the interference visibility < 1. For some devices (for instance, phase zero) we should have seen only light emerging from one of the tapers, but we always see some light coming out. On top of that, there was a considerable background, as can be appreciated in Figure 4.17.

Most likely, the explanation for the low visibility is an accumulation of many factors. On one side, the fact that diffusion times were accidentally increased means bigger lateral diffusion, which in turn implies a lower value of the coupling distance. That means that the 3dBs couplers are not really 3dBs. That fact alone, given that every coupler was fabricated the same way, does not account for that visibility in every device. For the case of a π phase, the observed output would be the same no matter what coupling phase the DC introduced, if both DCs are *identical*. Visibility would drop, however, if the latter condition does not hold, like could happen if we admit a random deviation from the expected value of the coupling distance. If we take Equation (4.21) and introduce a random variation of the coupling phase, and not the same for each of the two DCs composing the MZI, we could observe a drop in visibility. Such random deviation, nonetheless, should be small, thus visibility would be still bigger than measured.

Determine if and, above all, how far the 3dBs deviate from their design behaviour is not easy to determine. There is only a little amount of light getting scattered. Analysis of top images like the one in Figure 4.16 may act as a proxy. Sometimes, visual inspection suggested something that could be compatible with this, but we did not find a consistent pattern across devices or even inputs. Moreover, scattering does not need to be symmetric between one arm of the MZI and the another.

Possibly, this fact acts in conjunction to other imperfections in the sample and

the prisms, and, importantly, with a relevant contribution of the background signal, as can be appreciated in Figure 4.17c-(a). Imagine a simple case of a constant background on the signal, and ignore whether we launch light on the upper or the lower port. Then the normalized intensity ratio would be

$$r = \frac{P_u + P_{bckg} - P_d - P_{bckg}}{P_u + P_d + 2P_{bckg}} = \frac{P_u - P_d}{P_u + P_d + 2P_{bckg}}, \tag{4.30}$$

where *bckg* stands for 'background'. Clearly, that would reduce visibility.

An additional contribution maybe polarization, but the results obtained were not conclusive. We slightly modified the setup in Figure 4.14 and added a polarizer inbetween the cylindrical lenses and an analyzer attached to the macro objective. We know from previous results [48] that there is some *polarization dependent coupling* in potassium-exchanged waveguides, and also that coupling is quite insensitive to input polarization. In particular, launching TE light into a DC gives rise to a little amount of TM light after the coupler. That field will travel one interferometer arm and encounter the last where it will be split and some of it (almost half) will thus arrive at the wrong output port, reducing then the visibility. So, by using a polarizer-analyzer system, the idea was to rule out this possibility and increase visibility. *However*, we did not increase it (nor decrease it) appreciably. On the other side, what we did observe was that even with crossed polarizers, there was still light coming out of the prism, indicative of potassium's waveguides known anisotropy.

Plastic prisms, improvements and final remarks

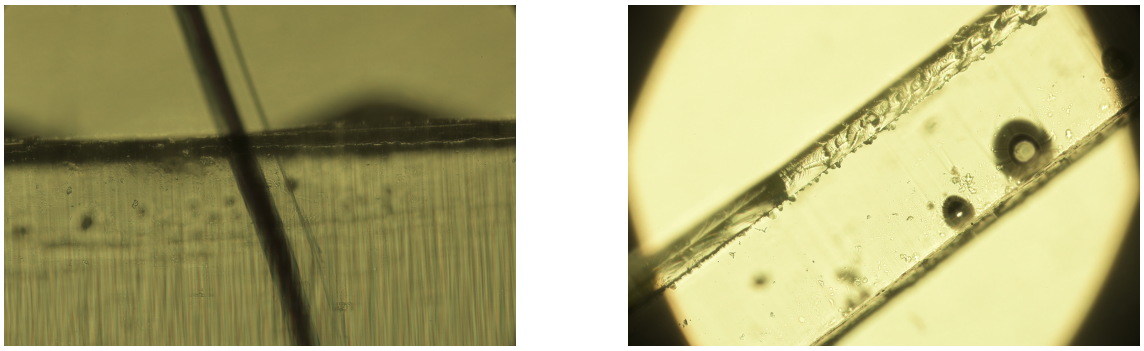
Finally, the process of manufacturing the plastic prisms is not fully controlled, and the behaviour of the prisms is not fully understood. They are made of optical polymer, which is intended to be behave well when illuminated. Nonetheless, some defects can be introduced in fabrication.

The first associated problem is de-moulding, which can render prisms with a not so regular edges. Also bubbles trapped inside the polymer disturb the overall transparency. On the other side, when observing the prisms under the microscope, a quasi-periodic pattern of grooves distributed along the prism's volume. This is shown in Figure 4.21. We hypothesize that this is in fact result of interference of the source. The UV lamp used for curing is particularly coherent. That opens the possibility for interference effects which result on differential curing of the prism. More specifically, higher degrees of polymerization should arise in intensity maxima, while lower doses of radiation correspond to the minima.

We attribute part of the overall noise observed in the images to this effect. Rotating continuously the polymer in the mould under the UV lamp, by means of an automatic electrical mechanism (recycled from a conventional, household alarm clock), we observed that the grooves almost disappeared. We tested the prism fabricated like so and observed a significant reduction of overall noise. In particular, we tested it for the device without a phase shifter (phase equal to zero), which should give a fully binary output, when fed with a binary input. We found that, however, visibility did not increase, as there was still light on the other output that should not be there.

To sum up our experimental efforts:

- We fabricated optical chips by means of Ionex in glass, comprising a number of MZI in order to probe integrated phase elements (Z gate, for instance), based in the widening of waveguide sections;
- To characterize such chips, we self-made a novel, custom optical prism-coupling setup, based on polymer prisms, by which we could access many integrated structures with the same prism, contrary to the usual prism-coupling method where glass prisms have only a point of contact with the sample, and astigmatic beam focusing, in order to couple and de-couple light from the waveguides, without the need for cutting and polishing the glass;
- The measured phase is proportional to the widened wave-guiding region's length, as expected, but the proportionality constant seems to be very sensitive to fabrication conditions;
- Moreover, the interference visibility is notably lower than expected, with improvements required in that direction. A possible path for further study would be to put the prisms in the MZI arms (after de DCs), extract light from there (difficult!) and see if we have really a 3dBs splitting.



(a) (b)

Figure 4.21: *(a) Groove pattern, bulk distributed on the plastic prisms fabricated by simple curating optical polymer under UV light, like those used for the sample characterization, as viewed under an optical microscope. For scale reference, the black line at the background of the image is a line drawn with a permanent marker ($\simeq 1$ mm wide). (b) If in the curation process the polymer is rotated grooves seem to greatly diminish. However, note that we still can not get rid of common imperfections like air bubbles etc.*

Chapter 5

Autocompensation in entanglement-based QKD

This Chapter is related to the following articles the author has contributed to (found at the end of this document, in Appendix D): a) it is fundamentally based on results published in [98].

So far, we have shown how to construct QKD protocols that have MDI characteristics which are, at the same time, endowed with autocompensation mechanisms in order to reduce errors and improve key generation.

With these autocompensation techniques we have contributed to a toolbox of options for passive mitigation of errors in quantum communications. This increases the possibilities of implementing various relevant QKD realisations with the current and near-term fiber optic infrastructure. This is one of the ideas we have been emphasizing throughout this Thesis.

It is natural, then, to try to extend this to other important protocols, which, by their different characteristics, will require from novel autocompensating solutions. It is also desirable that the conclusions obtained, regarding both possibility of autocompensation and the actual implementation, are applicable in general to the type of protocol considered. This makes sense as long as we are able to identify an underlying topology of the protocol, and relate it to the basis requirement of autocompensation which requires back-and-forth propagation.

It is a well-known fact that entanglement is a basic brick of quantum theory, and is often pointed out as one of the defining aspects of QM [155]. Moreover, it can be also thought of as a *resource* [156]. We have seen how entanglement can be exploited in QKD in various ways. In MDI, by post-selecting an entangled state, Alice and Bob can get rid of the responsibility of performing the final measurement, and thus QKD is liberated from the burden of full detection device characterization. In a more theoretical setting, we have mentioned how formulating BB84 as an entanglement

protocol allows for rigorously proving its security [104].

In this Section, we will be interested in the direct use of entanglement for secret key generation between remote parties. By direct use we mean that the source emits pairs of entangled photons, which, although experimentally more challenging (or inefficient), as we have seen, than WCP use, implies that the source does not need to be trusted [44], in the sense of *monogamy* of entanglement. This is in contrast with BB84, where the source was well shielded in Alice's laboratory.

5.1 E91 and BBM92 protocols

One of the first protocols, if not the first, to make use of entanglement was formulated by Artur Ekert in 1991 [43], which is known as the E91 protocol. Ekert considered a source that emitted of entangled photons in the singlet state. Such state was then simultaneously measured at Alice's and Bob's laboratories, respectively. The measurement was to be performed in *three* separate bases, so as Alice and Bob could check if a Bell inequality was violated or no. QM predicts a violation of Bell inequalities, while hidden variable theories do not. QM argues that the correlations entangled states give rise to, only exist when measurement takes place. Hidden variable theories say that such correlations where already there. This fact prompted A. Ekert to base the security of his protocol in the Bell inequalities. According to QM, information exists only when the state is measured, in this case by Alice and Bob. We will have a random outcome representing a given correlation of Alice and Bob's measurements. The key here is that such correlation cannot be replicated by a third party, Eve. If she does not measure, she does not obtain any information. If she does, she cannot possibly know what basis Alice and Bob will use. If she correctly guesses it, she may launch a product state, but such state would not violate the Bell inequality, and thus the adversary will uncover itself. Another option is to entangle the singlet state with other particles, thus creating a fake entangled source, but again, she will disturb the original state and be detected, because Bell inequality would not be violated with such a fake source. Thus, concluded Ekert, the Bell theorem protects key generation (as long as does not get disproved).

A simple version of the protocol, also using an entangled source of photons, was proposed shortly after by Bennet, Brassard and Mermin, the Bennet-Brassard-Mermin 1992 protocol (BBM92) protocol. However, in this case no third basis was needed, and no checking of a Bell inequality required. Simply, Alice and Bob could use the bases of BB84 and measure the singlet state and the protocol would still be secure, as, in one side, incorrectly guessing Alice and Bobs bases produces errors (this circumstance was already present in the E91 protocol). And on the other side, importantly, the fake source cannot possibly exist because of the monogamy of entanglement (which can indeed be used, as we mentioned, to argue for a security proof for BB84). Thus, as said, no Bell theorem is required for security.

The way the protocol works is essentially the following. Say for instance that we are working in the polarization encoding. Alice and Bob encode information as

usual. Recollect that the singlet state is given by

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|1_{aH}1_{bV}\rangle - |1_{aV}1_{bH}\rangle), \tag{5.1}$$

which can be generated with the schemes described in Chapter 2.

