



João Pedro
Serra Ribeiro

**Distribuição de chave quântica com estados de
polarização gerados usando moduladores de fase**

**Quantum key distribution with polarization states
generated using phase modulators**





**João Pedro
Serra Ribeiro**

**Distribuição de chave quântica com estados de
polarização gerados usando moduladores de fase**

**Quantum key distribution with polarization states
generated using phase modulators**

Apresentado à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção da unidade curricular Projeto. Realizado sob a orientação do Dr. Nuno Silva, Investigador do Instituto de Telecomunicações da Universidade de Aveiro, e do Dr. Nelson Muga, Investigador do Instituto de Telecomunicações da Universidade de Aveiro.

o júri / the jury

presidente / president

Dr. Leonel Marques Vitorino Joaquim

Professor Auxiliar da Universidade de Aveiro

vogais / examiners committee

Dr. Nuno Alexandre Peixoto Silva

Investigador no Instituto de Telecomunicações de Aveiro

Dr. Paulo Fernando da Costa Antunes

Professor Auxiliar da Universidade de Aveiro

acknowledgements

I take this opportunity to express my gratitude to my supervisors Dr. Nuno Silva and Dr. Nelson Muga for providing me with the possibility and the tools to understand the quantum key distribution process and its inherent processes. I am extremely grateful for the guidance, encouragement and support throughout the course of this thesis.

I thank my family, girlfriend and friends for their assistance in multiple occasions discussing the processes of quantum key distribution and for the support during the course of this project.

I would like to acknowledge the Instituto de Telecomunicações and the project UIDB/50008/2020-UIDP/50008/2020 (action QuRunner), founded in part by FCT/MCTES through national funds and when applicable co-funded EU funds.

Resumo

Neste projeto abordou-se o processo de distribuição de chave quântica, codificando-se a informação em variáveis discretas usando estados de polarização provenientes de um laser atenuado que emitia luz a $1.55 \mu\text{m}$. Os estados de polarização foram gerados usando moduladores de fase eletro-óticos. Foi efetuada uma descrição detalhada, teórica e numérica, à geração dos estados de polarização recorrendo a moduladores de fase. Mais ainda analisou-se o impacto da variação da polarização dos estados gerados durante a evolução numa fibra ótica. Para além disso, foi também estudado como os moduladores de fase podem ser usados como dispositivos que permitem escolher bases aleatórias. Para tal, foi desenvolvido um sistema de distribuição de chave quântica e analisada a partilha de chave para implementação de um protocolo quântico. Foi abordado o protocolo BB84 e analisados os estados de polarização essenciais para a sua implementação. Após este processo, foi avaliada a taxa de erro quântica, essencial neste protocolo quântico, para análise a possíveis ataques.

Abstract

In this project we analyzed the quantum key distribution process, considering that information was codified in discrete variables using states of polarization from a attenuated laser emitting light at $1.55 \mu\text{m}$. The states of polarization were generated using eletro-optical phase modulators. A theoretical and numerical detailed description about generating states of polarization using phase modulators was made. Furthermore, the process of random basis choice at receiver is also studied considering that Bob uses a phase modulator and a polarization beam-splitter. As well, we observed how phase modulators can be used as devices that allow to choose random basis. Besides that, in this project the impact of the random variations of the quantum states during its propagation in standard optical fibers is also studied. To do so, a laboratorial setup was implemented to test the generation of the quantum states associated to the BB84 protocol. After this process, conclusions were taken about the transmission process, being evaluated the quantum error associated to the generation, transmission and detection of the quantum states, essential in this quantum protocol, to analyse possible eavesdropper attacks.

Conteúdo

Conteúdo	i
Lista de Figuras	ii
1 Introdução	1
2 O Protocolo Quântico BB84 e Fundamentos Teóricos	3
2.1 Protocolo Experimental BB84	3
2.2 Moduladores de Fase	5
2.3 Divisores Óticos Passivos	10
2.3.1 Divisor Óptico de Polarização (PBS)	10
2.4 Detetores de Fotões Únicos	11
2.5 Descrição Protocolo Experimental	12
3 Descrição Numérica da Geração, Propagação e Deteção de Estados de Polarização	13
4 Resultados Experimentais do Sistema de Distribuição de Chave Quântica	21
5 Conclusão	28
Bibliografia	29

Listas de Figuras

2.1	Representação dos estados de polarização na esfera de Poincaré.	4
2.2	Representação esquemática de um modulador de fase eletro-ótico, com representação dos eixos principais (esquerda) e dos eixos óticos (direita).	5
2.3	Modulador de fase eletro-ótico.	7
2.4	Apresentação de um BS (esquerda) e de um VOA (direita).	10
2.5	Apresentação de um Divisor Ótico de Polarização.	10
2.6	Detetor de fotões únicos.	11
2.7	Sistema clássico para implementação de sistemas de distribuição de chave quântica. Retirado de [8].	12
2.8	Montagens esquemáticas dos subsistemas.	12
3.1	Modulador de fase eletro-ótico com sistema de eixos definidos na base ortonormala.	13
3.2	SOP gerados para uso no protocolo quântico BB84, no sistema de transmissão.	15
3.3	SOP gerados para uma tensão contínua aplicada ao modelador de fase e para os estados de polarização do BB84, no sistema de transmissão.	16
3.4	SOPs de receção para uma tensão contínua aplicada e para o protocolo quântico BB84.	17
3.5	SOP do sistema global e com discriminação do BB84, com aumento da relação linear de PDL.	18
3.6	Evolução da birrefringência local da fibra para uma variação do comprimento de autocorrelação, L_C , e batimento, L_B	19
3.7	Evolução da birrefringência local da fibra, para diferentes valores de comprimento de batimento, e para parâmetros gerados melhorados de σ' e ρ'	20
3.8	Representação dos estados de polarização gerados provenientes da rotação arbitrária induzida pelos parâmetros da fibra.	20
4.1	Estado de polarização à saída de um laser com comprimento de onda $\lambda = 1550.12$ nm.	21
4.2	Representação dos estados de polarização nos subsistemas de distribuição de chave.	22
4.3	Representação dos estados de polarização para o sistema global.	22
4.4	Representação na esfera de Poincaré dos SOPs respetivos do BB84.	23
4.5	Setup experimental implementado.	23
4.6	Simulação da montagem experimental.	24
4.7	Deteção de fotões nos detetores, sem tensão aplicada no modulador de fase do sistema de transmissão.	24
4.8	Deteção de fotões nos detetores, com 60 mV aplicados no modulador de fase do sistema de transmissão.	25

4.9	Deteção de fotões nos detetores, com 120 mV aplicados no modulador de fase do sistema de transmissão.	25
4.10	Deteção de fotões nos detetores, com 180 mV aplicados no modulador de fase do sistema de transmissão.	26
4.11	Deteção de fotões nos detetores, com 200 mV aplicados no modulador de fase do sistema de transmissão.	26
4.12	Observação de estados quânticos no polarímetro que condicionaram a obtenção de resultados válidos.	27

Capítulo 1

Introdução

Desde há várias décadas, a partilha de informação desempenhou um papel fundamental para a sociedade. Desde comunicação via código morse, sobre posições estratégicas a adotar a nível político, até aos dias de hoje em que há partilha de informação por milhares de dispositivos conectados à Internet das Coisas, a partilha de informação foi essencial para o desenvolvimento tecnológico. Cada vez mais a população em geral recorre a dispositivos para partilha de informação: desde publicações nas redes sociais a troca de mensagens entre si, a informação partilhada e o caráter que as pessoas lhe dão, necessita de ser toda ela codificada num formato para transmissão de dados, de uma forma segura e privada. Foram então desenvolvidas, ao longo dos anos, formas de codificar e encriptar a informação de tal forma que se possibilitasse a comunicação.

Em 1832, *Samuel Morse* procedeu ao estudo de comunicação código morse [1], assim como *H.Nyquist* e *R.Fisher* [1], uns anos mais tarde em 1925, tentaram definir uma medida de informação. Mas foi durante a 2^a Guerra Mundial que, *Alan Turing* desenvolveu a máquina criptográfica "Enigma" que permitiu encriptar e desencriptar informação, conseguindo partilhar sobretudo códigos de guerra [2]. Mas foi *Shannon* que, em 1948, procurou uma teoria básica para a comunicação através de canais públicos, dando assim o primeiro passo para a abordagem da criptografia [2], desenvolvendo um trabalho sobre quantificação, armazenamento e comunicação da informação, mostrando como a informação consegue ser quantificada sob o formato de variáveis, de forma a ser partilhada e formatada para ser transmitida, com o trabalho desenvolvido em a "Teoria da Informação" [3]. Desde o desenvolvimento da máquina "Enigma" até ao trabalho desenvolvido por *Shannon*, deram-se passos enormes neste ramo de segurança de dados, uma vez que desempenham um papel fundamental em garantir a transmissão de dados de uma forma segura ao seu destinatário, sendo responsável por garantir a privacidade dos dados, mesmo que o transmissor os decida partilhar com vários utilizadores, sendo eles apenas os únicos capazes de ler a mensagem. Para tal, foram desenvolvidos mecanismos que possibilitassem esta transmissão de dados. O mecanismo do *one-time pad* [4] surgiu como um mecanismo de codificação de informação em que receptor e transmissor partilhavam uma chave, previamente conhecida entre ambos, de tamanho igual ou similar ao tamanho da informação transmitida [4, 5], sendo a chave uma sequência de números aleatórios. O mecanismo do *one-time pad* conseguia transmitir apenas uma mensagem por cada chave gerada o que, deste modo, garantia a segurança da informação geral a ser partilhada, caso a informação fosse intercetada [4, 5]. No entanto a partilha de informação pelo mecanismo do *one-time pad* embora segura, exigia um mecanismo capaz de partilhar a chave criptográfica entre emissor e receptor.

Na década de 80, foi implementado um sistema de encriptação baseado na partilha de chave quântica em que, um transmissor enviava uma string de estados quânticos aleatórios por canal quântico para um receptor. Os estados quânticos aleatórios que eram transmitidos e prosseguiam no canal quântico podem ser simplesmente estados de polarização que codificam

informação - conceito de estado de polarização a ser abordado no próximo capítulo. Este mecanismo de partilha de chave não só possibilitou uma maior eficiência no processo de partilha de informação como automatizava um canal quântico para transmissão de dados. Ainda assim, esta transmissão de dados conseguiria ser manipulada, uma vez que sabendo a chave quântica, ter-se-ia acesso à informação toda a ser transmitida. Esta área de estudo de manipulação de dados e reconhecimento da chave quântica denominada por criptografia quântica, consegue manipular a informação de tal forma que o receptor receba informação diferente da inicialmente transmitida.

Foi desta forma que em 1984, *Bennet* e *Brassard* desenvolveram um protocolo de chaves quânticas baseada em variáveis discretas em que encriptavam informação no estado quântico de um fotão a ser transmitido [4, 6]. Basearam o seu protocolo em possíveis dois pares de estados de polarização ortogonais entre si [3, 6]. Foi proposto que, ao codificar informação no estado de polarização do fotão, conseguiram enviar informação entre utilizadores de tal forma que, a string binária de transmissão teria por base uma chave quântica de partilha [4, 6]. Desta forma, conseguiu-se gerar chaves quânticas com elevadas taxas de bits, o que traduz numa eficiência total do sistema de transmissão. Atualmente, podemos alcançar taxas de transmissão segura de informação a distâncias a mais de 20 km de fibra ótica a uma taxa de 1.02 Mb/s [7].

Assim neste trabalho, pretende-se observar como o processo de partilha de informação ocorre num sistema de distribuição de chave quântica, tendo por base o protocolo quântico de variáveis discretas BB84. Ter-se-á como objetivo alcançar todos os diferentes estados de polarização no sistema, proveniente da variação da tensão externa fornecida aos moduladores de fase, assim como a taxa de sucesso na transmissão da chave quântica, através da avaliação da percentagem de erros e do QBER. Com isto, pretende-se mostrar que sistemas de distribuição de chave quântica tomam os primeiros passos em garantir a segurança e privacidade da informação partilhada, de uma forma totalmente eficiente, tendo por base um protocolo que se fundamenta no envio de bits aleatórios que codificam informação [4, 8].

No capítulo 2, abordar-se-á o conceito teórico de estado de polarização e o conjunto de pares de estados necessários para a implementação do protocolo quântico BB84, assim como a definição e descrição do processo de distribuição de chave quântica. Uma descrição detalhada do material usado no decorrer da atividade será também inserida, assim como os principais desafios na implementação deste tipo de sistemas de distribuição de chave. No capítulo 3, serão abordados e analisados resultados pré-experimentais teóricos relativos a simulações nos subsistemas do sistema quântico implementado e, no capítulo 4, abordados resultados experimentais obtidos em laboratório. No capítulo 5, serão retiradas conclusões acerca do desempenho do sistema quântico implementado.

