Universidade de Aveiro Departamento de Electrónica,
2022 Telecomunicações e Informática

**Mariana
Ferreira Ramos**

Sistemas de Comunicação Quânticos Baseados em Qubits Codificados na Polarização

Quantum Communication Systems Based on Polarization Encoded Qubits

Universidade de Aveiro Departamento de Electrónica,
2022 Telecomunicações e Informática

Mariana
Ferreira Ramos

Sistemas de Comunicação Quânticos Baseados em Qubits Codificados na Polarização

Quantum Communication Systems Based on Polarization Encoded Qubits

Tese apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Engenharia Electrotécnica, realizada sob a orientação científica do Prof. Doutor Armando Nolasco Pinto, Professor Associado com Agregação do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro e coorientação do Doutor Nuno Alexandre Peixoto Silva, Investigador no Instituto de Telecomunicações, Aveiro, e do Prof. Doutor Paulo Alexandre Carreira Mateus, Professor Catedrático do Departamento de Matemática do Instituto Superior Técnico, Lisboa.

Este trabalho foi financiado pela Fundação para a Ciência e a Tecnologia (FCT) e pelo Ministério da Educação e Ciência (MEC) por fundos nacionais através do projecto Quantum-Mining com referência POCI-01-0145-FEDER-031826, do projeto UIDB/50008/2020-UIDP/50008/2020 (ação QUESTS), e também pela bolsa de doutoramento com a referência SFRH/BD/145670/2019 atribuída pela Fundação para a Ciência e a Tecnologia (FCT) através do orçamento de estado e pela União europeia através do Fundo Social europeu (FSE) segundo o Programa Operacional Regional do Centro.

REPÚBLICA PORTUGUESA | CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

FCT Fundação para a Ciência e a Tecnologia

CENTRO 2020

o júri / the jury

presidente / president

Doutor Vasco Afonso da Silva Branco
Professor Catedrático da Universidade de Aveiro (por delegação da Reitoria da Universidade de Aveiro)

vogais / examiners committee

Doutor Paulo Sérgio de Brito André
Professor CatedrÃ¡tico, Universidade de Lisboa

Doutor Luís Manuel Dias Coelho Soares Barbosa
Professor Catedrático da Universidade do Minho

Doutor Armando Humberto Moreira Nolasco Pinto
Professor Associado com Agregação da Universidade de Aveiro (Orientador)

Doutora Maria Helena Almeida Vieira Alberto
Professora Associada, Universidade de Coimbra

Doutora Pétia Georgieva Georgieva
Professora Associada, Universidade de Aveiro

agradecimentos

Gostaria de agradecer aos meus orientadores por me terem guiado ao longo deste trabalho de investigação para que os objetivos traçados fossem atingidos com a qualidade que é exigida.
Como um trabalho destas dimensões nunca é exequível, unicamente, por uma só pessoa, agradeço em particular ao Doutor Nuno Silva pelo conhecimento, motivação e paciência sempre transmitidos e demonstrados ao longo deste percurso hérculeo. O meu, também, profundo agradecimento ao Doutor Nelson Muga o qual, não obstante não ter integrado a equipa de orientação deste doutoramento, teve um papel importante na concretização da investigação levada a cabo.
Agradeço, de igual modo, ao meu colega de doutoramento Luis Almeida pela partilha de conhecimento e incansável paciência, o que me possibilitou atingir objetivos de trabalho laboratorial que seriam tremendamente mais difíceis sem a sua ajuda.
Agradeço ainda ao Instituto de Telecomunicações e à Universidade de Aveiro por me terem acolhido durante este percurso e me terem possibilitado as melhores condições para levar a cabo este trabalho sem que nada me faltasse.
Por último, mas não menos importante, gostaria de agradecer aos meus pais, à minha irmã e aos meus avós Lea, Nocas, Maria Augusta e Zé, não só pelo apoio financeiro, mas também porque considero que foram e são o principal suporte para as minhas decisões relativamente ao caminho a seguir. Considero este trabalho de doutoramento o abrir duma porta para um estilo de vida, e a chave desta porta foi-me dada por eles com apoio incondicional.

palavras-chave

Comunicações Quânticas, Criptografia Quântica, Distribuição de Chaves Quânticas, Variáveis Discretas, Codificação na Polarização, Deriva da Polarização, Algoritmos Quânticos, Diversidade de Polarizaçã0