Then, if they measure, with an Innsbruck type scheme, $|1_{aH}1_{bV}\rangle$ Alice assigns the bit 0 and Bob bit 1. They need to agree who performs a bit-flip. Assume it is Bob. Thus, after the measurement they share keystring bit 0. Conversely, if they project into $|1_{aV}1_{bH}\rangle$ they now will share bit 1.

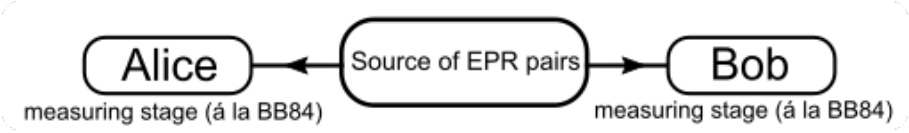


Figure 5.1: *Basic layout of the BBM92 protocol. A central source emits Bell states (also known as EPR pairs). Each "half" of the entangled state reaches Alice and Bob, respectively, who measure in the usual BB84 bases.*

Moving onto more practical matters, these protocols suffer from the common problem of QKD, which is a low rate of secret information transmission, specially at larger distances. It is clear, a priori, that a entangled state is also sensible to noise, and that noise will lead to errors, which reduce the key rate.

In this chapter, we will apply a similar philosophy we have been working on but to entanglement-based QKD protocols that are assimilable to BBM92. We shall make a general description of fiber perturbations on an entangled state, and how that translates into error probabilities and *error rates*. We will try to keep this analysis as general as possible, and give general models to deal with fiber imperfection's effects on the quantum states. We will consider, similarly to Chapter 3 three different encodings: polarization, collineal modes of FMFs (HG modes) and codirectional modes of MCFs. We shall decribe how, given the light circulation structure of BBM92, autocompensation is not a good solution. As a result, we will introduce a modified version of MDI with already entangled states that has a simple, built-in autocompensation mechanism.

5.2 Results

We shall now put in more concrete (and mathematical) terms the ideas we have been discussing. The starting point is analysing how fiber perturbations affect the entangled states. Then, from the (perturbed) quantum probability amplitudes, an error probability is derived. From this, an error rate is obtained. Finally, a secret key rate analysis is performed. We shall describe how to implement autocompensation in the BBM92 protocol. We will show that this is not possible for the general perturbation but only for a simpler phase perturbation. As an alternative, we formulate another entanglement-based protocol which can be endowed with a full autocompensation system.

In analogy to chapter 3 we also formulate our results in three separate encodings: polarization, collineal modes (implementation in FMFs) and codirectional modes (implementation in MCF). As seen, all three encodings induce Hilbert subspaces of dimension two, adequate to write down qubits and 2x2 transformations acting on them. For the case of the polarization encoding, our results are exact. For the other two, we have *again* to make the approximation of disregarding polarization. Recall than in a fiber each spatial mode has two polarizations. In general, this gives rise to a 4d-modal space with cross-couplings between each combination of spatial mode and polarization mode. In order to move into a 2d-subspace approximations need to be made. In particular, that polarization and spatial d.o.f can be factorized. For the case of collineal modes, as pulses travel the same, wide, core, it is reasonable to assume, in some regime, that polarization perturbations affect equally to both HG modes. Alternatively, a PM-FMF could be used, and polarization would be fixed for both modes and could be split up from the spatial d.o.f. For the case of codirectional modes, disregarding polarization is a far more restrictive approximation, as each core is different, so it should not be a priori a reason to assume that the polarization perturbations are common. Still, we can consider, as we did in Chapter 3 that the cores are close enough to this be the case. Torsions, stresses and other factors may cause polarization coupling, and this, if they come from the outside (bending of a MCF, for instance) may induce global polarization couplings affecting both cores the same. If intrinsic polarization couplings can be disregarded with respect to those, as it is assumed that fibers are well fabricated, then we can work within this assumption. Alternatively, special kinds of fibers with elliptical cores or two-core PANDA fibers could also be considered.

5.2.1 Singlet state under random perturbations

We will start by analysis how fiber perturbations affect BBM92. We do a generic analysis here, which is unrestrictive enough to deal with polarization, collineal modes and codirectional modes. The mathematical equations are general. One has to keep in mind, of course, that we are dealing with separate encodings.

As before (see Equation (2.53)), we formulate the perturbations as a 2x2 SU(2) matrix with totally general coefficients ($2^2 - 1$ independent parameters), which happen to be RVs. We have six parameters in total, three for Alice and three for Bob. Recall that perturbations can be understood as a random rotation of an input, ideal quantum state on the Bloch sphere, parametrized by angles ϕ, φ (azimuthal and precession) and θ (polar angle). As such, we may write it down as [77]

$$T(\phi,\varphi,\theta) = \begin{pmatrix} \cos\frac{\theta}{2}e^{-i(\phi+\varphi)/2} & -\sin\frac{\theta}{2}e^{(\phi-\varphi)/2} \\ \sin\frac{\theta}{2}e^{-i(\phi-\varphi)/2} & \cos\frac{\theta}{2}e^{i(\phi+\varphi)/2} \end{pmatrix}. \tag{5.2}$$

This particular parametrization will be useful for the particular analysis we will carry out in this chapter. To perform some computations, writing it down as in Equation (2.53) remains useful.

The starting point in BBM92 is Charlie preparing and sending a single state[1]

[1]The $|\phi^+\rangle$ Bell state is often also used, but whether which Bell state to use is not really relevant

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|1_{a\alpha}1_{b\beta}\rangle - |1_{a\alpha}1_{b\beta}\rangle). \tag{5.3}$$

In this notation, 1 is the photon number, as before, a and b means Alice and Bob, and α and β now signify any of the considered degrees of freedom: polarization, spatial mode functions or dual-rail path information. Thus we are also writing, at the same time

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|1_{aH}1_{bV}\rangle - |1_{aV}1_{bH}\rangle),$$

but also

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|1_{aX}1_{bY}\rangle - |1_{aX}1_{bY}\rangle), \tag{5.4}$$

and

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|1_{a1}1_{b2}\rangle - |1_{a2}1_{b1}\rangle). \tag{5.5}$$

Now, how does this gets transformed when $T_a(\phi_a, \varphi_a, \theta_a)$ and $T_b(\phi_b, \varphi_b, \theta_b)$ act on it? In the notation of Equation (2.53) we have

$$\begin{aligned} T_aT_b|\psi^-\rangle = \frac{1}{\sqrt{2}}[&(t_{12}^{-a}t_{11}{}^b - t_{11}{}^at_{12}^{-b})|1_{a\alpha}1_{b\alpha}\rangle + (t_{11}{}^at_{11}^{-b} + t_{12}^{-a}t_{12}{}^b)|1_{a\alpha}1_{b\beta}\rangle \\ &-(t_{11}^{-a}t_{11}{}^b + t_{12}{}^at_{12}^{-b})|1_{a\beta}1_{b\alpha}\rangle + (t_{12}{}^at_{11}^{-b} - t_{11}^{-a}t_{12}{}^b)|1_{a\beta}1_{b\beta}\rangle]. \end{aligned} \tag{5.6}$$

If perturbations were not present, Alice and Bob would never obtain coincidences which are not anticorrelated. That means that errors arise if Alice and Bob project into $|1_{a\alpha}1_{b\alpha}\rangle$ or $|1_{a\beta}1_{b\beta}\rangle$. These wrong clicks on the detectors happen with a probability

$$p_Z^{wrong} = \frac{1}{2}|t_{12}^{-a}t_{11}{}^b - t_{11}{}^at_{12}^{-b}|^2 + \frac{1}{2}|t_{12}{}^at_{11}^{-b} - t_{11}^{-a}t_{12}{}^b|^2 \tag{5.7}$$

This in the Z basis[2]. In the X basis something similar happens. Computations are lengthy but straightforward. One obtains

$$\begin{aligned} p_X^{\text{wrong}} = \frac{1}{8}&|t_{12}^{-a}t_{11}{}^b - t_{11}{}^at_{12}^{-b} + t_{11}{}^at_{11}^{-b} + t_{12}^{-a}t_{12}{}^b - \\ &t_{11}^{-a}t_{11}{}^b - t_{12}{}^at_{12}^{-b} + t_{12}{}^at_{11}^{-b} - t_{11}^{-a}t_{12}{}^b|^2 + \\ \frac{1}{8}&|t_{12}^{-a}t_{11}{}^b - t_{11}{}^at_{12}^{-b} - t_{11}{}^at_{11}^{-b} - t_{12}^{-a}t_{12}{}^b + \\ &t_{11}^{-a}t_{11}{}^b + t_{12}{}^at_{12}^{-b} + t_{12}{}^at_{11}^{-b} - t_{11}^{-a}t_{12}{}^b|^2. \end{aligned} \tag{5.8}$$

Note that $p_Z^{\text{wrong}} = p_X^{\text{wrong}} = 0$ when $T_a = T_b$. However, as the perturbations are random, this condition cannot be met in general. It is not a useful case to consider.

to our discussion.

[2]The singlet state remains invariant under the same change of basis in Alice and Bob. The correlations Alice and Bob obtain from measuring the singlet state are the same in the Z and X basis (in terms of anti-correlated bit values).

Phase perturbations

A particular but useful case occurs when only phase perturbations are present. This is to say, take Equation (5.2) and put $\varphi = \theta = 0$. The only perturbation on the modes consists on a relative phase, or phase drift, between them. Physically, this amounts to disregard coupling while retaining only the phase differences. Such a situation can arise, for instance, when MCF cores are far apart, such that coupling is negligible but still a phase difference arises due to the cores not being identical.

In this case, only errors in the X basis are present, as the Z basis is immune to phase drift. This is because a phase drift does not alter the bit encoding in such a basis. A phase perturbation cannot change an H-polarized photon into a V-polarized photon or viceversa, and the same goes for spatial modes. One can see this by going back to the input singlet state in Eq. 5.1 and put a phase between its two components. Clearly, a measurement in the Z basis is insensitive to this, while one in the X basis is not (the change of basis is done before the detection). Moreover, the error probability is greatly simplified, becoming

$$p_X^{\text{wrong}} = \frac{1}{2}[1 + \cos(\phi_a - \phi_b)]. \tag{5.9}$$

5.2.2 Error rates

Equations (5.7) and (5.8) above are error probabilities. If they did not change on each QKD round, they could be directly used as error rates and the secret key rate computed. However, the t's are RVs, so what we have to do is, actually, to compute the expected values of these probabilities. This way, we take an alternative route with respect to chapter 3, in which we proposed an heuristic model for the optical errors. It is useful to have various ways to model and try to give qualitative estimates to fiber perturbations on quantum states of light.

Now, this boils down to assume probability distributions for the variables ϕ, φ and θ, *i.e* a *noise model* [128]. Wanting to be general, it is reasonable to hypothesize Gaussian distributions for each variable. The perturbations we consider are small deviations from the ideal. Hence, we will assume Gaussian distributions centred in zero and with small variance. In particular, this parameter will be proportional to the fiber length L, capturing the fact that the further photons travel, the more the perturbations effects accumulate. The distributions will spread accordingly with length. Note that then the standard deviation goes as $\sqrt{L}$, which is consistent with a random walk process [157]. The proportionality constant between the length and the variance of the Gaussians we shall call γ. Thus, $\sigma^2 = \gamma L$.