Capítulo 2

O Protocolo Quântico BB84 e Fundamentos Teóricos

2.1 Protocolo Experimental BB84

Desenvolvido e implementado por *Bennet-Brassard*, o protocolo quântico BB84 consiste na implementação de uma comunicação segura entre utilizadores, através de um canal quântico. A escolha das bases de polarização por parte dos utilizadores - decorrente neste processo de distribuição de chave [4, 5] - consistia numa escolha aleatória entre duas bases de polarização não-comutáveis entre si, isto é, que permitam implementar pares de estados de polarização ortogonais entre si. Como exemplo, as bases retilínea e diagonal, representadas na tabela 2.1. Apresenta-se ainda, na tabela 2.1, uma possível correspondência entre estados de polarização e bits, sendo que o bit 1 correspondia a estados verticais, 90° na base retilínea, e estados a $+45^\circ$ na base diagonal, enquanto o bit 0 correspondia a estados horizontais, 0° na base retilínea e estados a -45° na base diagonal [6, 7].

Tabela 2.1: Ilustração em termos de bits dos estados de polarização.

Base	Bit 1	Bit 0
\oplus	$ \uparrow\rangle$	$ \leftrightarrow\rangle$
\otimes	$ \nearrow\rangle$	$ \searrow\rangle$

Neste relatório vamos implementar estados de polarização na base circular que serão perpendiculares à base de polarização diagonal. Os estados de polarização do fotão implementados, na base circular, são: polarização circular esquerda, $|LCP\rangle$, e polarização circular direita, $|RCP\rangle$. Os estados de polarização, denominados como *States of Polarization* (SOP), do fotão são descritos, na base diagonal e circular, baseado nos estados $|\uparrow\rangle$ e $|\leftrightarrow\rangle$ como [7, 8]:

$$|+45^\circ\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle + |\uparrow\rangle) \quad (2.1)$$

$$|-45^\circ\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle - |\uparrow\rangle) \quad (2.2)$$

$$|LCP\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle - i|\uparrow\rangle) \quad (2.3)$$

$$|RCP\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle + i|\uparrow\rangle) \quad (2.4)$$

A figura 2.1 ilustra os estados de polarização que serão implementados, nas bases diagonal e circular, assim como os estados definidos em base retilínea, $|\leftrightarrow\rangle$ e $|\uparrow\rangle$.

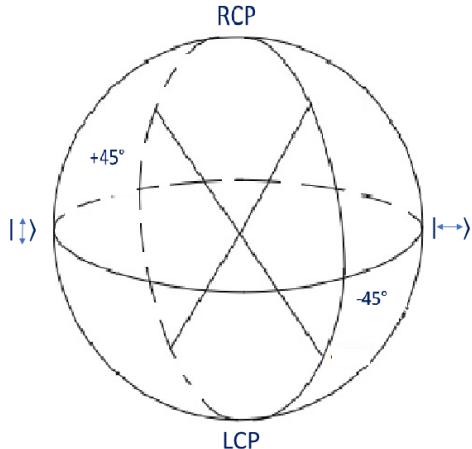


Figura 2.1: Representação dos estados de polarização na esfera de Poincaré.

De modo a observar-se como a distribuição de chave ocorre, são de seguida detalhados os passos inerentes a este processo [4, 5]:

1. O transmissor, normalmente conhecido como Alice, codifica informação em quatro estados de polarização gerados de forma aleatória, estados esses pertencendo a duas bases não ortogonais. Os fotões são enviados para o recetor, em intervalos de tempo bem definidos.
2. O recetor, normalmente conhecido como Bob, escolhe de forma aleatória e independente a base de polarização do fotão emitido, guardando a informação codificada nos fotões.
3. Através de um canal público, por exemplo um telefone, o recetor comunica a escolha de bases ao transmissor, analisando-se a correspondência entre bases, sem haver partilha de resultados.
4. As sequências aleatórias de bases de polarização são comparadas e o transmissor descarta as bases de polarização não coincidentes.
5. O transmissor informa por canal público o recetor em que intervalos de tempo pode validar os seus resultados, graças à correspondência entre bases emissor-recetor.
6. O recetor transforma o resultado das suas medições em bits e informa, por canal público, o transmissor dos bits obtidos. Desta forma, o transmissor é capaz de avaliar quantitativamente o erro associado à partilha de chave quântica através da taxa de erro quântica (QBER). Análises de QBER mostram que, caso o QBER seja inferior a 11% [11], a transferência de informação foi feita de forma segura, não havendo acesso à informação por parte do exterior. Os bits usados para obter o QBER do sistema são descartados pela Alice e pelo Bob.
7. No caso da comunicação ser segura, os utilizadores podem guardar os resultados partilhados como sendo a chave quântica secreta, utilizando a mesma para encriptação de mensagens. Contudo, no caso do erro ser superior a 25%, a comunicação não foi segura e todos os resultados deverão ser descartados e todo o processo efetuado novamente.

2.2 Moduladores de Fase

O modulador de fase eletro-ótico, constituído por Niobato de Lítio (LiNbO_3), baseia-se no efeito de Pockels onde o índice de refração de um dos eixos varia proporcionalmente ao campo elétrico aplicado. Na figura 2.2 apresentamos o sistema de eixos definido para representação do eixo ordinário, ao longo do eixo do y , e eixo extraordinário ao longo do eixo do z . A luz propaga-se segundo o eixo do x , sendo o campo elétrico aplicado entre faces do modulador, ao longo do eixo do z . Os índices de refração dos eixos ordinário e extraordinário são definidos respetivamente como [12]:

$$n_y = n_o - \frac{1}{2}n_o^3 r_o E_z \quad (2.5)$$

$$n_z = n_e - \frac{1}{2}n_e^3 r_e E_z \quad (2.6)$$

com n_o , n_e índices de refração dos eixos ordinário e extraordinário, respetivamente, e r_o , r_e coeficientes eletro-óticos.

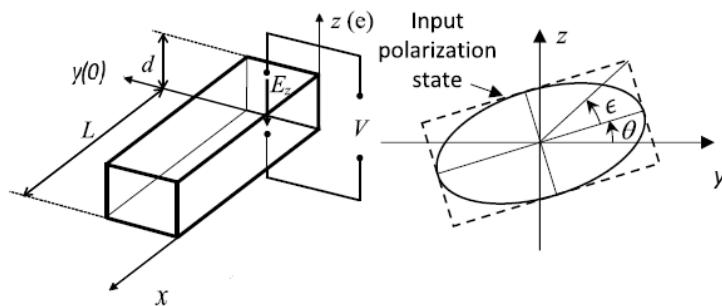


Figura 2.2: Representação esquemática de um modulador de fase eletro-ótico, com representação dos eixos principais (esquerda) e dos eixos óticos (direita).

Ideialmente, polarização perpendicular à propagação da luz seria segundo um dos seus eixos principais, neste caso z . Fibras que mantêm a polarização de um estado na sua propagação (PM) usadas no modulador de fase coincidem com os eixos principais do modulador. No entanto, fibras SMF, que não mantêm a polarização, assim como a má conexão nos adaptadores ao dispositivo, promovem um ligeiro desalinhamento relativamente aos eixos principais do modulador (ϵ), conferindo uma evolução elítica do estado de polarização. De modo a verificarmos como a evolui o estado de polarização no modulador de fase, analisemos em detalhe este processo definido em [12]:

- Na base($0y, 0z$), o campo ótico de entrada é definido como [12]:

$$q_0 = \begin{pmatrix} \cos \chi \\ \sin \chi e^{i\phi} \end{pmatrix} E_0 e^{i(2\pi v_0 t + \xi)} \quad (2.7)$$

com

$$\cos \chi = \sqrt{\cos^2(\theta) \cos^2(\epsilon) + \sin^2(\theta) \sin^2(\epsilon)} \quad (2.8)$$

$$\sin \chi = \sqrt{\sin^2(\theta) \cos^2(\epsilon) + \cos^2(\theta) \sin^2(\epsilon)} \quad (2.9)$$

$$\phi = \arg \left(\frac{\sin(\theta) \cos(\epsilon) + i \cos(\theta) \sin(\epsilon)}{\cos(\theta) \cos(\epsilon) - i \sin(\theta) \sin(\epsilon)} \right) \quad (2.10)$$

$$\xi = \arg(\cos(\theta) \cos(\epsilon) - i \sin(\theta) \sin(\epsilon)) \quad (2.11)$$

onde E_0 é a amplitude do campo elétrico, v_0 a frequência ótica, θ o ângulo entre eixo principal z e eixo ótico y , e ϕ está relacionado com a elipsidade do estado [12].

- A atuação do modulador de fase no campo ótico é descrita como [12]:

$$M_0 = \begin{pmatrix} e^{i\phi_y} & 0 \\ 0 & e^{i\phi_z} \end{pmatrix} \quad (2.12)$$

com ϕ_y e ϕ_z as fases impostas pelo modulador de fase ao longo dos eixos óticos. Para uma tensão aplicada ao modulador de fase $V(t) = V_{dc} + V_{rf} \sin(2\pi F_{mod} t)$, com fases relativas associadas ao eixos óticos [12]:

$$\phi_y = A_y + B_y \sin(2\pi F_{mod} t) \quad (2.13)$$

$$\phi_z = A_z + B_z \sin(2\pi F_{mod} t) \quad (2.14)$$

com V_{dc} voltagem DC imposta, V_{rf} sinal RF aplicado para modulação e F_{mod} frequência de modulação. Os coeficientes de 2.13, 2.14 são definidos como [12]:

$$A_y = -\frac{2\pi}{\lambda} L n_o + \frac{\pi}{\lambda} \frac{L}{d} n_o^3 r_o V_{dc} \quad (2.15)$$

$$B_y = \frac{\pi}{\lambda} \frac{L}{d} n_o^3 r_o V_{rf} \quad (2.16)$$

$$A_z = -\frac{2\pi}{\lambda} L n_e + \frac{\pi}{\lambda} \frac{L}{d} n_e^3 r_e V_{dc} \quad (2.17)$$

$$B_z = \frac{\pi}{\lambda} \frac{L}{d} n_e^3 r_e V_{rf} \quad (2.18)$$

com λ o comprimento de onda da luz incidente no modulador, proveniente do laser, L e d parâmetros físicos associados à largura e distância entre elétrodos do modulador de fase, respectivamente.

- O campo à saída do modulador de fase é definido como

$$Q_M = \begin{pmatrix} \cos \chi \\ \sin \chi e^{i[(\phi + A_z - A_y) + (B_z - B_y) \sin(2\pi F_{mod} t)]} \end{pmatrix} E_0 e^{i(2\pi v_0 t + \xi)} e^{i[A_z + B_y \sin(2\pi F_{mod} t)]} \quad (2.19)$$

- O estado elítico do SOP à saída do modulador de fase é descrito pelo termo

$$(\phi + A_z - A_y) + (B_z - B_y) \sin(2\pi F_{mod} t) \quad (2.20)$$

que traduz no aparecimento de uma modulação residual de polarização (RPM) proveniente da diferença dos diferentes valores de modulação dos índices óticos, sendo a sua

magnitude dada por $(B_z - B_y)$. Este efeito de RPM desaparece, no caso ideal, do estado de incidência no modulador ser linear ($\epsilon = 0$), o que traduz num alinhamento perfeito com os eixos principais do modulador de fase. Neste caso, verifica-se que se o SOP for perfeitamente linear, o SOP de saída do modulador é perfeitamente linear, sendo modulado com valor $B_y(\chi = 0^\circ)$ ou $B_z(\chi = 90^\circ)$.

- Existe ainda um valor residual de modulação, denominado como modulação residual de amplitude (RAM). Não é um valor intrínseco ao modulador de fase. Está associado às perdas dependentes da polarização (PDL) das fibras ópticas que constituem o material. As fibras ópticas apresentam valores típicos de PDL de 0.1 dB, o que promove intrinsecamente a criação de RAM. Situações de stress na fibra, devido ao seu enrolamento permite alterar a birrefringência das fibras ópticas, o que traduz na inserção de PDL [13]. Caso as fibras não tivessem PDL associado, não haveria criação de RAM embora houvesse RPM na mesma [12], [14].
- Na atividade, o sinal DC imposto é nulo, pelo que a magnitude de RPM não dependerá da componente DC do nosso sinal, apenas da componente de tensão aplicada para modulação, V_{rf} .

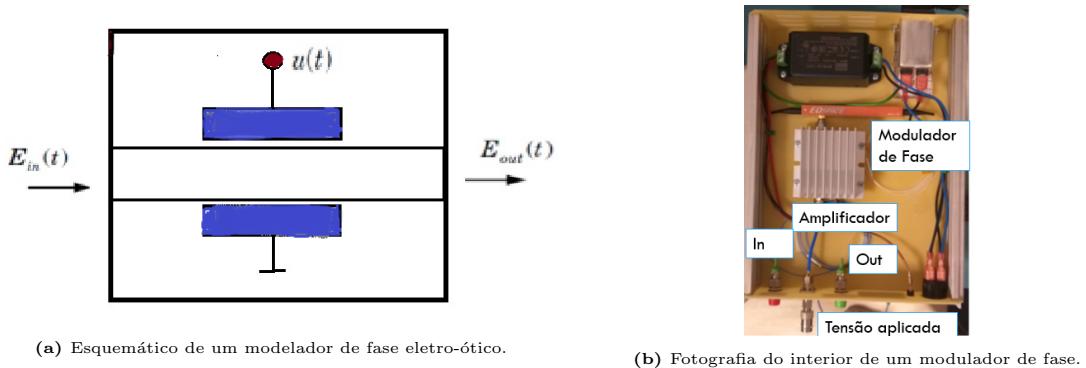


Figura 2.3: Modulador de fase eletro-ótico.

Observamos agora de forma detalhada como os moduladores de fases permitem gerar estados de polarização e, consequentemente gerar bases de polarização aleatórias, pela descrição do processo quântico de correspondência entre utilizadores, pela análise da tabela 2.2 [7, 8].

Neste sistema clássico de transmissão de chave quântica, com os utilizadores Alice e Bob, observamos como o processamento de toda a informação é efetuada, sendo a informação codificada na fase de fotões.

A Alice envia uma string binária de bits aleatórios codificados nas bases $(0, \pi)$ e $(\pi/2, 3\pi/2)$, tal como se observa na tabela 2.2, que representam o estado de polarização do fotão emitido. Na receção da string binária, o Bob efetua a escolha aleatória de bases entre 0 e $\pi/2$. O bit da Alice de transmissão condiciona a base dos estados de polarização do Bob, isto é, o bit 1 na base $(0, \pi)$ corresponde a termos $|\nearrow\rangle$, o que caso o Bob escolha a base $(0, \pi)$, corresponde a ter o mesmo SOP da Alice, havendo transmissão do bit quântico. Por outro lado, se a Alice envia um bit aleatório 0 na base $(0, \pi)$ corresponde a ter-se $|\searrow\rangle$ e caso o Bob escolha a base $(\pi/2, 3\pi/2)$, corresponde a termos $|RCP\rangle$, sem correspondência entre estados de polarização, não havendo transmissão do bit de informação. Se a Alice codificar a informação num bit aleatório 1 na base $(\pi/2, 3\pi/2)$, correspondente a transmitir um estado

Tabela 2.2: Representação do processo quântico de transmissão de chave.

Bit number	1	2	3	4	5	6
Alice bit	1	1	0	0	1	1
Base Alice	$(0,\pi)$	$(\pi/2,3\pi/2)$	$(0,\pi)$	$(\pi/2,3\pi/2)$	$(0,\pi)$	$(\pi/2,3\pi/2)$
Transmitted SOP	$ \nearrow \rangle$	$ LCP \rangle$	$ \searrow \rangle$	$ RCP \rangle$	$ \nearrow \rangle$	$ LCP \rangle$
Fase Alice	0	$\pi/2$	π	$3\pi/2$	0	$\pi/2$
Base Bob	$(0,\pi)$	$(0,\pi)$	$(0,\pi)$	$(0,\pi)$	$(\pi/2,3\pi/2)$	$(\pi/2,3\pi/2)$
Fase Bob	0	0	0	0	$\pi/2$	$\pi/2$
Received SOP	$ \nearrow \rangle$	$ \nearrow \rangle$	$ \searrow \rangle$	$ \searrow \rangle$	$ LCP \rangle$	$ LCP \rangle$
Phase's difference	0	$\pi/2$	π	$3\pi/2$	$-\pi/2$	0
Bob bit	1	-	0	-	-	1

circular $| LCP \rangle$, pelo que a informação do bit é partilhada caso, a base de polarização do Bob coincida com a base da Alice, isto é, base aleatória ($\pi/2, 3\pi/2$). Esta correspondência de bases não implica, necessariamente, uma validação dos resultados obtidos. Pelo que, uma das formas de erro, a mais clássica, pressupõe do facto de, o utilizador-espião usar um sistema de codificar informação em fotões únicos, semelhante ao da Alice, e/ou usar um sistema de deteção da informação idêntico ao do Bob. Este mecanismo de erro permite que, haja manipulação da informação partilhada sem que, qualquer dos utilizadores efetivamente se aperceba, uma vez que correspondência aleatória de bases de polarização, não corresponde necessariamente a resultados congruentes. Esta falta de congruência nos resultados, pressupõe dos sistemas de transmissão e/ou deteção utilizados pelo utilizador-espião, uma vez que estes resultam de escolhas arbitrárias de bases de polarização [7]. Por isto, como existem duas bases de polarização de transmissão do fotão, um potencial espião tem 50% de probabilidade de errar a base em que o fotão foi emitido, P_{right} , e o receptor tem 50% de probabilidade de receber informação totalmente manipulada, P_{eav} . Assim, os utilizadores podem guardar os resultados partilhados como sendo a chave quântica secreta, caso a probabilidade de erro, P_{Error} , seja inferior a 25% [7]-[9]:

$$P_{Error} = P_{right} \times P_{eav} = 0.5 \times 0.5 = 25\% \quad (2.21)$$

Para além deste ataque, existem outros. O melhor ataque de um utilizador-espião introduz um valor de QBER que ronda os 11%. A taxa de erro quântica (QBER), fulcral neste processo, permite avaliar quantitativamente a segurança do processo de distribuição de chave criptográfica, determinando se o processo de partilha de informação é comprometido. O QBER sendo uma probabilidade (determinística), consegue ser avaliado pelo rácio entre o número de bits errados (N_{Wrong}) e o número total de bits enviados (N_{Total}), sendo definido como [10]:

$$QBER = \frac{N_{Wrong}}{N_{Total}} \quad (2.22)$$

ou sendo definido à custa de taxas, nomeadamente pelo rácio entre taxa de erro (R_{Error}) e a taxa de compatibilidade associada à correspondência entre bases dos utilizadores (R_{Sift}) que correspondem a 50% dos casos. Assim, 2.22 pode ser reescrita como [10]:

$$QBER = \frac{R_{Error}}{R_{Sift}} \quad (2.23)$$

R_{Sift} é definido como [10]

$$R_{sift} = \frac{1}{2} q f_{rep} \mu \eta t_{link} \quad (2.24)$$

com q definido como um fator de correção, que para sistemas baseados na polarização é igual a 1, uma vez que está associado à taxa de correspondência da chave quântica entre os utilizadores, de tal forma que não está relacionada com erros indistinguíveis/ perdas na correspondência da transmissão de chave; f_{rep} frequência do sinal, μ número médio de fotões, η probabilidade de um fotão ser detetado e t_{link} , probabilidade do fotão chegar ao detector [10]. O número médio de fotões nesta atividade será $\mu \ll 1$. Para tal, usar-se-á um laser atenuado que permite gerar o número médio de fotões pretendido. Assim, a distribuição de fotões à saída do laser seguirá uma distribuição estatística de Poisson, que nos permite definir probabilidade de conter n fotões como [10]:

$$P(n, \mu) = \frac{\mu^n}{n!} \exp(-\mu) \quad (2.25)$$

e a probabilidade de um fotão ser detetado, η é definida como [10]:

$$\eta = 1 - P(n=0, \mu) \quad (2.26)$$

A probabilidade do fotão chegar ao detector é definida como [10, 11]:

$$t_{link} = 10^{-\alpha_F L} \quad (2.27)$$

com $\alpha_F = 0.22$, em unidades de dB/km, e L o comprimento da fibra, em unidades de km.

A taxa de erro, R_{Error} , é definida como um somatório de todas as contribuições de erro inerentes ao processo de distribuição de chave quântica. Uma das contribuições de erro provém das deteções das *dark counts* nos detectores desenvolvida por [11]:

$$R_{det} = \frac{1}{2} \frac{1}{2} f_{rep} n p_{dark} \quad (2.28)$$

com p_{dark} correspondente à probabilidade de detetar *dark counts* e n o número de detectores utilizados no processo de distribuição de chave quântica. O fator $\frac{1}{2}$ ocorre devido à probabilidade de ocorrer uma *dark count* quando não ocorre correspondência de bases entre utilizadores e, o outro fator de $\frac{1}{2}$, associado a uma probabilidade de ocorrer no detector errado. Outra forma de erro provém de um fotão ser detetado no detector errado. Este erro pode estar diretamente relacionado com interferências nos processos de polarização, nomeadamente stress aplicado nas fibras ópticas em processos de medição dos estados de polarização. A notação deste erro, R_{opt} é definido como [11]:

$$R_{opt} = R_{sift} p_{opt} = \frac{1}{2} q f_{rep} \mu n t_{link} p_{opt} \quad (2.29)$$

com p_{opt} probabilidade do fotão ir para o detector errado. Esta probabilidade de deteção de fotão no detector errado é definido como $p_{opt} = \frac{1-V}{2}$, com $V = 0.98$ definido como a visibilidade típica dos sistema de transmissão de chave quântica [11]. O QBER poderá ser reescrito como [11]:

$$QBER = \frac{R_{det} R_{opt}}{R_{sift}} = p_{opt} + \frac{n p_{dark}}{2 q \mu n t_{link}} \quad (2.30)$$

Por análise de 2.30, observa-se que o QBER não será nulo. A componente de visibilidade típica do sistema traduz num sistema quântico não-nulo. Dado que o QBER ocorre devido a ataques-espião e pode também ocorrer graças à imperfeição dos dispositivos, estes processos associados ao QBER tornam-se indistinguíveis. No entanto assume-se que, o QBER associado à partilha de chave-quântica do nosso sistema está associado a imperfeições dos dispositivos [11].

2.3 Divisores Óticos Passivos

Nesta secção, introduzimos os dispositivos de divisor de feixe e atenuadores ópticos essenciais neste processo de distribuição de chave, nomeadamente no processo da transmissão da informação, em que codificaremos a informação na fase do impulso ótico a ser transmitido. Desempenham um papel fundamental para atenuação do impulso, uma vez que os equipamentos apresentam limites (máximos e mínimos) de corrente e potência, sendo assim o sinal proveniente do laser atenuado. O divisor de intensidade (BS) usado será de 80/20 que, em conjunto com um atenuador óptico variável (VOA), permite ter um número médio de fotões a ser transmitido de $\langle n \rangle_T = 0.2$ fotões por impulso ótico.



Figura 2.4: Apresentação de um BS (esquerda) e de um VOA (direita).

2.3.1 Divisor Ótico de Polarização (PBS)

Nesta subsecção, introduzimos um dispositivo óptico de polarização que, neste sistema de transmissão de chave, desempenham um papel fulcral para correspondência entre bases transmissão-recepção. Um divisor de polarização decompõe o estado quântico nas suas componentes lineares, pelo que a correspondência entre bases de polarização, corresponde ao alinhamento de um dos eixos principais do PBS com uma das componentes lineares do estado de polarização, que permite confirmar a transmissão do bit, pela deteção do fotão - click num dos detetores [6, 7].



Figura 2.5: Apresentação de um Divisor Ótico de Polarização.

2.4 Detetores de Fotões Únicos

Neste subcapítulo, introduz-se os detetores de fotões únicos, essenciais em processos de distribuição de chave quântica (QKD). Adicionados após o divisor de polarização, segundo a figura 2.7, os detetores têm como principal objetivo determinar, de forma discreta, o número de fotões emitidos num impulso ótico. No entanto, os detetores apresentam algumas imperfeições internas que são notórias nestes processos de chave quântica como por exemplo, eventos de deteção "falsos" que descreveremos mais à frente. Assim, precedeu-se a uma caracterização total dos detetores, de forma a compreender-se como: (i) os detetores funcionam e (ii) que processos inerentes à deteção dos fotões condicionam processos QKD. Os detetores ideais de fotões únicos conseguem, na sua essência, detetar a totalidade de fotões emitidos num pulso. No entanto, o processo de deteção de fotões únicos num detector segue uma distribuição de Poisson [15]

$$p(\eta) = \lambda_0 T^\eta \frac{e^{-\eta}}{\eta!} \quad (2.31)$$

onde p representa a probabilidade de detetar η fotões, num impulso de período T , com λ_0 a taxa média de chegada de fotões, em unidades de fotões por segundo. No mesmo intervalo, a média de contagem de fotões únicos e a variância é desenvolvida por [15]

$$\mu_0 = \lambda_0 T \quad (2.32)$$



Figura 2.6: Detetor de fotões únicos.

No entanto, o rendimento de um detector usual não é o mesmo de um ideal. Eventos de *afterpulses* e *darkcounts* são das principais imperfeições num detector de fotões únicos [16]. Optou-se por configurar os detetores em modo *gated mode* - dos três modos, o mais útil para configurar o *deadtime* (período que o detector fica sem detetar, após uma deteção) e reduzir a largura da gate. Inicialmente, foram avaliados processos de *dark counts* - eventos de deteção falsos por parte dos detetores. As *dark counts* são, muitas vezes associadas, a cargas geradas por processos térmicos de transição que condicionam as contagens efetivas do detector pelo que, uma das formas de reduzir as *dark counts* seria arrefecer o detector, uma vez que a sua probabilidade de ocorrência está diretamente dependente da tensão fornecida e da sua temperatura, assim como a constituição interna dos sensores e arquitetura do detector [16]. As contagens das *dark counts* devem-se a dois fenômenos que são estatisticamente independentes, a criação das *dark counts* e a sua deteção. Diretamente relacionada com a frequência de deteção (ou frequência de click) e frequência da gate input, a probabilidade das *dark counts* é dada por:

$$P_{dc} = \frac{F_{dc}}{F_{gate}} \quad (2.33)$$

Processos de *afterpulses* não serão abordados neste processo de distribuição de chave, uma vez que não condicionam a taxa de erro quântica (QBER) do nosso sistema. Estes eventos de deteção "falsas" consistem no aprisionamento de cargas que se soltam e geram clicks nos detectores. Estes processos são condicionados pela temperatura e pelo processo de configuração de intervalo de tempo entre dois pulsos de gate. Estes processos de deteção de auto-interação são condicionados pela intensidade de luz que chega ao detector de fotões únicos, sendo a configuração do *deadtime* uma das soluções na diminuição na ocorrência destes eventos [16].