For the case of the θ variable, we need to include a non-unity Haar measure [77]. We need it in order to uniformly sample from the Bloch sphere, like we need the scale factor $\sin\theta$ in spherical coordinates. We attach it to the distribution, thus effectively multiplying it by a factor $\sin\theta$. Writing all this down

$$f(\psi) = \frac{1}{\sqrt{2\pi N_\psi \gamma_\psi L}} e^{-\frac{\psi^2}{2\gamma_\psi L}}, \tag{5.10}$$

where $\psi = \phi, \varphi$ and

$$f(\theta) = \frac{\sin\theta}{\sqrt{2\pi N_\theta \gamma_\theta L}} e^{-\frac{\theta^2}{2\gamma_\theta L}}. \tag{5.11}$$

Where each γ is associated to the corresponding variable. Actually, we will consider the same value of γ for the angles φ and ϕ, thus we group their distributions. The normalization factors are there because we will evaluate the averages by a Monte Carlo method, and, as the number of samples is finite, though convergent, N_ψ and N_θ are not exactly one, but almost.

The important thing now is what value give to the parameters of the distribution, γ_ψ and γ_θ. It will be, in general, different for each variable and, although strictly it could be different for Alice and for Bob we shall consider a symmetric scenario with the same kind of fiber and similar external perturbations, assuming that the probability distributions evolve the same with the respective propagation distance.

We are considering three different encodings, but still we want to be general enough to use the same model for all three of them. Ideally, we should provide some estimate for γ that captures the three scenarios; given such complication, falling beyond the scope of this analysis, it is enough to give a lower bound for the error rates across encodings. In particular, it can be assumed, in good approximation, that modal coupling, specially in the case of MCF is small, and smaller than phase drift, as phase varies much more uncontrollably. Coupling between modes is expected to be stronger in the polarization encoding, as the overlap between the modes is very big, being the modes almost identical.

To give an order of magnitude for the γ's, we need to link the perturbation to experimental values. We may consider then the least coupling scenario of MCF, thus giving a lower bound of the modal coupling perturbations. For that case, we go back to Equation (2.53) and identify the intercore cross-talk with the square of the off-diagonal terms, as power goes with the square of the electric field, and the electric field is at first order with the mode operators. Typical values of the cross-talk, which can be obtained by launching light into a fiber core and then measuring the resulting output on the involved cores, are in the order of -40 dB per kilometer [121]. So, in that case, we can compute a "maximum" value θ could take, and infer from it the value of the variance that could, at the tail of the distribution, produce that value. So, at $L = 1$ km, $(\sin\theta/2)^2 = 10^{-4}$, thus $\theta \simeq 2 \cdot 10^{-2}$ ($\sin\theta \simeq \theta$). Admitting that the resulting value of θ is $\simeq 3\sigma$, where $\sigma = \sqrt{\gamma_\theta L} \rightarrow \gamma_\theta = 4.4 \cdot 10^{-5}$ km^{-1}, or, rounding up to a slight bigger value $5 \cdot 10^{-5}$ km^{-1}.

For the case of the phase, obtaining an estimation that is useful for us is more difficult, as phase excursions tend to be quite big. Indeed, measurements of the *skew* (delay on the time of arrivel of light travelling different cores) in MCFs [158], shows that the phase drift is so big, as measured over an interval of hours, that would make non-compensated protocols almost useless. The phase noise would then be modelled by a similar distribution, but not as narrower as the one of cross-talk; it would be a wrapped Gaussian distribution on the interval $(0, 2\pi]$.

All of this would support even more the need for autocompensation. Still, MCFs are the worst case for phase perturbations. The case of polarization is a bit different

[159], as phase noise is not as big. It is still big enough, however, as typical best-case anisotropies generate a polarization mode dispersion of 0.04 ps/km^{-1}. For light having a wavelength in the C-band, and reasoning from the distribution as we did for the cross-talk, this would correspond to γ_ψ on the order of thousands, which would render again un-compensated protocols useless.

So, for the case of phase, in order to have an useful way to state our case, we introduce a hypotetical value of γ_ψ assuming an ultra-best case scenario where only some small phase fluctuations have been left uncontrolled (one may imagine a correction/calibration is made initially and then the system is left uncontrolled). In particular, assuming a phase fluctuation of 2π radians on 100 km propagation, that leads to $\gamma_\psi \simeq 3 \cdot 10^{-2}$).

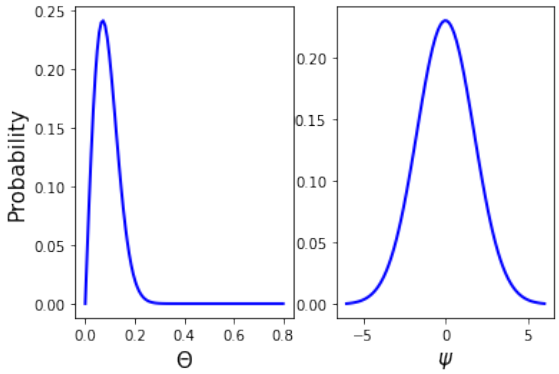


Figure 5.2: *Probability distribution functions for the perturbation errors, for the θ and $\psi = \phi, \varphi$ variables, respectively, with values of $\gamma_\theta = 5 \cdot 10^{-5}$ km^{-1} and $\gamma_{\phi,\varphi} = 3 \cdot 10^{-2}$ km^{-1}.*

The discussion above is condensed into an *optical error* term, E_{opt}, as in Chapter 3, given in this case by

$$E_{opt}(L) = \frac{\langle p_Z^{\text{wrong}} \rangle + \langle p_X^{\text{wrong}} \rangle}{2}. \tag{5.12}$$

Plots of the errors according to the probability density functions (PDFs) above and within the aforementioned range of parameters are shown in Figure 5.3. We show the full and only phase optical errors as a function of channel length (Alice/Bob $\rightarrow$ Charlie).

5.2.3 Autocompensation capabilities in BBM92 and BBM92-like protocols

Although we will later make a short security analysis, we can advance, from Figure, that errors caused by the perturbations are a clear obstacle to key distribution at large distances. So, we need an autocompensating system in order to mitigate them. However, at first glance, we observe that the BBM92 protocol (and other alike than can be reduced to BBM92) poses some serious difficulties. In the BBM92 protocol, light pulses do not end in the same place they are produced. On the

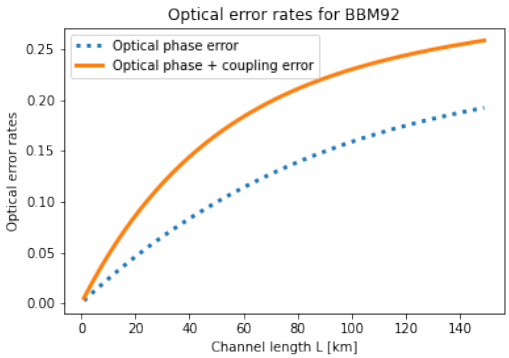


Figure 5.3: *Error comparison between the only phase perturbation case and phase + coupling errors. For the θ and $\psi = \phi, \varphi$ variables, respectively, we consider values of $\gamma_\theta = 5 \cdot 10^{-5}$ km^{-1} and $\gamma_{\phi,\varphi} = 3 \cdot 10^{-2}$ km^{-1}. Reproduced from own work in [98].*

other side, for autocompensation we need a back-and-forth loop. The consequence is that we need an odd number of circulations between Alice/Bob and Charlie for compensating. Moreover, only phase can be compensated, by suitable adapting this triple-path architecture. General perturbations, that include coupling, cannot be possibly compensated.

In Figure 5.4 we show an example of a scheme capable of compensating phase perturbations, assuming only phase drift is present. It is not much involved, but importantly, has the disadvantage of requiring the photons travel three times the distance L. In other words, we have three times the attenuation. This scheme is common to all three encodings, albeit the need for demultiplexing and multiplexing in the case of polarization and collinear modes.

5.2.4 Alternative protocol based on Bell-state parity

This difficulties advise to modify the BBM92 protocol in order to achieve more favourable autocompensation characteristics. We may sacrifice the need for *not* using quantum random number generators, which are not required when Alice and Bob share an entangled state and do nothing but measure it. Instead, we can make Alice and Bob encode information on a pre-shared Bell state by phase modulation. The state is launched by Charlie and arrives at Charlie, thus we have an optimal[3] two-way circulation. Moreover, as Charlie will perform the measurement, the protocol also has MDI characteristics. The layout of this protocol, which we term Bell states exchange parity (BSEP) is schematically represented in Figure 5.5.

In detail, the BSEP protocol works as follows. A blank Bell state $|\psi^+\rangle$ is emitted by Charlie, the source.

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|1_{a\alpha}1_{b\beta}\rangle + |1_{a\beta}1_{b\alpha}\rangle). \tag{5.13}$$

Then, it arrives at Alice and Bob's station, where phase modulation plus au-

[3]From the point of view of autocompensation.

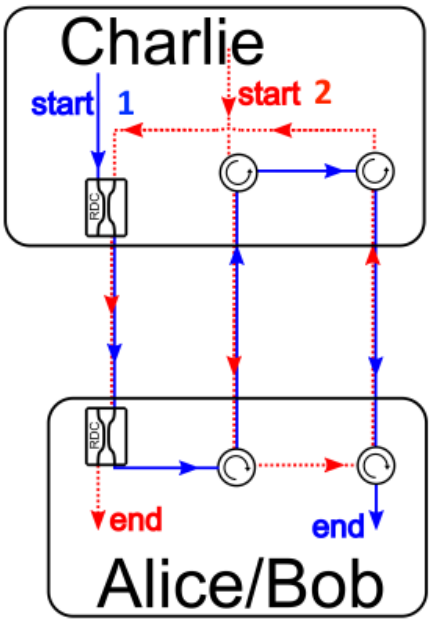


Figure 5.4: *Phase drift autocompensating topology for BBM92. It requires for suitable reconfigurable directional coupler (RDC)-coordination, three-way circulation of the light pulses, and thus three times the attenuation. This scheme is valid for polarization by demultiplexing and multiplexing the pulses with PBSs at the fiber ends. Similarly for collinear modes with mode-sorting MZIs for demux/mux. For codirectional modes, it works in a straightforward manner. Reproduced from own contribution [98].*

tocompensation transformations are applied. Information is encoded as a relative phase

$$|\psi(\Delta\omega)\rangle = \frac{1}{\sqrt{2}}(|1_{a\alpha}1_{b\beta}\rangle + e^{i(\omega_a-\omega_b)}|1_{a\beta}1_{b\alpha}\rangle) = \frac{1}{\sqrt{2}}(|1_{a\alpha}1_{b\beta}\rangle + e^{i\Delta\omega}|1_{a\beta}1_{b\alpha}\rangle), \quad (5.14)$$

where ω_a is the phase introduced by Alice's phase modulator and ω_b the phase introduced by Bob's phase modulator. These phases take values 0 or π, respectively. Bit assignment is 0 for $\omega_a = 0$ and 1 for $\omega_a = \pi$. Bob applies a bit flip. This protocol is conceptually similar to the virtual protocol proposed in [160] (just for demonstrative purposes), but here it is implemented in actual terms, with beneficial results.