2.5 Descrição Protocolo Experimental

O protocolo experimental seguirá uma abordagem quântica relativa a processos optoeletrónicos, sobre estados de polarização, moduladores de fase, controladores de polarização, divisores de polarização e detectores de fotões únicos [8, 9]. Uma das dificuldades incidiu sobre emitir impulsos óticos de fotões únicos. Uma abordagem passaria por utilizar lasers que emitem impulsos óticos atenuados, denominados por *faint pulse sources* (FPS), que podem ser usados como aproximação a uma fonte verdadeira de fotões únicos nos casos em que o número de fotões médio é muito baixo, da ordem dos 0.2 fotões por impulso ótico. A figura 2.7 ilustra o setup experimental que seguiremos.

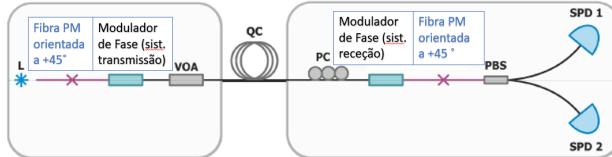


Figura 2.7: Sistema clássico para implementação de sistemas de distribuição de chave quântica. Retirado de [8].

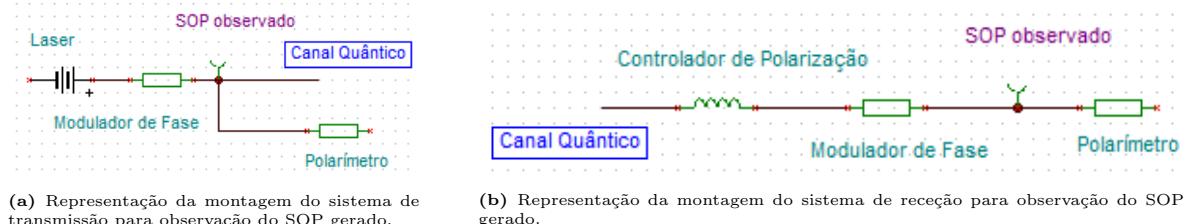


Figura 2.8: Montagens esquemáticas dos subsistemas.

A figura 2.8 ilustra esquematicamente onde foram efetuadas as medições dos estados de polarização dos subsistemas. Na receção da informação, o controlador de polarização permite compensar desvios de polarização, provenientes da propagação do estado de polarização em fibras convencionais, e rodar o plano de polarização de 90° no modulador de LiNbO_3 [8, 9]. O estado de polarização do fotão inicialmente transmitido propaga-se no modo TM do modulador eletro-ótico, pelo que a inserção de um controlador de polarização permitirá rodar o plano para o modo TE. O estado de polarização à saída do modulador de fase do sistema de receção segue, por fibra PM até ao PBS, onde será detetado o fotão, no sistema de receção. Neste ponto, é efetuada a correspondência entre bases de polarização e, como descrito no capítulo 2.1, validam-se os resultados obtidos e os erros associados à partilha de informação [8, 9]. No capítulo 3, abordar-se-á a análise prévia de resultados de um sistema de distribuição de chave quântica.

Capítulo 3

Descrição Numérica da Geração, Propagação e Detecção de Estados de Polarização

Neste capítulo abordar-se-ão os resultados previstos, por simulação numérica, em laboratório. A descrição numérica do esquema experimental, efetuada em python, permitiu observar como os subsistemas, de transmissão e receção, evoluem tendo em consideração PDL e o campo elétrico de entrada (E_{in}), para o sistema de transmissão. Permitiu assim, observar como o modulador de fase atuava no estado de polarização inicial e como os efeitos de PDL afetavam o estado quântico de saída. No sistema de receção, foi também descrito um sistema em python, com inserção de PDL e de um *Rotator*, por parte do controlador de polarização, para compensação de perdas, tal como descrito no capítulo 2.2.

De forma a gerarem-se estados de polarização necessários para a implementação do protocolo quântico BB84, aplicou-se V_0 , $V_{\frac{\pi}{2}}$, V_π , $V_{\frac{3\pi}{2}}$ no modulador de fase do sistema de transmissão. A tensão V_0 permite-nos manter o estado de polarização que chega ao modulador de fase por fibra PM, $| + 45^\circ \rangle$, tal como descrito na figura 2.7. Estas tensões aplicadas de $V_{\frac{\pi}{2}}$ e V_π corresponde a aplicar lentes de atraso de quarto de onda e meia-onda correspondentes a gerar estados quânticos $|RCP\rangle$ e $| - 45^\circ \rangle$, nomeadamente, pelo que $V_{\frac{3\pi}{2}}$ permite gerar um estado quântico simétrico a $V_{\frac{\pi}{2}}$, isto é, $|LCP\rangle$.

A tabela 3.1 mostra os valores das tensões V_0 , $V_{\frac{\pi}{2}}$, V_π , $V_{\frac{3\pi}{2}}$ externas aplicadas.

Tabela 3.1: Valores das tensões externas aplicadas para gerar estados quânticos, segundo o protocolo quântico BB84.

	V_0	$V_{\pi/2}$	V_π	$V_{3\pi/2}$
Tensão nominal/ mV	0	63	126	188

Na figura 3.1, descreve-se o sistema de eixos da base ortonormada considerada permitindo observar-se como a modulação de luz ocorre e como a equação 3.1 é manipulada, assim como a tensão aplicada V entre os elétrodos do modulador de fase.

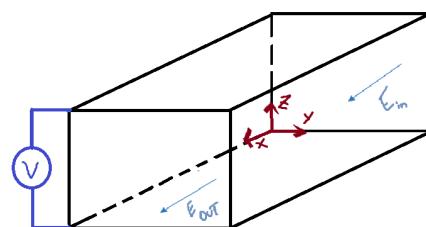


Figura 3.1: Modulador de fase eletro-ótico com sistema de eixos definidos na base ortonormada.

A equação que descreve todo o sistema de transmissão de informação é definida como [12]:

$$M_T = \phi_T \cdot J \cdot E_{\text{in}} \quad (3.1)$$

com ϕ_T a atuação do modulador de fase do sistema de transmissão no campo, $J_{2 \times 2}$ matriz correspondente à PDL do modulador de fase e E_{in} o campo elétrico à entrada do modulador de fase. A equação 3.1 é ainda desenvolvida, em termos de exponenciais, para modulação da luz. A propagação do campo elétrico é decomposto, segundo os eixos ópticos, no formato de equações de onda plana

$$\begin{cases} E_y = A_y \cdot e^{i(k_y - wt)} \\ E_z = A_z \cdot e^{i(k_z - wt)} \end{cases} \quad (3.2)$$

Este sistema de equações permite verificar que, sendo o estado quântico de incidência no modulador de fase é o $|+45^\circ\rangle$, uma vez que incide um SOP orientado a $|+45^\circ\rangle$ no modulador de fase do sistema de transmissão por fibra PM, segundo a figura 2.7, sendo as amplitudes de propagação do campo elétrico são numericamente iguais de valor $1/\sqrt{2}$. O modulador de fase eletro-ótico comporta-se como um guia de onda, pelo que as amplitudes de propagação do campo elétrico mantém-se constantes. A evolução do vetor de onda k poderá provocar alterações no campo elétrico, alterando residualmente as suas componentes vetoriais.

Para o desenvolvimento da equação 3.1, são definidas as funções de transferência do modulador de fase de transmissão, ao longo dos eixos ópticos, com fases impostas ϕ_{Ty} e ϕ_z . São também definidos os coeficientes de PDL associados a cada um dos eixos ópticos, J_y e J_z respectivamente.

$$M_T = \begin{pmatrix} e^{i\phi_{Ty}} & 0 \\ 0 & e^{i\phi_z} \end{pmatrix} \begin{pmatrix} J_y & 0 \\ 0 & J_z \end{pmatrix} \begin{pmatrix} E_y \\ E_z \end{pmatrix} \quad (3.3)$$

Como efetuamos modulação segundo o eixo ordinário O_y , a fase imposta pelo modulador de fase ao longo do eixo extraordinário considera-se constante. Considerou-se também efeitos de PDL ao longo do eixo ordinário. Assim, a fase imposta segundo o eixo modulado é definida como [12]:

$$\phi_{Ty} = \frac{V_{PM}}{V_\pi} \pi \quad (3.4)$$

com V_{PM} tensão aplicada no modulador de fase do sistema de transmissão e V_π , tensão a meio comprimento de onda [12]. Reescrevendo a equação 3.3, temos

$$M_T = \begin{pmatrix} e^{i\frac{V_{PM}}{V_\pi}\pi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} J & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad (3.5)$$

Desta forma, analisa-se que, o estado de polarização do impulso à saída do primeiro modulador será definido como:

$$\begin{cases} M_y = \frac{J}{\sqrt{2}} \cdot e^{i\frac{V_{PM}}{V_\pi}\pi} \hat{y} \\ M_z = \frac{1}{\sqrt{2}} \hat{z} \end{cases} \quad (3.6)$$

O código gerado em python permitiu então descrever, na forma matricial, os estados de entrada do modulador, do campo elétrico de entrada, da fibra ótica e de todo o sistema do receptor para toda a informação partilhada. Observou-se na esfera de Poincaré, gerada também em python, a representação dos estados de polarização do BB84 para as respetivas tensões fornecidas. Obteve-se os quatro estados de polarização do fotão que se conseguiram gerar na

esfera, através da implementação dos parâmetros de Stokes [17, 18]. O vetor de Stokes, que codifica os parâmetros de Stokes, tem quatro dimensões e é descrito como [17, 18]:

$$S = [S_0, S_1, S_2, S_3]^T \quad (3.7)$$

Os seus elementos descrevem a potência ótica de um sinal segundo determinados estados de polarização referência, os quais podem ser usados para implementação do protocolo quântico BB84.

Em termos de potência ótica do sinal, os parâmetros de Stokes têm o seguinte significado ótico [17, 18]:

S_0 = Potência total (polarizada e despolarizada).

S_1 = Diferença entre a potência ótica que passa por um polarizador linear horizontal e a potência ótica que passa por um polarizador linear vertical.

S_2 = Diferença entre a potência ótica que passa por um polarizador linear colocado segundo um ângulo $+45^\circ$ e a potência ótica que passa por um polarizador linear colocado segundo um ângulo -45° .

S_3 = Diferença entre a potência ótica que passa por um polarizador circular direito e um polarizador circular esquerdo.

Os parâmetros de Stokes normalizados correlacionam-se com o campo elétrico do sinal ótico, o que permite facilmente avaliar a transmissão de informação pela função de transferência do modulador de fase, através das expressões [17, 18]:

$$\frac{S_1}{S_0} = \frac{E_y E_y^* - E_z E_z^*}{E_y E_y^* + E_z E_z^*} \quad (3.8)$$

$$\frac{S_2}{S_0} = \frac{E_y E_z^* + E_z E_y^*}{E_y E_y^* + E_z E_z^*} \quad (3.9)$$

$$\frac{S_3}{S_0} = \frac{i(E_y E_z^* - E_z E_y^*)}{E_y E_y^* + E_z E_z^*} \quad (3.10)$$

Os parâmetros de Stokes normalizados foram gerados em python, de modo a gerarem estados de polarização do protocolo quântico BB84, sem PDL de transmissão.

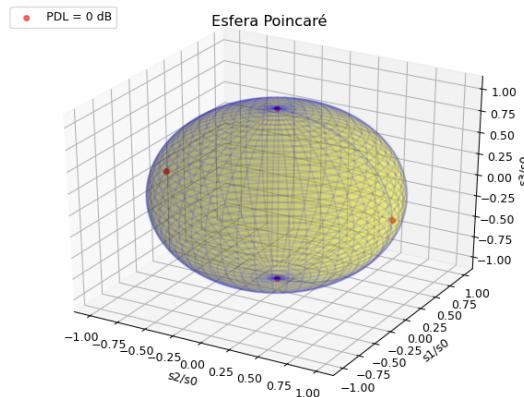


Figura 3.2: SOP gerados para uso no protocolo quântico BB84, no sistema de transmissão.

Ao observar-se a figura 3.2, vê-se que os estados circulares de polarização ocupam os pólos da esfera. Polarização circular direita em $S_3 = 1$ e polarização circular esquerda em $S_3 = -1$.

Luz linearmente polarizada a $+45^\circ$ e -45° distribuem-se no plano S_2-S_3 , nomeadamente, em $S_2 = 1$ e $S_2 = -1$. No plano S_1-S_2 , plano equatorial, encontram-se os estados de polarização lineares, desde o estado vertical $S_1 = -1$ ao estado horizontal $S_1 = 1$ [18].

Ao considerar-se os efeitos da PDL nos estados de polarização à entrada do modulador de fase, introduz-se uma descompensação nos índices de refração dos eixos ópticos. Deste modo, o estado de polarização do fotão poderá não coincidir totalmente com as componentes lineares dos estados de polarização obtidos. Por exemplo, um SOP a $+45^\circ$ poderá apresentar uma ligeira atenuação no estado $|\uparrow\downarrow\rangle$, devido à diferença refrativa dos índices gerada localmente que a PDL provoca [13]. Os estados de polarização $|+45^\circ\rangle$ e $| -45^\circ\rangle$ apresentam agora uma componente em S_1, S_3 assim como os estados de polarização em base circular que apresentam parâmetros de Stokes, em S_1, S_2 [17, 18].

A figura 3.3 representa os estados de polarização gerados para um aumento linear de PDL entre $[0, 2]$ dB.

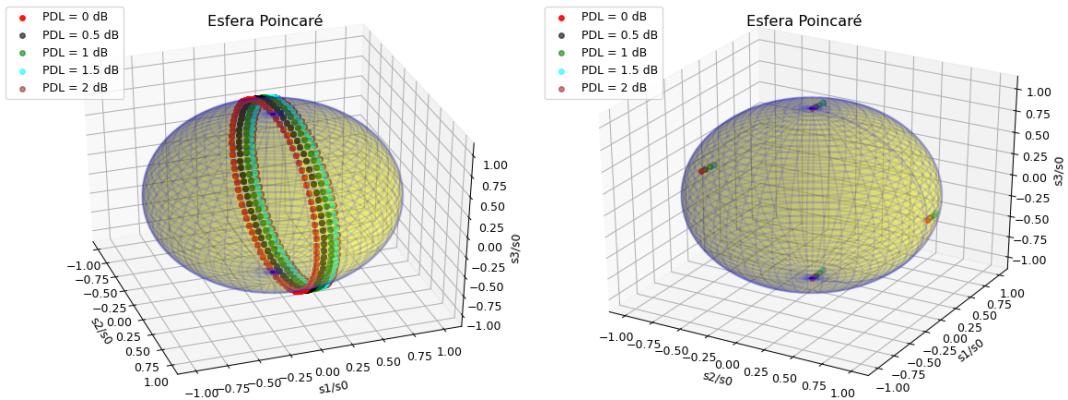


Figura 3.3: SOP gerados para uma tensão contínua aplicada ao modelador de fase e para os estados de polarização do BB84, no sistema de transmissão.

Pela análise da figura 3.3, vê-se que gerámos os estados de polarização necessários para a implementação do protocolo quântico BB84. Como o transmissor pode codificar informação em duas bases de polarização aleatórias, pode encriptar informação em possíveis quatro bits. Através da tensão externa fornecida de 0 V, 0.5 V, 1 V, 1.5 V, consegue gerar nomeadamente os estados quânticos possíveis: $|+45^\circ\rangle$, $|RCP\rangle$, $| -45^\circ\rangle$ e $|LCP\rangle$, respetivamente.

O sistema de receção é definido como [12]:

$$M_R = \phi_R \cdot \alpha \cdot R_\theta \quad (3.11)$$

com ϕ_R a atuação do modulador de fase do sistema de receção, $J_{2 \times 2}$ matriz correspondente ao PDL do sistema de receção, e R_θ como matriz rotação à entrada do modulador do sistema de receção. Estes parâmetros de compensação do PDL podem ser efetuados recorrendo a um *rotator*, descrito no espaço de Jones como [19]:

$$R_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \quad (3.12)$$

A equação 3.11 será desenvolvida pela transformação de $\theta = \pi/2$,

$$M_R = \begin{pmatrix} e^{i\phi_{Ry}} & 0 \\ 0 & e^{i\phi_z} \end{pmatrix} \begin{pmatrix} \alpha_y & 0 \\ 0 & \alpha_z \end{pmatrix} \begin{pmatrix} \cos(\frac{\pi}{2}) & \sin(\frac{\pi}{2}) \\ -\sin(\frac{\pi}{2}) & \cos(\frac{\pi}{2}) \end{pmatrix} \quad (3.13)$$

As componentes de receção da informação e de PDL, segundo o eixo extraordinário O_z consideram-se constantes. Assim, a fase imposta pelo modulador de fase do sistema de receção é definida como [12]:

$$\phi_R = \frac{V_{PM}}{V_\pi} \pi \quad (3.14)$$

com V_{PM} tensão aplicada no modulador de fase do sistema de receção [12]. Reescrevendo 3.13, temos

$$M = \begin{pmatrix} e^{i \frac{V_{PM}}{V_\pi} \pi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha_R & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad (3.15)$$

O sistema de receção da informação partilhada é definido pelo sistema de equações

$$\begin{cases} E_y = -\hat{y} \\ E_z = \alpha_R \cdot e^{i \frac{V_{PM}}{V_\pi} \pi} \hat{z} \end{cases} \quad (3.16)$$

A figura 3.4 retrata o sistema de receção de informação, descrito por 2.7, para observação de valores discretos dos parâmetros de Stokes, com um aumento linear de PDL. Os estados quânticos à entrada do *Rotator* são $|+45^\circ\rangle$ e $|RCP\rangle$, respetivamente.

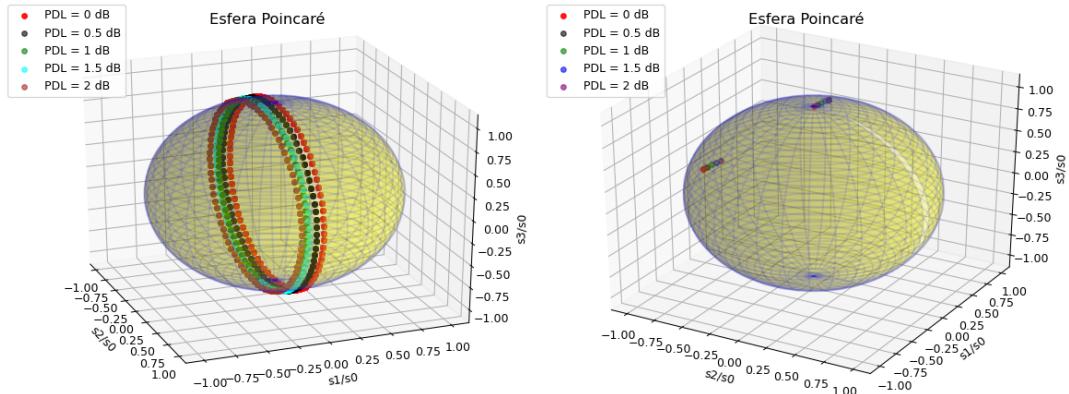


Figura 3.4: SOPs de receção para uma tensão contínua aplicada e para o protocolo quântico BB84.

Pela possível escolha de duas bases de polarização, o Bob consegue codificar informação em possíveis dois estados quânticos. Forneceu-se assim, 0 V e 0.5 V ao modulador de fase do sistema de receção, que nos permitiu gerar os estados quânticos orientados $| -45^\circ\rangle$ e $|RCP\rangle$, respetivamente.

A figura 3.5 descreve o sistema global de transmissão. Consideraram-se relações lineares $\Delta\alpha$, com $\Delta\alpha = \alpha_{R_y} - J_{T_y}$. Esta relação linear, com α a variar entre [0,2] dB e J fixo em 0 dB, traduz numa propagação da esquerda para a direita dos estados de polarização, na esfera de Poincaré.

Esta análise detalhada do sistema global, permite-nos verificar que os estados de polarização necessários para a implementação do protocolo quântico BB84 é alcançado, gerando-se os estados quânticos $| +45^\circ\rangle$, $| -45^\circ\rangle$, $|RCP\rangle$ e $|LCP\rangle$, respetivamente.

Os parâmetros da fibra que permitem rodar os estados de polarização de uma forma arbitrária serão agora abordados. De acordo com [19], os parâmetros da fibra ótica são

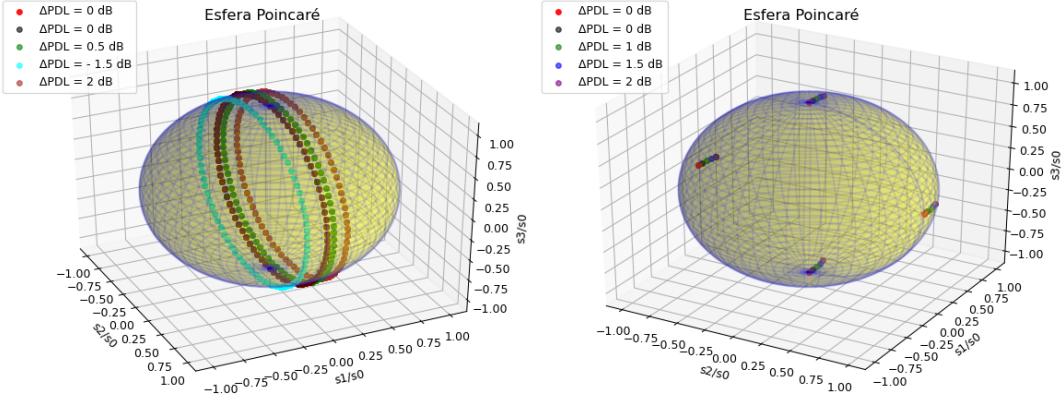


Figura 3.5: SOP do sistema global e com discriminação do BB84, com aumento da relação linear de PDL.

definidos no formato matricial como

$$R_{\theta_F} = \begin{pmatrix} \cos(\theta_F) & \sin(\theta_F) \\ -\sin(\theta_F) & \cos(\theta_F) \end{pmatrix} \quad (3.17)$$

com θ_F o ângulo de rotação induzido pela fibra.

Assim consegue-se prever que, num processo estatístico com parâmetros de valor médio e variância em distribuição normal, consegue-se gerar valores que permitem rodar os estados de polarização de forma totalmente aleatória [20].

A birrefringência em fibras ópticas segue uma distribuição linear. Deste modo, o vetor birrefringência local $\vec{\beta}$, para uma determinada frequência ω , pode ser descrito como [20]:

$$\vec{\beta}_{linear} = \omega \vec{b} = [\beta_1, \beta_2, 0]^T \quad (3.18)$$

O vetor birrefringência poderá ainda ter uma componente β_3 correspondente à componente circular do estado. Deste modo, vetor birrefringência pode ser descrito como o somatório das componentes lineares e circulares de um SOP [20]:

$$\vec{\beta} = \vec{\beta}_{circular} + \vec{\beta}_{linear} = \begin{bmatrix} 0 \\ 0 \\ \beta_3 \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \beta_2 \\ 0 \end{bmatrix} \quad (3.19)$$

Este caso de birrefringência, com componente circular e linear, traduz numa propagação elítica do estado de polarização na fibra [20, 21]. De modo a validarem-se os resultados obtidos em distribuição normal, foram gerados processos de Langevin [20, 21] para se atribuírem valores de birrefringência β_i que permitam modelar os estados de polarização. O processo de Langevin é definido como [20, 21]:

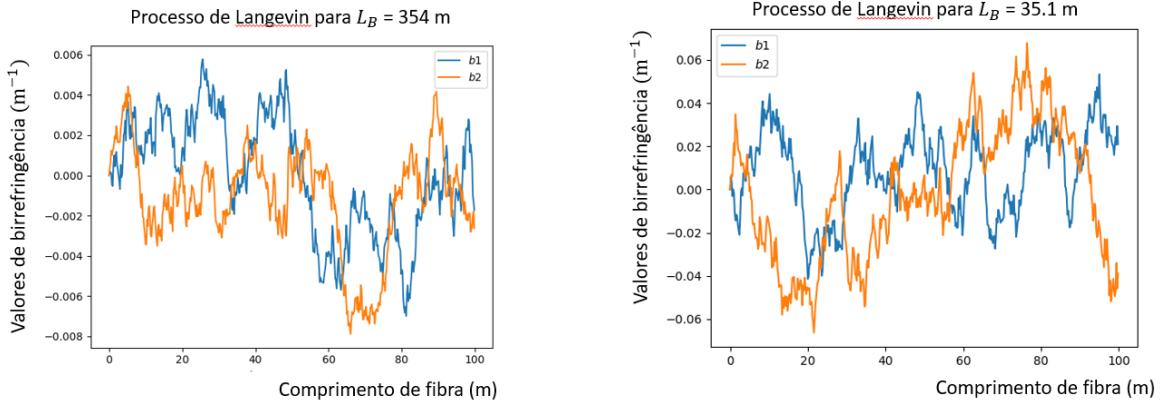
$$\frac{d\beta_i}{dz} = -\rho\beta_i + \sigma\eta_i \quad (3.20)$$

em que, η_1 e η_2 são funções de ruído branco independentes que seguem uma distribuição gaussiana, com valor médio nulo e variância igual a 1 [20, 21]. Os parâmetros ρ e σ são definidos em função de características do comprimento de fibra : comprimento de auto-correlação L_C , onde se considera que a evolução de estados de polarização são definidos à

custa do comprimento de fibra quando submetidos a perturbações estatísticas [20, 21], que permitem observar que, a potência ao longo do eixos óticos varia de acordo com [20]:

$$\frac{\langle P_y(L_C) \rangle - \langle P_z(L_C) \rangle}{P_{Total}} = \frac{1}{e^2} \quad (3.21)$$

e do comprimento de batimento, L_B , que corresponde à distância física que os estados de polarização percorrem para voltarem às configurações iniciais de polarização [20, 21].