Table 5.1: *Bit encoding and signal (corresponding detector's clicks) in the BSEP protocol for polarization encoding.*

Alice	Bob	Detectors firing up	Bit
0	0	D_{aH}, D_{aV} or D_{bH}, D_{bV}	0
0	π	D_{aH}, D_{bV} or D_{bH}, D_{aV}	0
π	0	D_{aH}, D_{bV} or D_{bH}, D_{aV}	1
π	π	D_{aH}, D_{aV} or D_{bH}, D_{bV}	1

Delays between the pulses are required at Alice and Bob's respective lines in

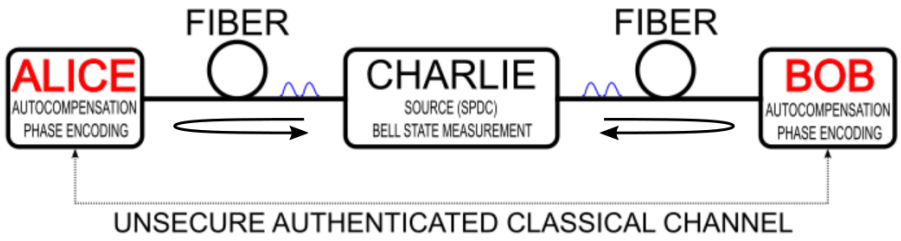


Figure 5.5: *Basic structure of the BSEP protocol. A central node (Charlie) emits entangled pairs that are shared between Alice and Bob, who modulate the relative phase randomly, encoding bits of key. The state then returns to Charlie and a Bell state measurement is carried on it. Reproduced from own contribution [98].*

order to process one pulse separately from the other, the same way it was done in Chapter 3, following [79].

The autocompensation transformations are provided by devices as shown in Figure 5.6. We need a separate scheme for each encoding. For the case of polarization, it is totally analogous to that of Chapter 3. For the others, we introduce slight modifications. For the case of collinear modes, the CLC plus DP is substituted by an arrangement of a couple of DP, with the appropriate rotation angles. The mode-sorting MZI used for delaying the pulses is not affected. For the case of codirectional modes, we opt for a setup using a pair of circulators and a small fiber circuit instead of an integrated device. In any case, this is just an alternative. Both of them are valid.

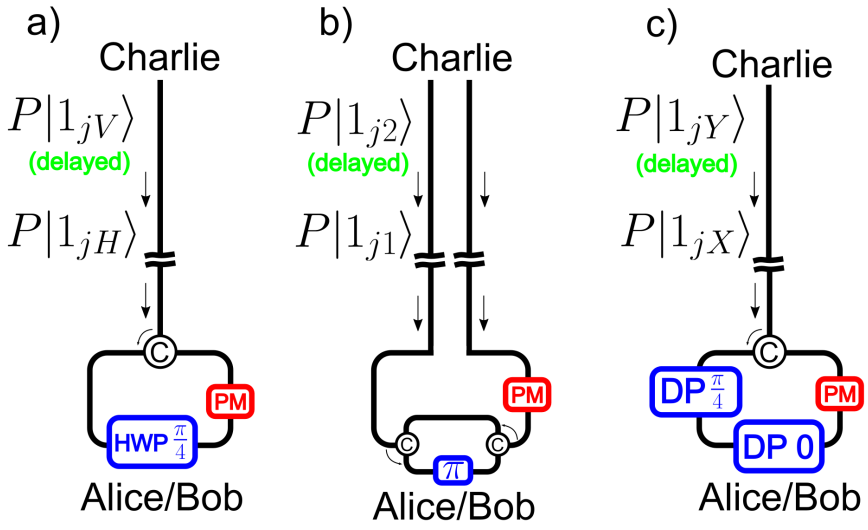


Figure 5.6: *Autocompensation devices for the three encodings we consider for BSEP implementation, with the corresponding dedicated optical hardware. Their operation is very similar to those in Chapter 3. Reproduced from own contribution [98].*

Then, the state arrives back to Charlie. There, it is processed by a BMD. Depending on the encoding, we have three different types of BMDs, which are identical to those in Chapter 3. Depending on the relative phase Alice and Bob

randomly choose, a pair of detectors or another will register coincidences. The principle is no other than the well-studied behaviour of entangled states launched into a BS [55], which allows for Bell state discrimination, and has already been used in Chapter 3. As the total photon wavefunction needs to be symmetric, a singlet state results in photons exiting the BS in opposite ports, and thus reaching different pairs of detectors. On the other side, if they are in any other Bell state, they leave the beam-splitter on the same output arm, thus reaching another different set of detectors. The detection stages (see 5.7) are identical to those used in Chapter 3. We include them here for completeness, but no novelty is included.

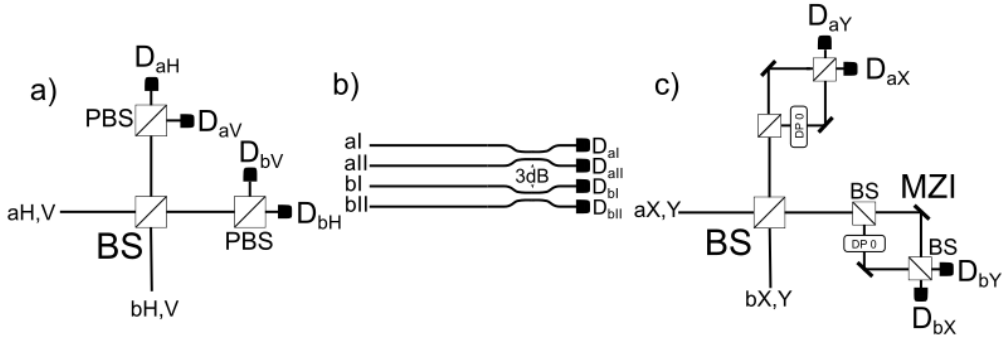


Figure 5.7: *Bell state measurement devices for the three encodings we consider for BSEP implementation, with the corresponding dedicated optical hardware. Their operation is identical to those in Chapter 3. Reproduced from own contribution [98].*

The way key is generated is the following (assuming Bob performs a bit-flip when required). Bit 0 corresponds to choices $\omega_a = \omega_b = 0$ or $\omega_a = 0, \omega_b = \pi$. Bit 1, on the other side, corresponds to choices $\omega_a = \omega_b = \pi$ or $\omega_a = \pi, \omega_b = 0$. Thus the same bit corresponds to totally different outcomes (see Table 5.1). Hence, Eve cannot guess the choice of phase. Only Alice and Bob know about it. They know that they chose, and can deduce what the other chose from the measurement outcome Charlie broadcasts.

Key rate analysis

In order to compare the BBM92 and BSEP protocols, we will perform a basic security analysis. We compute the single-photon key rate in the asymptotic limit. That means single-photon sources are considered, and we assume a infinite number of signals are exchanged. No practical correction (decoy states) is applied to the sources, they are assumed to be perfectly single-photon. On the other side, detectors are characterized by an efficiency (in which apparatus transmittance can be included) and a dark count rate.

The lower bound for secret key rate R is given by [104, 91]

$$R \geq qY_{11}[1 - fH(e_{11}) - H(e_{11})], \tag{5.15}$$

where the upper bound for the two-photon coincidence error is given by

$$e_{11} \leq \frac{(E_{opt} + e_{ad})\eta^2}{Y_{11}} + \frac{1}{2}\left(1 - \frac{\eta^2}{Y_{11}}\right). \tag{5.16}$$

Here, the two-photon yield Y_{11} is given by

$$Y_{11} = [1 - (1 - Y_0)(1 - \eta)]^2, \tag{5.17}$$

the transmissivity η has the usual definition (includes efficiency of detectors), and we take it symmetric for Alice and Bob, Y_0 is the dark count yield ($2p_d$) and e_{ad} is an additional, non-autocompensable, residual source of error (we expect it to be very small, typically, and we identify it to the so-called misalignment error in QKD literature). The optical error E_{opt} is given by $E_{opt} = \frac{1}{2}(e_Z + e_X)$ as previously computed in Equation (5.12).

We examine various cases and compute the key rate accordingly: BBM92 with full perturbations; BBM92 with only phase perturbations, autocompensated and not so; and, finally, BSEP. As before, autocompensation means that the corresponding optical error term is null.

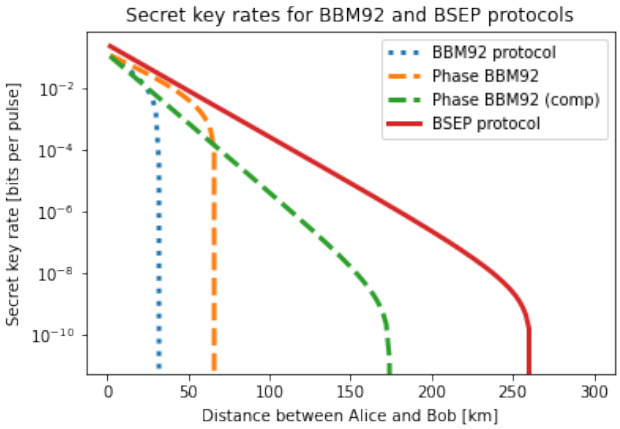


Figure 5.8: *Secret key rate R comparison between BBM92 in three separate cases: full perturbation no autocompensation (blue dotted line), only phase perturbation not compensated (orange dotted) and only phase perturbation but compensated (red dotted) and BSEP protocol (green solid). For the θ and $\psi = \phi, \varphi$ variables, respectively, we consider values of $\gamma_\theta = 5 \cdot 10^{-5}$ km^{-1} and $\gamma_{\phi,\varphi} = 3 \cdot 10^{-2}$ km^{-1}. The experimental parameters are collected in 5.2. Reproduced from own work [98].*

Figure 5.8 shows how the BSEP protocol beats any version of BBM92 for this choice of parameters, which is a reasonable choice. If the fiber was to good, we insist, autocompensation would not be considered an option, thus it falls out the objective of this Thesis. For perturbations stronger than considered, the BSEP protocol advantage is clearer. Note that cross-talk indeed can be increasingly reduced by building better fibers, and that is something that may be expected of the future. Phase drift however is a more serious issue, and it's case is of more practical interest. Even if the cross-talk was zero, phase instabilities would still exist, and a need for their compensation remains.

Table 5.2: *Experimental parameters for the computation of the secret key rate for entanglement-based QKD protocols in this Chapter.*

Parameter	Value
p_d	$6.02 \cdot 10^{-6}$
f	1.35
e_{ad}	1%
η	60%
α_{att}	0.15 dB/km
γ_ψ	$3 \cdot 10^{-2}$
γ_θ	$5 \cdot 10^{-5}$

Conclusions and future prospects

As we have seen, QKD offers very, very good possibilities to furnish future communication systems with information-theoretic secure key generation, thus protecting it against quantum computer attacks. Still, to bring it to practical terms, a number of adjustments need to be made.

On the one hand, we have made theoretical contributions in the optical hardware realm. We proposed devices making use of optical integrated gratings and two-mode waveguides in order to generate topological phases, which are more robust than their purely dynamical counterparts, to use as phase gates in QKD quantum information processing tasks (in particular, state generation and detection). We have shown that generating topological phases with photonic structures is feasible, while also highlighting connections to the area of quantum simulation, which may offer interesting perspectives in the future.

on the other hand, we have contributed with this Thesis towards the objective of realistic QKD implementations. We have taken protocols which, by design, offer enhanced security, specially in the case of MDI-QKD, and we have shown how to implement them in such a way that undesired errors due to imperfections in optical fibers are autocompensated. We have designed MDI protocols, making use thus of two-photon coincidences, in three separate settings, depending on the photonic degree of freedom used. Not only polarization modes, but also spatial modes: encodings more adequate for novel types of fibers with higher bandwidth: collinear modes, arising naturally in FMFs and codirectional modes, natural in MCFs. In short, plug and play MDI-QKD systems have been proposed and analyzed.

Likewise, we have proposed a novel protocol, based on the exchange parity of Bell states (in short, BSEP), retaining MDI characteristics, and designed to overcome fundamental difficulties of entanglement-based QKD in terms of autocompensation of fiber perturbations, which the new protocol achieves in an intrinsic way, also in such three separate encodings. All of this implies additional, and varied, hardware requirements (more devices), though not very complicated, as our systems are essentially passive (apart from reconfigurable directional coupler (RDC) synchronization) and makes light circulation more complex. Still, the benefits are an enhancement of the key rate and the achievable distance.

Besides, we have carried on experimental work, exploring the more usual dynamical realization of phases, by means of adiabatic widening the waveguide section and obtaining as such phases due to modification of the effective refractive index of the structure. These phase elements, which can be readily combined with direc-

tional couplers in integrated chips for QKD applications, where microfrabricated in and inexpensive platform as is glass, by means of conventional photo-lithography and ion-exchange. Computer-aided design of the structures (Mach-Zehnder type devices, in order to measure phases by output light analysis) was carried on; then photolithography in glass substrates, in order to obtain masks suitable for ion-exchange modulation of the refractive index. The resulting waveguides were tested by phase retrieval algorithms in a microscope, and were also subject of a input/output light characterization, by using a tailored, useful, practical and flexible, prism-coupling setup. The novelty was fundamentally, on the one hand, in using an input astigmatic beam; on the other, in making the prisms in-house, from UV-curated polymer,in order to couple to extense regions of the integrated chip; thus many structures can be probed without having to take out the prism and put it back again.

Looking into the future further effort is required in the topological devices part, in the sense of advancing the ideas here proposed, requiring from further both design and experimental proof-of-concept implementation.

In terms of error mitigation in fiber-based QKD, there is room for improvement in the sense of looking for autocompensation mechanisms that deal with perturbations in full, not only for special fibers, with reduced either polarization fluctuations or cross-talk, but a simultaneous treatment of spatial and polarization effects altogether. On the other hand, further exploration of the high-dimensional case -namely, for MDI, is required, though it is not without difficulty, as already stated. This is related to the perspective discussed just above, as one may consider high-dimensional encodings involving both polarization and another spatial encoding. For faithful transmission of the quantum state, being able to recover it amounts, in a sense, to search for mechanisms which enable to restore quantum states that undergo random polarization and spatial mode perturbations.

Regarding the experimental efforts, further analysis is required to analyse why the visibility

Xdoes not reach bigger values. The root of the problem was likely to some uncontrolled aspects in the fabrication process. Is thus desirable to improve this in the future, increasing the number of intermediate checks (for instance, more microscope inspection), and making it a more systematic process overall, so the problems at the end of fabrication can be easily traced back. On the other hand, if this custom prism-coupling setup would be used in combination with "quantum light", i.e attenuated pulses, we are required to have very good in-coupling efficiencies. This seems a very difficult task, do to the way prism-coupling works, so this setup could be best used only in the out-coupling part. It will save time, either way, as it would not require for cutting and polishing the end face of the sample, and would serve as an intermediate stage in testing. If the sample happens to fail the tests, then this would preclude further more work-intensive testing: there is no need to advance into a full cutting and polishing final characterization if the chip does not work.

Appendices

Appendix A

Key rate equations for A-MDI-QKD

The expression of the key rate used in Chapter 3 [Equation (3.34)] is directly obtained from results in [15, 123, 124]. Some of the principles behind the computation of the key rate have already been outlined in Chapter 2, when we described sources, fiber losses, and detection probabilities, together with chapter 3 where we described the decoy state method and gave some notions about security proofs.

Under the assumption of an infinite number of exchanged signals (asymptotic key rate), making use of decoy states and considering that we use the rectilinear (Z) and diagonal basis (X), the lower bound to the secret key rate is given by

$$R \geq Q_{11}^{Z}[1 - H(e_{11}^{X})] - Q_{\mu_a\mu_b}^{Z} f H(E_{\mu_a\mu_b}^{Z}), \tag{A.1}$$

where Q_{11}^{Z} is the single-photon gain (coincidences) in the Z basis, H is the binary Shannon entropy [Equation(3.2)], e_{11}^{X} is the single-photon error rate in the X basis, $Q_{\mu_a\mu_b}^{Z}$ is the overall gain in the Z basis, considering signal pulses of mean photon number μ_a (Alice) and μ_b (Bob). The parameter f is the error inefficiency factor and $E_{\mu_a\mu_b}^{Z}$ is the overall error rate in the Z basis, under the same conditions as the overall gain.

For the case of the overall gain and error rates, they are computed as

$$Q_{\mu_a\mu_b}^{Z} = Q_C + Q_E, \tag{A.2}$$

$$E_{\mu_a\mu_b}^{Z} = \frac{E_{opt}Q_C + (1 - E_{opt})Q_E}{Q_{\mu_a\mu_b}^{Z}}, \tag{A.3}$$

where E_{opt} is given by Equation (3.31),

$$Q_C = 2(1 - p_d)^2 e^{-\mu'/2}[1 - (1 - p_d)e^{-\eta_a\mu_a/2}] \times [1 - (1 - p_d)e^{-\eta_b\mu_b}], \tag{A.4}$$

and

$$Q_E = 2p_d(1 - p_d)^2 e^{-\mu'/2}[I_0(2\xi) - (1 - p_d)e^{-\mu'/2}], \tag{A.5}$$

where p_d is the dark count rate of a single detector, $\mu' = \eta_a\mu_a + \eta_b\mu_b$ is an 'weighted average' of the mean photon numbers of Alice and Bob signal pulses by the transmissivities of Alice's and Bob's respective channels, which are equal in under the symmetric assumption we make. The transmissitivies already include the fiber attenuation, the detector efficiency and the interal transmissivities of the devices $\eta = 10^{-\alpha_{att}L/10}\eta_d\eta_{internal}$. $I_0(\xi)$ is the modified Bessel function of the first kind, and its argument is $\xi = \sqrt{\mu_a\eta_a\mu_b\eta_b}/2$.

On the other side, the single-photon gains and error rates are to be estimated with the aid of the decoy state method. In particular, we consider a practical decoy state setting where Alice and Bob send, respectively, a signal state (mean photon number μ_a, μ_b), a weak decoy ($\nu_a, \nu_b << 1$) and a vacuum (mean photon number equal to zero). First, the three following quantities are to be defined

$$a = \frac{\mu_a\mu_b^2 - \nu_a\nu_b^2}{\mu_a\nu_b^2 + \nu_a\mu_b^2};\ b = \frac{\mu_a^2\mu_b - \nu_a^2\nu_a}{\mu_a^2\nu_b + \nu_a^2\mu_b};\ c = \frac{\mu_b^2\mu_a^2 - \nu_b^2\nu_a^2}{\mu_a^2\nu_b^2 + \nu_a^2\mu_b^2}. \tag{A.6}$$

Now, compute $m = \min(a, b, c)$ and define new variables

$$\begin{aligned} g_1^\beta &= e^{\mu_b}Q_{0\mu_b}^\beta + e^{\mu_a}Q_{\mu_a 0}^\beta - e^{\nu_b}Q_{0\nu_b}^\beta - e^{\nu_a}Q_{\nu_a 0}^\beta, \\ g_2^\beta &= m(e^{\mu_a+\nu_b}Q_{\mu_a\nu_b}^\beta + e^{\nu_b}Q_{0\nu_b}^\beta - e^{\mu_a}Q_{\mu_a 0}^\beta + Q_{00}^\beta), \\ g_3^\beta &= m(e^{\nu_a+\mu_b}Q_{\nu_a\mu_b}^\beta - e^{\mu_b}Q_{0\mu_b}^\beta - e^{\nu_a}Q_{\nu_a 0}^\beta + Q_{00}^\beta), \\ g_4^\beta &= e^{\nu_b}Q_{0\nu_b}^\beta E_{0\nu_b}^\beta + e^{\nu_a}Q_{\nu_a 0}^\beta E_{\nu_a 0}^\beta - Q_{00}^\beta E_{00}^\beta, \end{aligned} \tag{A.7}$$

where β can stand for either the Z basis or the X basis. For the Z basis we already have written down the expression of the overall gains and error rates. For the case of the X basis, they are given by

$$Q_{\mu_a\mu_b}^X = 2\gamma^2[1 + 2\gamma^2 - 4\gamma I_0(\xi) + I_0(2\xi)], \tag{A.8}$$

$$E_{\mu_a\mu_b}^X = \frac{1}{Q_{\mu_a\mu_b}^X} \times \left\{\frac{1}{2} - 2\left(\frac{1}{2} - E_{opt}\right)\gamma^2[I_0(2\gamma) - 1]\right\}. \tag{A.9}$$

with $\gamma = (1 - p_d)^{-\mu'/4}$.