(a) Características da componentes da fibra para: comprimento de auto-correlação $L_C = 10$ m e um comprimento de batimento $L_B = 354$ m, com parâmetros $\sigma = 0.0056\text{ m}^{-1}$ e $\rho = 0.1\text{ m}^{-1}$.

(b) Características da fibra: comprimento de autocorrelação $L_C = 19.7$ m e um comprimento de batimento $L_B = 35.1$ m, com parâmetros $\sigma = 0.0433\text{ m}^{-1}$ e $\rho = 0.051\text{ m}^{-1}$

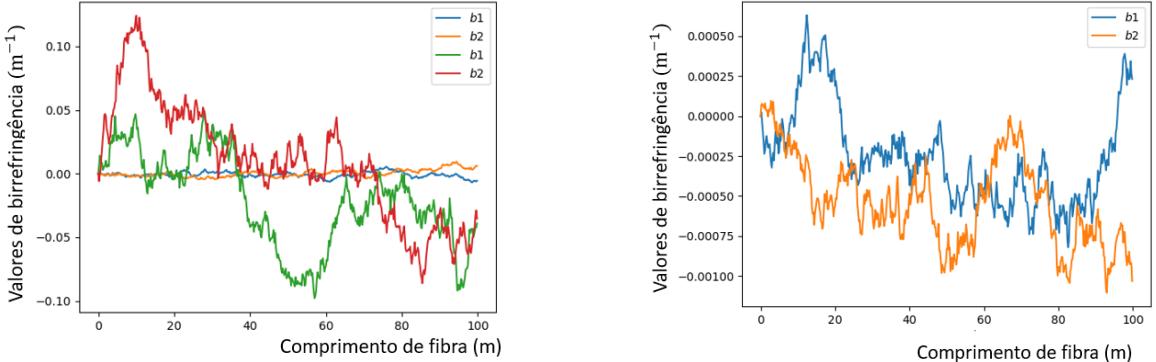
Figura 3.6: Evolução da birrefringência local da fibra para uma variação do comprimento de autocorrelação, L_C , e batimento, L_B .

De modo a avaliar-se esta birrefringência local, analisou-se em python a equação 3.20 com parâmetros específicos, que permitiu avaliar como a birrefringência local β_i da fibra evoluía para uma gama variável de comprimento de fibra [20, 21]. O comprimento de fibra considerado foi 100 m. No entanto, foi considerado um incremento local de 20 cm, considerando que este incremento é muito menor que qualquer comprimento inerente às características da fibra [20, 21]. A figura 3.7 ilustra a evolução da equação 3.20, para as componentes locais de birrefringência linear, β_1 e β_2 .

Da análise dos gráficos, vê-se que, uma diminuição do parâmetro ρ devido ao aumento do comprimento de autocorrelação L_C promova uma variação mais lenta de valores aleatórios de birrefringência gerada localmente, devido à memória armazenada em cada uma das componentes. No entanto, um aumento no comprimento de batimento L_B favorece uma diminuição do número de picos no gráfico, por diminuição nas flutuações, devido a perturbações estatísticas [20, 21]. Repare-se que, esta integração local dos parâmetros de birrefringência local, β_1 e β_2 , por parte do desenvolvimento dos processos de Langevin, representam a evolução do processo de birrefringência na fibra [20, 21], devido à memória armazenada no processo de birrefringência local.

Os gráficos 3.8 ilustram como os parâmetros da fibra influenciam a rotação arbitrária dos estados de polarização gerados para implementação do BB84, na esfera de Poincaré.

Na fase final experimental, foram adicionados dois detetores de fotões únicos, onde se procedeu à sua total caracterização. Ligados diretamente ao gerador de sinais, foi gerada uma onda quadrada, com frequência aplicada de 10 MHz, tensão aplicada pico-a-pico 2 V



(a) Gráfico ilustrativo da diferença entre valores de birrefringência alcançados de forma aleatória para um comprimento de batimento $L_B = 354$ m (linhas amarela e azul) e para um comprimento de batimento $L_B = 35,1$ m (linhas vermelha e verde).

(b) Gráfico representativo para o caso considerado, comprimento de autocorrelação $L_C = 10$ m e um comprimento de batimento $L_B = 354$ m, com parâmetros específicos (aleatórios) gerados: $\sigma' = 0.00056$ m⁻¹ e $\rho' = 0.001$ m⁻¹.

Figura 3.7: Evolução da birrefringência local da fibra, para diferentes valores de comprimento de batimento, e para parâmetros gerados melhorados de σ' e ρ' .

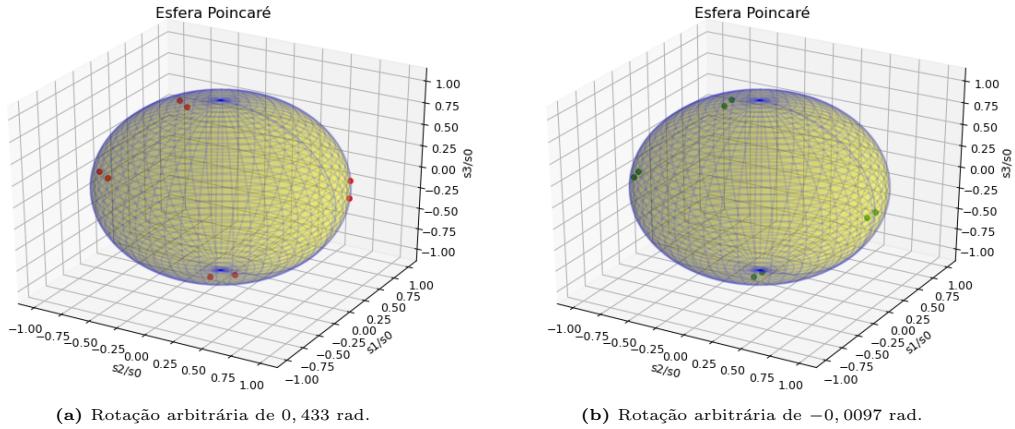


Figura 3.8: Representação dos estados de polarização gerados provenientes da rotação arbitrária induzida pelos parâmetros da fibra.

e com largura de banda de 15 ns, determinando-se as probabilidades das *dark counts* em cada um dos detetores. Para tal foi usado um software específico, fornecido pela Aurea, onde se configuraram os detetores com 10% eficiência, 10 s de *counting-rate*, 10 μ s de *deadtime* num intervalo de integração de 10 s. Estes parâmetros descritos influenciam diretamente a probabilidade destes eventos, pelo que durante a atividade mantiveram-se constantes. Assim, tal como descrito no capítulo 2.4, obtiveram-se experimentalmente as probabilidades de *dark counts* para o Model ID 005972:

$$P_{dc} = 0.0000360 \quad [\text{gate}^{-1}] \quad (3.22)$$

E para o Model ID 005973, com uma probabilidade inferior relativamente ao Model ID 005972, obteve-se experimentalmente:

$$P_{dc} = 0.0000041 \quad [\text{gate}^{-1}] \quad (3.23)$$

Estas probabilidades de *dark-counts* serão, deste modo essenciais, no cálculo do QBER associado à nossa atividade experimental.

Capítulo 4

Resultados Experimentais do Sistema de Distribuição de Chave Quântica

Em laboratório, a montagem experimental teve por base o esquema representado na figura 2.7. Tal como no capítulo anterior, dividiu-se o sistema em duas componentes: sistema de transmissão e sistema de receção, efetuando-se o tratamento de dados de cada um dos subsistemas. Após esta análise, observou-se o comportamento do sistema global, constituído por ambos os subsistemas. Um gerador de sinais foi adicionado com o modulador de fase de cada um dos subsistemas, de modo a fornecer um impulso de radio-frequência (RF). Forneceu-se uma onda quadrada com parâmetros: tensão de pico V_p variável entre [0,200] mV, com um incremento de 20 mV; duty cycle de 93.75 % - valor máximo de largura de banda que podemos implementar- de modo a ter-se componente DC num maior intervalo de tempo; frequência $f = 10$ MHz, com tempo de subida de 5 ns. Adicionou-se um laser centrado no comprimento de onda $\lambda = 1550.12$ nm. Primariamente mediram-se as componentes de PDL experimentais, à saída do laser, através de medições relativas a diferença entre valores máximos, P_{max} , e mínimos, P_{min} , de potência com recurso a medidores de potência ótica. As equações relativas aos valores experimentais de PDL são

$$PDL_{T_y} \equiv J = P_{max}(\text{dBm}) - P_{min}(\text{dBm}) = 1.38 \text{ dB} \quad (4.1)$$

$$PDL_{R_y} \equiv \alpha = P_{max}(\text{dBm}) - P_{min}(\text{dBm}) = 1.01 \text{ dB} \quad (4.2)$$

E observou-se o SOP à saída do laser, ligando-se diretamente o laser ao polarímetro (sem tensão aplicada no gerador de sinais), tal como mostra a figura 4.1.

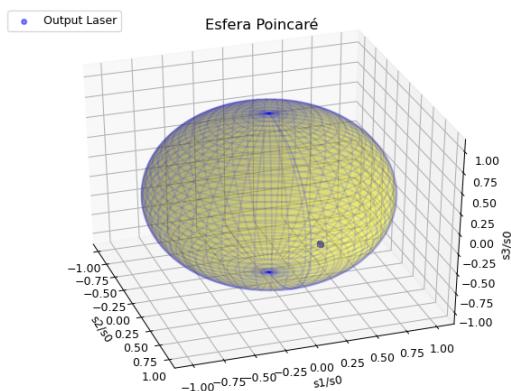


Figura 4.1: Estado de polarização à saída de um laser com comprimento de onda $\lambda = 1550.12$ nm.

As figuras 4.2 ilustram os estados de polarização com PDL associado aos subsistemas do sistema de distribuição de chave, implementando-se o protocolo quântico BB84. Note-se que estes resultados são teóricos e gerados em python. Nesta parte de tratamento de dados, apenas se alterou o parâmetro de PDL dos subsistemas, de modo a avaliar-se os resultados previstos.

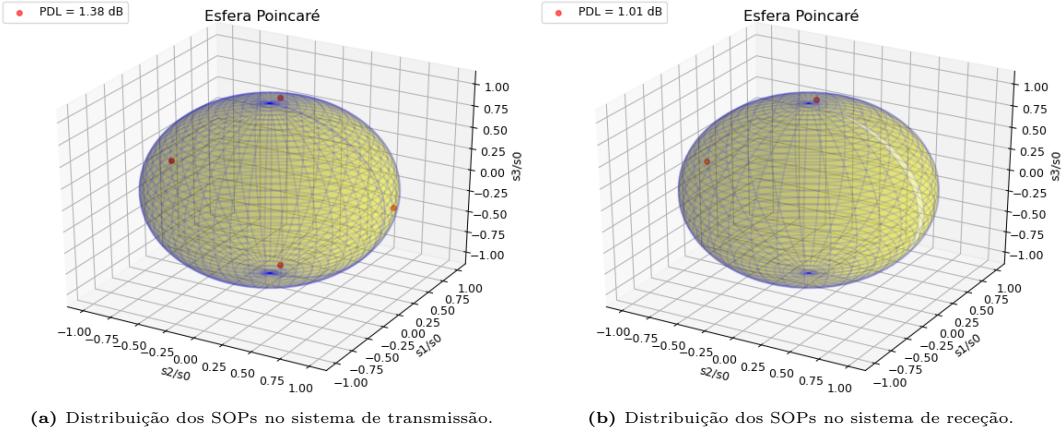


Figura 4.2: Representação dos estados de polarização nos subsistemas de distribuição de chave.

A figura 4.3 ilustra a distribuição dos estados de polarização no sistema global. Montou-se a montagem experimental representada na figura 2.7, e observou-se como se comportava o sistema na globalidade, com PDL associado.