Finally, all these expressions are combined to obtain the final estimates (lower bound and upper bound, respectively) of the single photon gain and error rate in the Z and X basis

$$Q_{11}^Z \geq \mu_a\mu_b e^{-\mu_a-\mu_b}\frac{g_1^Z + g_2^Z + g_3^Z - e^{\mu_a+\mu_b}Q_{\mu_a\mu_b}^Z + e^{\nu_a+\nu_b}Q_{\nu_a\nu_b}^Z}{\nu_a\nu_b - \mu_a\mu_b + m\mu_a\nu_b + m\nu_a\mu_b}, \tag{A.10}$$

and

$$e_{11}^X \leq \frac{e^{\nu_a+\nu_b}Q_{\nu_a\nu_b}^X E_{\nu_a\nu_b}^X - g_4^X}{\nu_a\nu_b Y_{11}^X}, \tag{A.11}$$

with

$$Y_{11}^X \geq \frac{g_1^X + g_2^X + g_3^X - e^{\mu_a+\mu_b}Q_{\mu_a\mu_b}^X + e^{\nu_a+\nu_b}Q_{\nu_a\nu_b}^X}{\nu_a\nu_b - \mu_a\mu_b + m\mu_a\nu_b + m\nu_a\mu_b}. \tag{A.12}$$

Appendix B

Experimental procedure flowchart

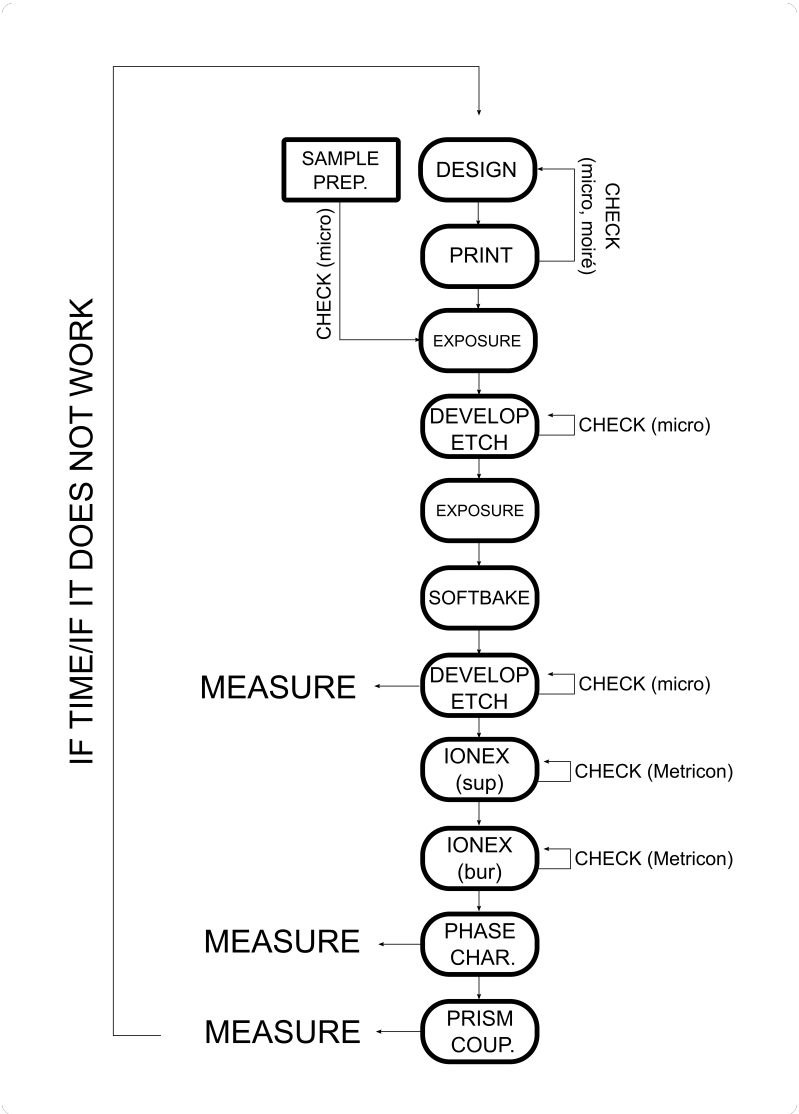


Figure B.1: *Flowchart comprising the main steps and workflow of the experimental microfabrication and characterization of the integrated devices described in Chapter 4.*

Appendix C

Full mask blueprint

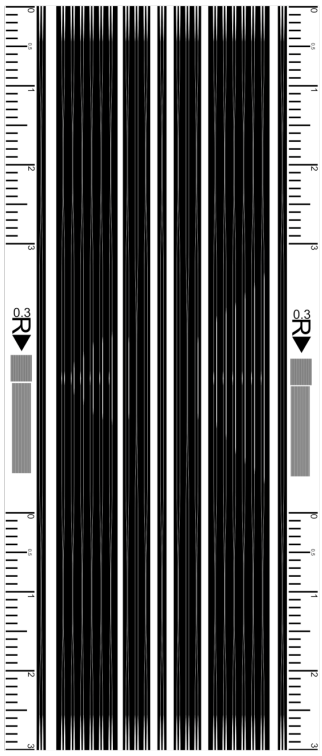


Figure C.1: *Blueprint of the mask used to obtain the results in Chapter 4. Rulers are for checking measures, while marks are used for orientation/reference. Diffraction gratings (pattern between the rulers) are for checking correct focusing, photoresist developing and etching during the fabrications stages. In the final sample, diffraction is visible on them to the naked eye as a bright colored dot.*

Appendix D

List of works related to this Thesis

- [50]: J. Liñares, X. Prieto-Blanco, G. M. Carral, M. C Nistal. Quantum Photonic Simulation of Spin-Magnetic-Field Coupling and Atom-Optical Field Interaction. *App. Sci.* 2020, 10, 8850. DOI: `https://www.doi.org/10.3390/app10248850`. ISSN=2076-3417. Applied Science Impact Factor (I.F) = 2.679 (2020); Q2 Applied Physics (2020). **Author contribution**: *literature review, computations regarding the photonic device specifics and illustrations, initial draft preparation.*
- [49]: J. Liñares, X. Prieto-Blanco, D. Balado and G. M. Carral. Fully Autocompensating High-Dimensional Quantum Cryptography by Quantum Degenerate Four-Wave Mixing. *Phys. Rev. A*, 2021. DOI:`https://www.doi.org/10.1103/PhysRevA.103.043710`. ISSN=2469-9934 (Online), 2469-9926 (Print). I.F=2.971 (2021); Q1 AMO Physics (2021). **Author contribution**: *optical error and secret key rate numerical simulations.*
- [76]: J. Liñares, G.M. Carral, X. Prieto-Blanco and D. Balado. Autocompensating Measurement Device - Independent Quantum Cryptography in Space Division Multiplexing Optical Fibers. *Journal of the European Optical Society - Rapid Publications*, 17(1):19, 2021. DOI:`https://www.doi.org/10.1186/s41476-021-00166-7`. ISSN=1990-2573. I.F = 2.021 (2021); Q2 (2021)) **Author contribution**: *device operations and security analysis (key rate simulation), initial draft preparation, illustrations.*
- [98]: G. M. Carral, J. Liñares, Eduardo F. Mateo, Xesús Prieto-Blanco. Bell State Exchange Parity-based Protocol for Efficient Autocompensation of QKD encoded in Polarization or Spatial Modes[1]. DOI: `https://www.doi.org/10.3390/app132312907`. ISSN=2076-3417. I.F = 2.7 (2022); Q2 Applied Physics (2023) **Author contribution**: conceptualization, computations & simulations, draft preparation, illustrations.
- [99]: G.M. Carral, J. Liñares and X. Prieto-Blanco. Autocompensating Measurement Device - Independent Multichannel Quantum Key Distribution in Multicore Optical Fibers. *XIII Reunión Nacional de Óptica*, 2021. **Author contribution**: *protocol design & numerical computations, text preparation.*

[1]Sent to AppSci on 10-10-2023, published on 1-12-2023.

Appendix E

Figure permissions

This Thesis is built upon content that the author of this Thesis has contributed to (co-authored). Of such content, only some figures (as specifically stated throughout the text) are exactly reproduced. The papers those figures where taken from ([50, 76, 98]) were published under a Creative Commons licence (CC BY 4.0), **that allows for full reproduction and adaptation of the licensed material, including figures**. The terms of such licence can be found in [161]. Other figures are work of this author original to this Thesis.

Below, screenshots of the licence as specifically noted in the review's webpages are shown.

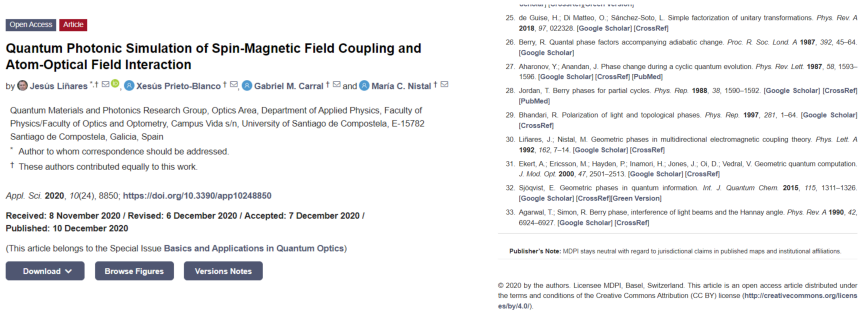


Figure E.1: *Screenshot of the CC-BY 4.0 Licence in Applied Sciences publication [50].*

Figure E.2: *Screenshot of the CC-BY 4.0 Licence in Applied Sciences publication [98].*

Rights and permissions

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Reprints and Permissions

About this article

Check for updates

Cite this article

Liñares, J., Carral, G.M., Prieto-Blanco, X. *et al.* Autocompensating measurement-device-independent quantum cryptography in space division multiplexing optical fibers. *J. Eur. Opt. Soc.-Rapid Publ.* **17**, 19 (2021). https://doi.org/10.1186/s41476-021-00166-7

Figure E.3: *Screenshot of the CC-BY 4.0 Licence in Journal of the European Optics Society - Rapid Publications, that is, publication [76], with reference to that same article at the bottom of the image.*

Bibliography

[1] John Dooley. *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*. Springer Cham, 2018.

[2] Peter Wayner. Chapter 2 - Encryption. In *Disappearing Cryptography (Third Edition)*, The Morgan Kaufmann Series in Software Engineering and Programming, pages 19–36. Morgan Kaufmann, Boston, third edition edition, 2009.

[3] IBM. Public key cryptography. `https://www.ibm.com/docs/en/ztpf/1.1.0.15?topic=concepts-public-key-cryptography`. Retrieved 15-05-2023.

[4] IBM. Exchanging DES or AES data-encrypting keys using an RSA key scheme. `https://www.ibm.com/docs/en/zos/2.3.0?topic=eksbn-exchanging-des-aes-data-encrypting-keys-using-rsa-key-scheme`. Retrieved 07-10-2023.

[5] Daniel M. Gordon. *Discrete Logarithm Problem*, pages 164–168. Springer US, Boston, MA, 2005.

[6] William P. Wardlaw. The rsa public key cryptosystem. In David Joyner, editor, *Coding Theory and Cryptography*, pages 101–123, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.

[7] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[8] Lily Chen *et al.* Report on post-quantum cryptography. *National Institute of Standards and Technology*, April 2016.

[9] NSA. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). `https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/`. Retrieved 15-05-2023.

[10] Eric Rescorla. Diffie-Hellman Key Agreement Method. RFC 2631, jun 1999.

[11] Hoi-Kwong Lo and Norbert Lütkenhaus. Quantum cryptography: from theory to practice. *arXiv: quant-ph/0702202v3*, 2007.