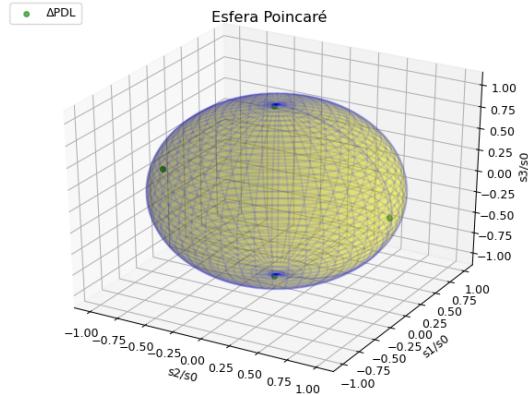
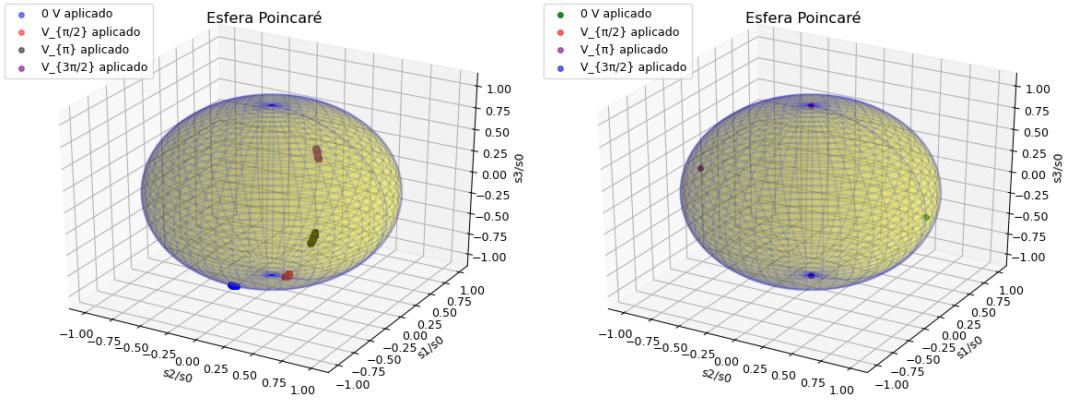


Figura 4.3: Representação dos estados de polarização para o sistema global.

Após este processo de distribuição de estados de polarização nos subsistemas do esquema experimental de distribuição de chave, aplicaram-se as respetivas tensões $V_{\frac{\pi}{2}}$, V_π e $V_{\frac{3\pi}{2}}$ no sistema de transmissão de modo a observar-se como os estados de polarização se distribuíam na esfera, representado na figura 4.4.

Analizando-se a figura 4.4, verifica-se que, sem tensão aplicada, o estado de polarização de saída do modulador de fase do sistema de transmissão apresenta componentes normalizados de Stokes em S_2-S_3 pelo que, tensões externas aplicadas no modulador de fase, para implementação do BB84, geram estados de polarização não-ortogonais uma vez que não estarão perfeitamente alinhados com os eixos da esfera. Observa-se por outro lado que, as tensões aplicadas de $V_{\frac{\pi}{2}}$ e $V_{\frac{3\pi}{2}}$ não geram de forma ideal os estados de polarização $|RCP\rangle$ e $|LCP\rangle$,



(a) Distribuição dos quatro estados de polarização para uso do protocolo quântico BB84.
(b) Representação do caso ideal dos quatro estados quânticos respectivos do protocolo quântico BB84.

Figura 4.4: Representação na esfera de Poincaré dos SOPs respetivos do BB84.

respetivamente. Isto poderá dever-se ao facto dos moduladores de fase estarem a apresentar uma deriva de estado de polarização para algumas das voltagens usadas. Da análise efetuada, tal efeito poderá dever-se a alguma imperfeição intrínseca ao próprio modulador de fase, não tendo sido possível de identificar no âmbito deste projeto. Para além disso, as figuras 4.2 e 4.3 foram geradas em python e representam resultados teóricos previstos, uma vez que esta deriva do estado de polarização para as voltagens para gerar estados quânticos condicionou a implementação dos estados quânticos necessários à implementação do protocolo quântico BB84. No entanto, de modo a verificar-se se a correspondência de bases aleatórias ocorria entre a Alice e o Bob, foi montado um setup experimental que permitisse observar os processos de deteção de fôtons nos detectores. Para tal, foi fornecido um impulso de voltagem de entrada entre [0,200] mV, com um incremento de 20 mV, que permitia gerar estados de polarização na esfera de Poincaré toda, ao modulador de fase do sistema de transmissão, tal como representado na figura ???. Logo após, foi ligado um VOA em série com um BS com 40 dB de atenuação. O BS 80/20 permite que 20% da luz siga para o sistema de receção, contendo a informação que se deseja partilhar. Após este processo, é adicionado um controlador de polarização em série com o modulador de fase do sistema de receção, em conjunto com um PBS, que permite decompor o estado de polarização nas suas componentes lineares. Finalmente, nos detectores veremos como os picos de deteção traduzem a coincidência de bases de polarização do sistema quântico.

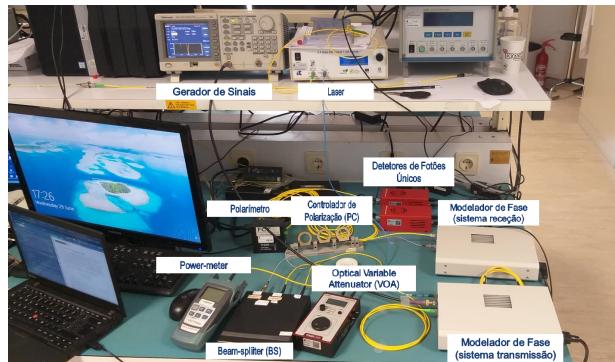


Figura 4.5: Setup experimental implementado.

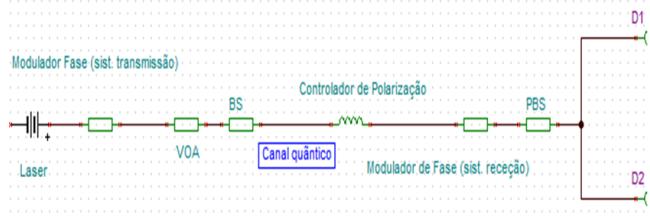


Figura 4.6: Simulação da montagem experimental.

Para este efeito de deteção de click nos detetores, foram definidas as mesmas configurações das medições realizadas nas equações 3.22 e 3.23, mas em modo contínuo. Vamos considerar os casos em que se forneceu tensão que permitia implementar estados quânticos relativos ao protocolo quântico BB84, descrito na secção 3.1. Para tal, foi montado experimentalmente o esquema representado pela figura ???. Os detetores foram adicionados após o divisor de polarização. Prevê-se que, caso as bases de polarização coincidam, haja um aumento de amplitude significativo num dos detetores, mantendo-se o pico de amplitude no outro detetor constante, proveniente da decomposição do estado quântico, nas suas componentes lineares, que alinham com um dos eixos do PBS [23]. A figura 4.7 ilustra as combinações de bases de polarização, de acordo com o protocolo quântico BB84.

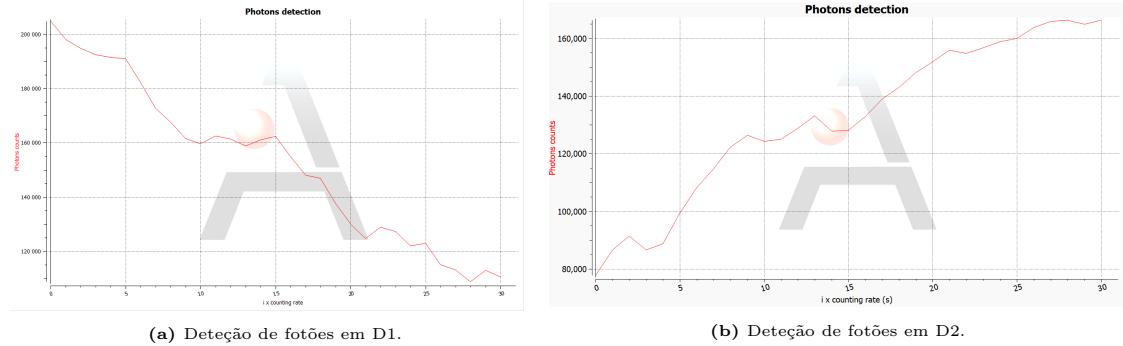


Figura 4.7: Deteção de fotões nos detetores, sem tensão aplicada no modulador de fase do sistema de transmissão.

Da análise dos resultados presentes na figura 4.7 verifica-se que, no instante inicial do processo de contagem, há uma diferença significativa entre amplitudes de pico nos detetores, o que traduz que, durante *counting-rate* inicial, há congruência entre bases de polarização. Nota-se que, no segundo processo de *counting-rate*, há um diminuição significativa de amplitude de pico em D1, havendo igualdade no número de contagens de fotões quer em D1 quer em D2, o que traduz que as bases de polarização não coincidem. Na última *counting-rate*, há um aumento significativo da contagem de fotões em D2 relativamente a D1. Traduz assim num aumento de amplitude de pico, devido à correspondência de bases.

Um caso bastante notório desta diferença entre amplitude de picos, ocorre para uma tensão externa fornecida próxima dos 60 mV, correspondente a fornecer-se $V_{\frac{\pi}{2}}$, o que implica teoricamente que, à saída do modulador de fase do sistema de transmissão, gerámos um estado quântico circular $|RCP\rangle$ [22].

Logo no início do intervalo de *counting-rate*, na figura 4.8, a diferença entre amplitudes de pico já é bastante notória. Veja-se que, há uma diferença a rondar 70000 contagens de fotões, o que evidencia de forma clara, a validação de bases de polarização entre a Alice e

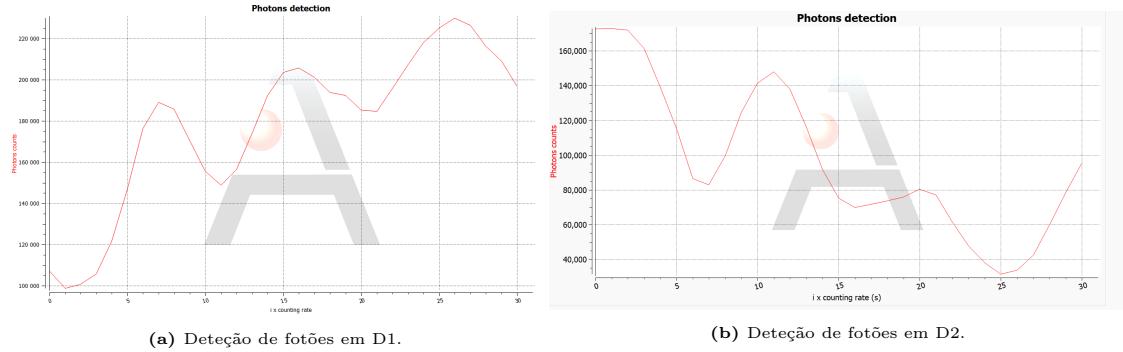


Figura 4.8: Deteção de fotões nos detetores, com 60 mV aplicados no modulador de fase do sistema de transmissão.

o Bob. Na mesma *counting-rate*, por volta dos sete segundos, nota-se numa descida abrupta da amplitude de pico em D2 e num aumento do número de fotões em D1, que traduz numa diferença entre amplitudes significativa, correspondente à coincidência de bases. Já no início do segundo intervalo de *counting-rate*, o número de fotões detetados é o mesmo, que traduz na não coincidência entre bases de polarização. Já a partir dos quinze segundos, observa-se que a amplitude de pico em D2 diminui significativamente, correspondendo à ativação total de D1, ou seja, coincidência de bases de polarização entre utilizadores.

A figura 4.9 corresponde a fornecer V_π ao modulador de fase do sistema de transmissão. Segundo [22], corresponde a ter na saída do modulador de fase um estado quântico orientado a -45° , na base diagonal.

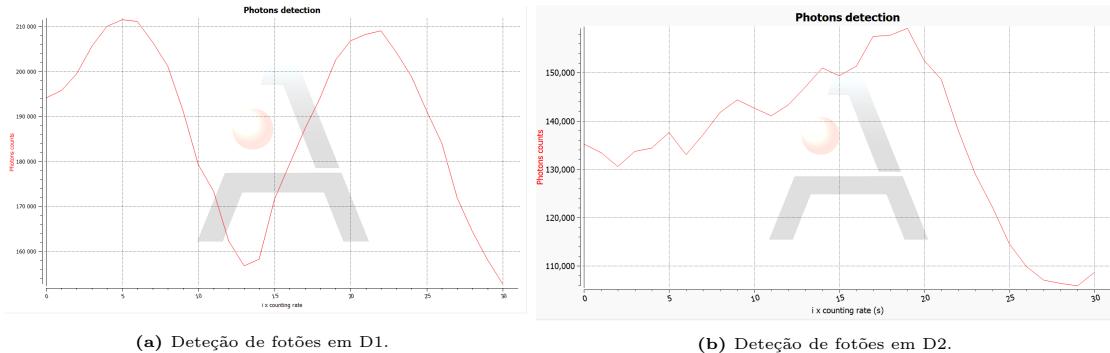


Figura 4.9: Deteção de fotões nos detetores, com 120 mV aplicados no modulador de fase do sistema de transmissão.

Por análise de 4.9, vê-se que praticamente durante todo o intervalo de integração existiu correspondência entre bases emissor-recetor. Observa-se que, a contagem de fotões é sempre maior em D1, exceto no intervalo de tempo [10, 15] segundos, onde se regista um valor de pico de amplitude idêntico [7, 8]-[23].

As figuras 4.10 e 4.11, correspondem a fornecer-se $V_{\frac{3\pi}{2}}$ ao modulador de fase gerando-se $|LCP\rangle$ [22].