[12] Ryan Amiri *et al.* Secure quantum signatures using insecure quantum channels. *Phys. Rev. A*, 93:032325, Mar 2016.

[13] Liu-Jun Wang *et al.* Experimental authentication of quantum key distribution with post-quantum cryptography. *npj Quantum Information*, 7(1):67, May

2021.

[14] Valerio Scarani and Christian Kurtsiefer. The black paper of quantum cryptography: Real implementation problems. *Theoretical Computer Science*, 560:27–32, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[15] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[16] Víctor Zapatero *et al.* Advances in device-independent quantum key distribution. *npj Quantum Information*, 9(1):10, Feb 2023.

[17] Stefano Pirandola *et al.* Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4):1012–1236, Dec 2020.

[18] Marco Pistoia *et al.* Paving the way toward 800 gbps quantum-secured optical channel deployment in mission-critical environments. *Quantum Science and Technology*, 8(3):035015, may 2023.

[19] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10):686–689, Aug 2010.

[20] ETSI. Industry Specification Group (ISG) on Quantum Key Distribution (QKD). `https://www.etsi.org/committee/qkd`. Retrieved 15-05-2023.

[21] M Stanley, Y Gui, D Unnikrishnan, S.R.G Hall, and I Fatadin. Recent progress in quantum key distribution network deployments and standards. *Journal of Physics: Conference Series*, 2416(1):012001, dec 2022.

[22] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018.

[23] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.

[24] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, Oct 1982.

[25] Howard *et al.* Barnum. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett.*, 76:2818–2821, Apr 1996.

[26] Heng Fan *et al.* Quantum cloning machines and the applications. *Physics Reports*, 544(3):241–322, 2014. Quantum cloning machines and the applications.

[27] Christopher Monroe. Demolishing quantum nondemolition. *Physics Today*, 64(1):8–8, 01 2011.

[28] *Quantum Cryptography: Public key distribution and coin tossing.* New York: IEEE, 1984.

[29] David P. DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik*, 48(9-11):771–783, sep 2000.

[30] Khabat Heshami *et al.* Quantum memories: emerging applications and recent

advances. *Journal of Modern Optics*, 63(20):2005–2028, mar 2016.

[31] T. D. Ladd *et al.* Quantum computers. *Nature*, 464(7285):45–53, Mar 2010.

[32] Harry J.R. Dutton. *Understanding Optical Communications*. IBM, 1998.

[33] Emanuele Pelucchi *et al.* The potential and global outlook of integrated photonics for quantum technologies. *Nature Reviews Physics*, 4(3):194–208, Mar 2022.

[34] Taira Giordani *et al.* Integrated photonics in quantum technologies. *La Rivista del Nuovo Cimento*, 46(2):71–103, Feb 2023.

[35] Feihu *et al.* Xu. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92:025002, May 2020.

[36] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, pages 136–, 2004.

[37] Wenyuan Wang *et al.* Fully-passive quantum key distribution, 2022.

[38] Víctor Zapatero, Wenyuan Wang, and Marcos Curty. A fully passive transmitter for decoy-state quantum key distribution. *Quantum Science and Technology*, 8(2):025014, feb 2023.

[39] Marco Lucamarini *et al.* Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, May 2018.

[40] Stefano Pirandola *et al.* Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):15043, Apr 2017.

[41] Yang Liu *et al.* Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.*, 130:210801, May 2023.

[42] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, pages 503–509, 1998.

[43] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[44] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992.

[45] Teng-Yun Chen *et al.* Implementation of a 46-node quantum metropolitan area network. *npj Quantum Information*, 7(1):134, Sep 2021.

[46] Vicente Martin *et al.* The Madrid Testbed: QKD SDN Control and Key Management in a Production Network. In *2023 23rd International Conference on Transparent Optical Networks (ICTON)*, pages 1–4, 2023.

[47] M. Sasaki *et al.* Field test of quantum key distribution in the tokyo qkd network. *Opt. Express*, 19(11):10387–10409, May 2011.

[48] Daniel Balado Souto. *High dimensional autocompensating quantum cryptography in optical fibers implemented with discrete and integrated photonic devices.*

Phd thesis, University of Santiago de Compostela, 2021.

[49] Jesús Liñares *et al.* Fully autocompensating high-dimensional quantum cryptography by quantum degenerate four-wave mixing. *Phys. Rev. A*, 103:043710, Apr 2021.

[50] Jesús Liñares *et al.* Quantum photonic simulation of spin-magnetic field coupling and atom-optical field interaction. *Applied Sciences*, 10(24), 2020.

[51] Davide Scalcon *et al.* Cross-encoded quantum key distribution exploiting time-bin and polarization states with qubit-based synchronization. *Advanced Quantum Technologies*, 5(12):2200051, 2022.

[52] René-Jean Essiambre, Gerhard Kramer, Peter J. Winzer, Gerard J. Foschini, and Bernhard Goebel. Capacity limits of optical fiber networks. *Journal of Lightwave Technology*, 28(4):662–701, 2010.

[53] Christopher Gerry and Peter Knight. *Introductory Quantum Optics*. Cambridge University Press, 2004.

[54] Ulf Leonhardt. Quantum physics of simple optical instruments. *Reports on Progress in Physics*, 66(7):1207–1249, jun 2003.

[55] Gregor Weihs and Anton Zeilinger. Photon statistics at beam splitters: an essential tool in quantum information and teleportation. 2001.

[56] Yuan Cao *et al.* Entanglement-based quantum key distribution with biased basis choice via free space. *Opt. Express*, 21(22):27260–27268, Nov 2013.

[57] A. Pathak, A. Banerjee, and Society of Photo-optical Instrumentation Engineers. *Optical Quantum Information and Quantum Communication*. SPIE spotlight. SPIE press, 2016.

[58] Pieter Kok and Brendon W. Lovett. *Introduction to Optical Quantum Information Processing*. Cambridge University Press, 2010.

[59] Ralf Menzel *et al.* The photon: the role of its mode function in analyzing complementarity. *J. Opt. Soc. Am. B*, 36(6):1668–1675, Jun 2019.

[60] Ivan Moreno, Gonzalo Paez, and Marija Strojnik. Polarization transforming properties of dove prisms. *Optics Communications*, 220(4):257–268, 2003.

[61] Xesús Prieto-Blanco *et al.* Design of spatial-mode (de)multiplexer for few-mode fibers based on a cyclically used michelson-like interferometer. *Applied Sciences*, 10(23), 2020.

[62] Robert G. Hunsperger. *Integrated optics: theory and technology*. Springer, Berlin, 4th ed edition, 1995.

[63] B. Huttner, S. Serulnik, and Y. Ben-Aryeh. Quantum analysis of light propagation in a parametric amplifier. *Phys. Rev. A*, 42:5594–5600, Nov 1990.

[64] Jesús Liñares and María C. Nistal. Quantization of coupled modes propagation in integrated optical waveguides. *Journal of Modern Optics*, 50(5):781–790, 2003.

[65] Anthony Laing *et al.* Reference-frame-independent quantum key distribution.

Phys. Rev. A, 82:012304, Jul 2010.

[66] Michael Reck *et al.* Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61, Jul 1994.

[67] Artur Ekert *et al.* Geometric quantum computation. *Journal of Modern Optics*, 47(14-15):2501–2513, 2000.

[68] Michael V. Berry. Quantal phase factors accompanying adiabatic changes. *Proc. R. Soc. London A*, 392:45–57, 1984.

[69] Y. Aharonov and J. Anandan. Phase change during a cyclic quantum evolution. *Phys. Rev. Lett.*, 58:1593–1596, Apr 1987.

[70] Shun-Jin Wang. Nonadiabatic berry's phase for a spin particle in a rotating magnetic field. *Phys. Rev. A*, 42:5107–5110, Nov 1990.

[71] LP modes - RP Photonics Encyclopedia. `https://www.rp-photonics.com/lp_modes.html`. Retrieved 20-07-2023.

[72] I. Kaminow. Polarization in optical fibers. *IEEE Journal of Quantum Electronics*, 17(1):15–22, 1981.

[73] I. P. Kaminow. Polarization-maintaining fibers. *Applied Scientific Research*, 41(3):257–270, Sep 1984.

[74] Marcos Curty, What theorists should know when working with experimentalists. `https://www.youtube.com/watch?v=vFBSHBcLmGk`. Retrieved 20-07-2023.

[75] Hoi-Kwong Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, 18(2):133–165, Apr 2005.

[76] Jesús Liñares *et al.* Autocompensating measurement-device-independent quantum cryptography in space division multiplexing optical fibers. *Journal of the European Optical Society-Rapid Publications*, 17(1):19, Sep 2021.

[77] Understanding the Haar measure. `https://pennylane.ai/qml/demos/tutorial_haar_measure.html#understanding-the-haar-measure`. Accessed: 2023-04-19.

[78] T. A. Birks *et al.* The photonic lantern. *Adv. Opt. Photon.*, 7(2):107–167, Jun 2015.

[79] Donald S. Bethune and William P. Risk. Autocompensating quantum cryptography. *New Journal of Physics*, 4(1):42, jul 2002.

[80] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. Plug and play systems for quantum cryptography. *Applied Physics Letters*, 70(7):793–795, feb 1997.

[81] M. Eisaman *et al.* Invited Review Article: Single-photon sources and detectors. *Review of Scientific Instruments*, 82(7):071101, 07 2011.

[82] Pascale Senellart, Glenn Solomon, and Andrew White. High-performance semiconductor quantum-dot single-photon sources. *Nature Nanotechnology*,

12(11):1026–1039, Nov 2017.

[83] Evan Meyer-Scott, Christine Silberhorn, and Alan Migdall. Single-photon sources: Approaching the ideal through multiplexing. *Review of Scientific Instruments*, 91(4):041101, 04 2020.

[84] Pulse Repetition Rate. `https://www.rp-photonics.com/pulse_repetition_rate.html`. Accessed: 02-09-2023.

[85] Hoi-Kwong Lo and John Preskill. Security of quantum key distribution using weak coherent states with nonrandom phases, 2007.

[86] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[87] Robert W. Boyd. Chapter 2 - wave-equation description of nonlinear optical interactions. In Robert W. Boyd, editor, *Nonlinear Optics (Third Edition)*, pages 69–133. Academic Press, Burlington, third edition edition, 2008.

[88] Paul G. Kwiat *et al.* Ultrabright source of polarization-entangled photons. *Phys. Rev. A*, 60:R773–R776, Aug 1999.

[89] Fumihiro Kaneda *et al.* Heralded single-photon source utilizing highly nondegenerate, spectrally factorable spontaneous parametric downconversion. *Opt. Express*, 24(10):10733–10747, May 2016.

[90] Jesús Liñares *et al.* Interferometric space-mode multiplexing based on binary phase plates and refractive phase shifters. *Optics express*, 25 10:10925–10938, 2017.

[91] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76:012307, Jul 2007.

[92] James Schneeloch *et al.* Introduction to the absolute brightness and number statistics in spontaneous parametric down-conversion. *Journal of Optics*, 21(4):043501, feb 2019.

[93] Pieter Kok and Samuel L. Braunstein. Postselected versus nonpostselected quantum teleportation using parametric down-conversion. *Phys. Rev. A*, 61:042304, Mar 2000.

[94] M. Avenhaus *et al.* Photon number statistics of multimode parametric down-conversion. *Phys. Rev. Lett.*, 101:053601, Aug 2008.

[95] Christopher J. Chunnilall *et al.* Metrology of single-photon sources and detectors: a review. *Optical Engineering*, 53(8):081910, 2014.

[96] Robert H. Hadfield. Single-photon detectors for optical quantum information applications. *Nature Photonics*, 3(12):696–705, Dec 2009.

[97] Chandra M. Natarajan, Michael G. Tanner, and Robert H. Hadfield. Superconducting nanowire single-photon detectors: physics and applications. *Supercond. Sci. Technol.*, 25, Apr 2012.

[98] Gabriel M. Carral *et al.* Bell-state-exchange-parity-based protocol for efficient autocompensation of quantum key distribution encoded in polarization or spatial modes. *Applied Sciences*, 13(23), 2023.

[99] Gabriel M. Carral, Jesús Liñares, and Xesús Prieto-Blanco. Autocompensating Measurement-Device-Independent multichannel quantum key distribution in multicore optical fibers. *Reunión Nacional de Óptica*, 2021.

[100] W. T. Buttler *et al.* Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.*, 81:3283–3286, Oct 1998.

[101] Zhizhong Yan *et al.* Novel high-speed polarization source for decoy-state bb84 quantum key distribution over free space and satellite links. *Journal of Lightwave Technology*, 31(9):1399–1408, 2013.

[102] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948.

[103] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[104] Daniel Gottesman*et al.* Security of quantum key distribution with imperfect devices, 2004.

[105] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[106] Feihu *et al.* Xu. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92:025002, May 2020.

[107] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nature Photonics*, 8(8):595–604, jul 2014.

[108] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23), jun 2005.

[109] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Physical Review A*, 72(1), jul 2005.

[110] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, Apr 2000.

[111] Hoi-Kwong Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and proof of its unconditional security, 2005.

[112] Horace P. Yuen. Some physics and system issues in the security analysis of quantum key distribution protocols, 2014.

[113] Chi-Hang Fred Fung *et al.* Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A*, 75:032314, Mar 2007.

[114] Yi Zhao *et al.* Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78:042333, Oct 2008.

[115] Antonio Acín *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007.

[116] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014.

[117] H Yan *et al.* Design of panda ring-core fiber with 10 polarization-maintaining

modes. *Photon. Res.*, 5:1–5, Aug 2017.

[118] RP Encyclopedia. Retrieved 10-09-2023.

[119] Boosting subsea cables with Multi-Core fiber technology. `https://cloud.google.com/blog/products/infrastructure/delivering-multi-core-fiber-technology-in-subsea-cables`. Accessed: 2023-09-13.

[120] Nicolas Riesen *et al.* Monolithic mode-selective few-mode multicore fiber multiplexers. *Scientific Rep.*, 7:69711, Aug 2017.

[121] Tetsuya Hayashi. Multi-core fiber technology from design to deployment. In *European Conference on Optical Communication (ECOC) 2022*, page Mo4D.1. Optica Publishing Group, 2022.

[122] Feihu Xu, Marcos Curty, Bing Qi, and Hoi-Kwong Lo. Practical aspects of measurement-device-independent quantum key distribution. *New Journal of Physics*, 15(11):113007, nov 2013.

[123] Xiongfeng Ma and Mohsen Razavi. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A*, 86:062319, Dec 2012.

[124] Shi-Hai Sun *et al.* Practical decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A*, 87:052329, May 2013.

[125] Daniele Cozzolino *et al.* High-dimensional quantum communication: Benefits, progress, and future challenges. *Advanced Quantum Technologies*, 2(12):1900038, 2019.

[126] John Calsamiglia. Generalized measurements by linear elements. *Phys. Rev. A*, 65:030301, Feb 2002.

[127] Miloslav Dušek. Discrimination of the bell states of qudits by means of linear optics. *Optics Communications*, 199(1):161–166, 2001.

[128] Luca Dellantonio, Anders S. Sørensen, and Davide Bacco. High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces. *Physical Review A*, 98(6), dec 2018.

[129] Yonggi Jo *et al.* Efficient high-dimensional quantum key distribution with hybrid encoding. *Entropy*, 21(1), 2019.

[130] Yonggi Jo, Kwangil Bae, and Wonmin Son. Enhanced bell state measurement for efficient measurement-device-independent quantum key distribution using 3-dimensional quantum states. *Scientific Reports*, 9(1):687, Jan 2019.

[131] Comfort Sekga, Mhlambululi Mafu, and Makhamisa Senekane. High-dimensional quantum key distribution implemented with biphotons. *Scientific Reports*, 13(1):1229, Jan 2023.

[132] Jean-Emmanuel Broquin. Glass integrated optics: state of the art and position toward other technologies. In Yakov Sidorin and Christoph A. Waechter, editors, *Integrated Optics: Devices, Materials, and Technologies XI*, volume 6475, page 647507. International Society for Optics and Photonics, SPIE, 2007.

[133] Jean-Emmanuel Broquin and Seppo Honkanen. Integrated photonics on glass: A review of the ion-exchange technology achievements. *Applied Sciences*, 11(10), 2021.

[134] Giancarlo C. Righini *et al.* Glass integrated optics: 50 years and still growing strong. In *2019 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC)*, pages 1–1, 2019.

[135] P. K. Tien and R. Ulrich. Theory of prism–film coupler and thin-film light guides. *J. Opt. Soc. Am.*, 60(10):1325–1337, Oct 1970.

[136] R. Ulrich and R. Torge. Measurement of thin film parameters with a prism coupler. *Appl. Opt.*, 12(12):2901–2908, Dec 1973.

[137] Ming-Jun Li. Optical waveguide-characterization techniques. In S. Iraj Najafi, editor, *Introduction to glass integrated optics*, chapter 5, pages 107–136. Boston: Artech House, 1992.

[138] Xesús Prieto-Blanco *et al.* Quantum projectors implemented with optical directional couplers in ion-exchanged glasses. *Journal of Lightwave Technology*, 40(23):7676–7684, 2022.

[139] A. Milton and W. Burns. Mode coupling in optical waveguide horns. *IEEE Journal of Quantum Electronics*, 13(10):828–835, 1977.

[140] E. A. J. Marcatili. Dielectric rectangular waveguide and directional coupler for integrated optics. *The Bell System Technical Journal*, 48(7):2071–2102, 1969.

[141] Ari Tervonen. Theoretical analysis of ion-exchanged glass waveguides. In S. Iraj Najafi, editor, *Introduction to glass integrated optics*, chapter 4, pages 73–106. Boston: Artech House, 1992.

[142] W. Minford, S. Korotky, and R. Alferness. Low-loss ti:linbo3 waveguide bends at wavelength 1.3 µm. *IEEE Journal of Quantum Electronics*, 18(10):1802–1806, 1982.

[143] Carlos Montero Orille. *Modelización de guías de onda GRIN planares por intercambios iónicos sucesivos en vidro: aplicacións ó deseño e fabricación de compoñentes integrados.* Phd thesis, University of Santiago de Compostela, 1996.

[144] Xesús Prieto Blanco. *Guías ópticas integradas fabricadas por intercambio iónico en vidro mediante difusión asistida por campo eléctrico con efecto ión mixto.* Phd thesis, University of Santiago de Compostela, 2016.

[145] Xesús Prieto-Blanco and Carlos Montero-Orille. Theoretical modelling of ion exchange processes in glass: Advances and challenges. *Applied Sciences*, 11(11), 2021.

[146] M. Pluta. *Advanced light microscopy: Specialized methods. Vol. 2.* Advanced light microscopy: Specialized methods. PWN-Polish Scientific Publishers, 1988.

[147] Chrysanthe Preza, Donald L. Snyder, and José-Angel Conchello. Theoretical

development and experimental evaluation of imaging models for differential-interference-contrast microscopy. *J. Opt. Soc. Am. A*, 16(9):2185–2199, Sep 1999.

[148] Héctor González-Núñez and Xesús Prieto-Blanco. Quantitative multispectral wavefront sensing in the de senarmont dic microscope configuration.

[149] Daniel Malacara. *Optical Shop Testing (Wiley Series in Pure and Applied Optics)*. Wiley-Interscience, USA, 2007.

[150] C. Joenathan. Phase-measuring interferometry: new methods and error analysis. *Appl. Opt.*, 33(19):4147–4155, Jul 1994.

[151] M. R. *et al.* Arnison. Linear phase imaging using differential interference contrast microscopy. *Journal of Microscopy*, 214(1):7–12, 2004.

[152] Kou Shan Shan. Quantitative phase imaging and reconstructions for biological applications, 2010.

[153] Nobuyuki Otsu. A threshold selection method from gray-level histograms. *IEEE Transactions on Systems, Man, and Cybernetics*, 9(1):62–66, 1979.

[154] OCTAVE. Tresholding methods. `https://octave.sourceforge.io/image/function/im2bw.html`. Retrieved 28-09-2023.

[155] David J. Griffiths and Darrell F. Schroeter. *Introduction to Quantum Mechanics*. Cambridge University Press, 3 edition, 2018.

[156] Patricia Contreras-Tejada, Carlos Palazuelos, and Julio I. de Vicente. Resource theory of entanglement with a unique multipartite maximally entangled state. *Physical Review Letters*, 122(12), mar 2019.

[157] Joseph W. Goodman. *Statistical optics / Joseph W. Goodman*. Wiley series in pure and applied optics. John Wiley and Sons Inc., Hoboken, New Jersey, 2nd ed edition, 2015.

[158] Benjamin J. Puttnam *et al.* Characteristics of homogeneous multi-core fibers for SDM transmission. *APL Photonics*, 4(2):022804, 12 2018.

[159] T. Imai and T. Matsumoto. Polarization fluctuations in a single-mode optical fiber. *Journal of Lightwave Technology*, 6(9):1366–1375, 1988.

[160] Xiang-Bin Wang, Zong-Wen Yu, and Xiao-Long Hu. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A*, 98:062323, Dec 2018.

[161] Creative Commons. Attribution 4.0 international cc by 4.0 licence. `Attribution4.0InternationalCCBY4.0Licence`. Retrieved 17-07-2023.

Quantum Key Distribution (QKD) is a technique that provides perfect secrecy for communication systems, which is crucial against quantum computers capable of breaking current public-key cryptosystems.

QKD is becoming a mature technology but it still suffers from implementation problems due to imperfections on real hardware that soften it's security. To correct those is necessary to develop error mitigation mechanisms, as well as security by design through use of two-photon protocols.

In this Thesis, we combine these two approaches in fiber-based QKD, particularizing for evolved fibers with improved data bandwidths. At the same time, we emphasize integration with quantum photonics, and carry out actual microfabrication of basic elements in the laboratory for future QKD applications.