A figura 4.10 evidencia concordância de bases de polarização no primeiro intervalo de *counting-rate* [23]. No intervalo [10,15] segundos do segundo intervalo de *counting-rate*, as bases de polarização poderão coincidir ou não, uma vez que o número de fotões nos picos de integração são próximos. A partir deste instante, há plenamente uma concordância de bases de polarização entre a Alice e o Bob. Consegue-se mostrar em 4.11 a simetria das curvas de

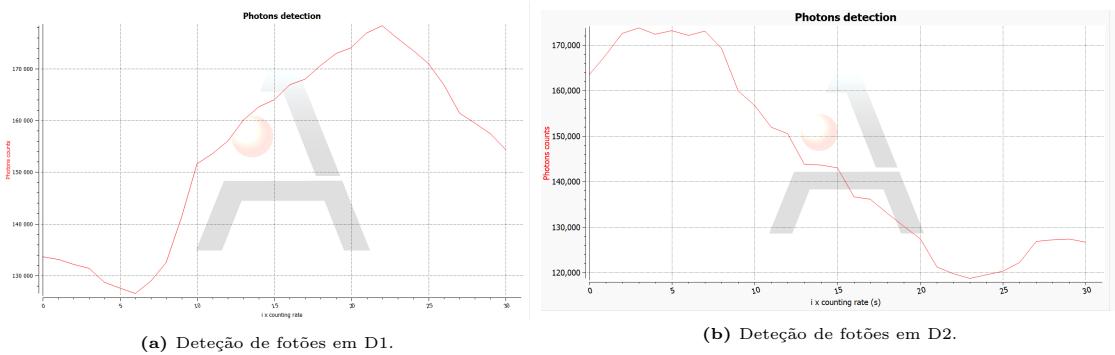


Figura 4.10: Deteção de fotões nos detetores, com 180 mV aplicados no modulador de fase do sistema de transmissão.

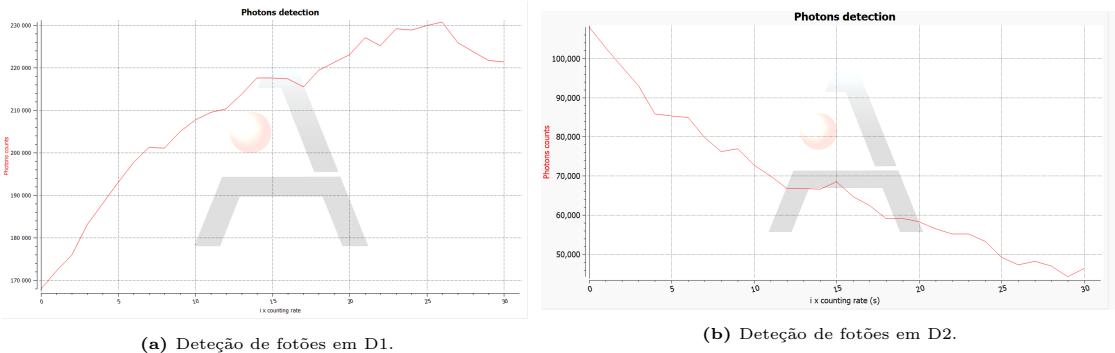


Figura 4.11: Deteção de fotões nos detetores, com 200 mV aplicados no modulador de fase do sistema de transmissão.

deteção em D2 relativamente a D1. Assim, evidencia-se a concordância de bases aleatórias de polarização [23].

Avaliemos agora a taxa de erro quântica associado ao nosso sistema de distribuição de chave quântica. A tabela 4.1 contém os parâmetros necessários para cálculo do QBER associado.

Tabela 4.1: Parâmetros experimentais para cálculo da taxa de erro quântica.

Parâmetros quânticos	Valor nominal
p_{opt}	0.01
μ	0.2 [fotões por impulso ótico]
t_{link}	6.3×10^{-3} [dB]
η	0.181
α	0.22 [dB/km]
L	10 [km]

As probabilidades de dark-counts, definidas por 3.22 e 3.23, obtemos experimentalmente a taxa de erro quântica, obtida por 2.30.

$$QBER_{005972} = 0.01 + \frac{0.0000360}{0.2 \times 0.181 \times (6.3 \cdot 10^{-3})} \approx 16.8\% \quad (4.3)$$

$$QBER_{005973} = 0.01 + \frac{0.0000041}{0.2 \times 0.181 \times (6.3 \cdot 10^{-3})} \approx 2.8\% \quad (4.4)$$

Em suma, a análise dos resultados experimentais foi condicionada por erros associados aos moduladores de fase. Não se conseguiram gerar estados de polarização que seguissem um padrão aleatório de distribuição e inclusive, nos casos em que se aplicou uma onda quadrada a variar entre [0,200] mV, surgiu uma deriva nos respetivos estados de polarização de saída, que condicionaram a obtenção de resultados teóricos que fossem validados pelos resultados práticos. Uma das opções a ser abrangida passou por aumentar as tensões fornecidas, mas o estado quântico de saída do modulador de fase do sistema de transmissão descrevia trajetórias circulares, percorrendo-as a um ritmo alto.

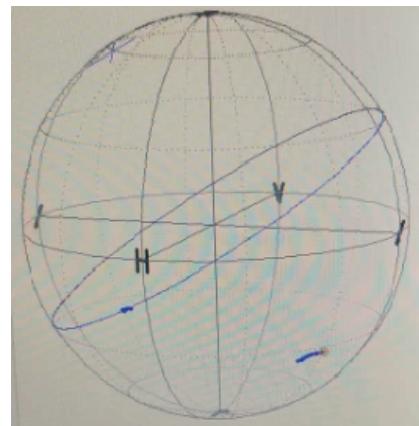


Figura 4.12: Observação de estados quânticos no polarímetro que condicionaram a obtenção de resultados válidos.

A figura 4.12 ilustra as trajetórias circulares descritas pelos estados quânticos, no polarímetro, em casos que os estados saíam da trajetória prevista, sendo por isso difícil extrair resultados válidos.

Capítulo 5

Conclusão

Neste projeto, conseguiu-se observar o efeito dos moduladores de fase em gerar estados de polarização arbitrários, proveniente da variação da tensão externa fornecida aos moduladores. Observou-se também o impacto da variação da polarização dos estados ao longo duma fibra ótica, proveniente de processos de Langevin, assim como na prática de aplicações de stress na fibra ótica que promoviam uma birrefringência local. E, finalmente, analisou-se detalhadamente a propagação do estado quântico gerado até à receção da informação e consequente correspondência entre bases de polarização, por uma análise da deteção de fotões nos dois detetores, verificando a diferença entre valores de pico por parte da contagem do número de fotões.

Assim, o QBER calculado por 2.30, é analisado no sistema, para cada um dos detetores. No detetor *Model 005972*, o QBER associado ronda os 16,8% pelo que, a probabilidade de se detetar informação errada seria elevada, devido à facilidade que o espião teria no acesso à informação. Já no detetor *Model 005973*, o QBER associado ronda os 2,8%, pelo que a informação que chega a este detetor é pouco provável que tenha sido manipulada, no canal quântico. Considerou-se, pela análise do QBER em geral, que o sistema quântico de partilha não é totalmente seguro, uma vez que apresenta, num dos detetores, um erro quântico $> 11\%$. Note-se ainda que, uma das razões prováveis do QBER obtido ter sido elevado, deve-se a imperfeições associadas aos dispositivos quânticos [21], o que é perfeitamente válido neste projeto, dado a deriva que surgia nos estados quânticos de saída.

No futuro, o principal objetivo passa por observar este processo de transmissão de informação, tentando efetivamente encriptar informação no estado de polarização de fotões únicos, observando -se até que distância máxima, se consegue partilhar informação, de forma a que o nosso sistema quântico implementado seja totalmente seguro, tendo por base, por exemplo, o protocolo quântico abordado neste projeto.

Em suma, caracterizou-se de forma detalhada todo o modelo e processo de distribuição de chave quântica, num formato teórico e numérico, analisando-se como ocorria a distribuição de chave quântica. Todo este processo criptográfico, desde gerar bits aleatórios provenientes de escolhas de bases arbitrárias à deteção dos mesmos, à avaliação do QBER, deu-me uma melhor compreensão de todo este processo complexo, sendo sistemas baseados em QKD uma tecnologia que soma passos para a segurança e privacidade dos sistemas de comunicação.

Bibliografia

- [1] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, Zhiqiang Yuan, "Practical challenges in quantum key distribution", Quantum Information, November 2016.
- [2] Su, HY. "Simple analysis of security of the BB84 quantum key distribution protocol", Quantum Inf Process 19, 169 (2020).
- [3] Prof. Dr. Raúl Alcaraz Martínez, "Information Theory, Probability and Statistics", Entropy (ISSN 1099-4300), Basel, April 2022.
- [4] Charles H.Bennett, Gilles Brassard, "Quantum Cryptography: Public key distribution and coin tossing", International Conference on Computers, Systems Signal Processing, December 10-12, 1984.
- [5] Charles H.Bennett, Gilles Brassard, "The dawn of a new era for quantum cryptography: The experimental prototype is working!", 29 October 1989.
- [6] A. Ruiz-Alba, D. Calvo, V. Garcia-Muñoz, A. Martinez, W. Amaya, J.G. Rozo, J. Mora, J. Capmany, "Practical Quantum Key Distribution based on the BB84 protocol", Instituto de Telecomunicaciones y Aplicaciones Multimedia, Universitat Politècnica de València, ISSN 1889-8297, 2010.
- [7] Mark Fox, "Quantum Optics: An Introduction", Oxford Master in Series in Atomic, Optical and Laser Physics", Oxford University Press Inc., 2006.
- [8] A.Duplinsky, V.Ustimchik, A.Kanapin, V.Kurochkin,Y.Kurochkin, "Low Loss QKD optical scheme for fastpolarization encoding", Optics Express 25(23), 28886(2017).
- [9] A.Duplinsky,V.Ustimchik,A.Kanapin, Y.Kurochkin , "Fastpolarization QKD scheme based on LiNbO₃ phase modulators", SPIE 28(2016).
- [10] Álvaro J. Almeida, Daniel L. Macedo, Nuno A. Silva, Nelson J. Muga, Paulo S. André, Armando N. Pinto, "Quantum Communication Using Polarization-Encoded Photons in Optical Fibers", Proc Conf. on Telecommunications - ConfTele, Castelo Branco, Portugal, Vol. 1, pp. 205 - 208, May, 2013.
- [11] Ahmed I. Khaleel, Shelan Kh. Tawfeeq, "Real Time Quantum Bit Error Rate Performance Test for a Quantum Cryptography System Based on BB84 protocol", Iraqi J. Laser, Part A, Vol. 8, pp. 29-35 (2009).
- [12] Frédéric Du-Burck , Karim Manamanni, Tatiana Steshchenko, Amine Chaouche Ramdane, and Vincent Roncin, "Effects of Polarization Modulation Induced by Electro-Optic Modulators in Fiber-Based Setups", IEEE Photonics Technology Letters, VOL. 34, NO. 3, February 1, 2022.
- [13] Nelson J. Muga, Armando Nolasco Pinto, Mário F. S. Ferreira, and José R. Ferreira da Rocha, "UniformPolarization Scattering With Fiber-Coiled-BasedPolarization Controllers", IEEE, Journal of LightwaveTechnology, Vol. 24, no. 11, Novembro 2006.
- [14] P. Grüning et al., "All-fiber ring-cavity for frequency stability transfer at 1.55 μm ", Appl. Opt., vol. 58, no. 6, pp. 1502–1507, 2019.
- [15] E. Sarbazi, M. Safari, H. Haas, "The impact of long dead time on the photo count distribution of SPAD receivers", Dec. 2018.
- [16] G. Ribordy, N. Gisin, O. Guinnard, D. Stucki, M. Wegmuller, H. Zbinden, "Pho-ton counting at telecom wavelengths with commercial InGaAs/InP avalanche photo-diodes: current performance", Journal of Modern Optics, vol. 51, pp. 1381–1398, Jan.2004.

- [17] Dennis Goldstein, "Polarized Light", Second Edition, Revised and Expanded, Air Force Research Laboratory, Eglin Ar Force Base, Florida, U.S.A, 2003.
- [18] P.S.André, J.L.Pinto, "Birrenfringência e Dispersão Devido aos Modos de Polarização em Fibras Óticas", Instituto de Telecomunicações - Polo de Aveiro e Departamento de Física, Revista do DETUA, Vol.3, Nº5, Janeiro 2002.
- [19] Govind P. Agrawal, "Nonlinear Fiber Optics Fifth Edition", ELSEVIER, 2013.
- [20] Nelson de Jesus Cordeiro Muga, "Efeitos da Polarização em Sistemas de Comunicação por Fibras Óticas", Universidade de Aveiro, Departamento de Física, 2011.
- [21] T. Wanner, B. S. Marks, C. R. Menyuk, J. Zweck, "Polarization decorrelation in optical fibers with randomly varying elliptical birefringence", OPTICS LETTERS , Vol. 28, No. 19 , October 1, 2003.
- [22] N.Sasirekha, M.Hemalatha, "Quantum Cryptography using Quantum Key Distribution and its Applications", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.
- [23] M. Jofre, A. Gardelein, G. Anzolin, G. Molina-Terriza, J.P. Torres, M. W. Mitchell, V. Pruneri, "100 MHz amplitudeand polarization modulated optical source for free-spacequantum key distribution at 850 nm,"Journal of Lightwave Technology 28(17), 2572–2578 (2010).