resumo

Estamos perante a segunda revolução quântica, a qual começou no início do século 21 trazendo avanços significativos na ciência, na indústria e na sociedade baseados nos avanços da teoria da informação. A emergência eminente de um computador quântico tem despoletado preocupaçẽs relativamente à segurança dos atuais sistemas de criptografia pública clássica. Um tópico importante no campo da investigação de informação quântica diz respeito à forma de distribuição de chaves criptográficas de forma a garantir comunicações seguras entre partes distantes. Os sistemas de distribuição de chaves quânticas estão já num estágio comercial, o que tem atraído investimento de empresas e governos para a investigação nas tecnologias de informação quântica. Contudo, existe ainda muita investigação a ser feita neste campo, especialmente no que diz respeito a elevadas taxas de transmissão, distância atingida, e obviamente o custo duma implentação prática. Neste trabalho de doutoramento, começamos por implementar experimentalmente um sistema de comunicações quânticas que usa variáveis discretas com codificação na polarização, o que nos permite identificar os problemas a serem resolvidos de forma a tornar possível a implementação prática de protocolos de distribuição de chave quântica. Desta forma, propomos um método heurístico não intrusivo para compensar automaticamente a deriva aleatória de polarização em canais padrão de fibra ótica devido a efeitos de birrefringência, e que induzem erros durante a transmissão de Qubits. A compensação da deriva de polarização induzida pelo canal quântico é fundamental para permitir a implementação prática generalizada da transmissão de fotões únicos com codificação na polarização nas redes atuais de fibra ótica. Neste trabalho de doutoramento propomos ainda e validamos através de simulações numéricas um novo sistema de DV-QKD baseado na polarização que combina o uso de moduladores de fase para gerar quatro estados de polarização e mudança de base com um esquema de deteção coerente. Este sistema permite a implementação de sistemas de DV-QKD usandi unicamente equipamento clássico, o que garante um custo reduzido da implementação de sistemas Quantum Key Distribution (QKD) baseados em fotões únicos codificados na polarização e ao mesmo tempo um aumento da taxa de transmissão. Os nossos resultados abrem a porta a sistemas de transmissão de qubits a débitos elevados aquando da sua implementaçao nas redes instaladas de fibra ótica. Reportamos transmisões continuas de qubits mesmo em ambientes sujeitos a elevada deriva da polarização, sem a necessidade de consumir largura de banda extra com uma taxa de erro quântico máxima de 2%.

keywords

Quantum Communications, Quantum Cryptography, Quantum Key Distribution, Discrete-variables, Polarization Encoding, Polarization Drift, Quantum Algorithms, Polarization Diversity

abstract

We are now facing a second quantum revolution, that started in the early 21st century, bringing significant technological advances to science, industry and society based on advances on quantum information. The eminent emergence of a quantum computer has boosted concerns about the security of current classical public-key cryptography systems. One important topic in the research field of quantum information is the way we distribute keys in order to allow secure communication between distant parties. QKD systems are already in a pre-commercial stage attracting companies and government heavy investment in researching for quantum information technologies. However, there still are a lot of research to be done in this field, specially regarding high rate transmission, achievable distance reach, and obviously the practical implementation cost. In this thesis, we start by experimentally implement a polarization-encoded discrete variables based quantum communication system which allowed us to identify issues that must be solved in order to make it suitable for QKD protocols practical implementation. In this way, we propose a non-intrusive heuristic method to automatically compensate polarization random drift in standard optical-fiber channels due birefringence effects, and that induces errors during qubit transmission. The compensation of polarization drifts induced by the quantum channel is fundamental to enable the deployment of polarization encoded single-photons transmission over the current optical fiber networks. Furthermore, in this thesis we also propose and validated though numerical simulations a novel polarization-based DV-QKD system that combines the use of phase-modulators for state of polarization (SOP) generation and basis switching with a polarization diversity coherent detection scheme. This enables a full implementation of DV-QKD systems using only classical hardware, which low the cost of QKD systems based on polarization encoded single-photons at the same time that increases the transmission rate. Our results open the door to very high baud-rate polarization qubits transmission in access and metro networks. We report continuous qubit transmission, even in environments subjected to high polarization drift, without consuming extra-bandwidth with a maximum Quantum Bit Error Rate (QBER) of 2%.

Contents

List of Figures

List of Acronyms

QKD Quantum Key Distribution

QOKD Quantum oblivious Key Distribution

FPGA field programmable gate array

QBER Quantum Bit Error Rate

VHDL Very High Speed Integrated Circuits Hardware Description Language

DAC Digital to Analogue Converter

AES advanced encryption standard

3DES data encryption standard

QTx quantum transmitter

QRx quantum receiver

PBA polarization basis alignment

VOA Variable Optical Attenuator

SOP state of polarization

PMD polarization mode dispersion

PM phase-modulator

PC polarization controller

PBS polarization beam splitter

MZM mach-zehnder modulator

EPC electronic polarization controller

RSA Rivest-Shamir-Adleman

QC Quantum Communications

DV-QKD Discrete-variables quantum key distribution

CV-QKD Continuous-variables quantum key distribution

WDM wavelength-division multiplexer

TTL transistor-transistor logic

DV-QC discrete variables quantum communication

HWP half-wave plate

QWP quarter-wave plate

BS beam-splitter

TDM-PBA time-division multiplexing polarization basis alignment

TDM time-division multiplexing

WDM-PBA wavelength-division multiplexing polarization basis alignment

WDM wavelength-division multiplexing

TIA trans-impendance amplifier

PDL polarization dispersion loss

Chapter 1

Introduction

In this chapter, we start by introducing the research topic contextualization of this thesis followed by the motivation, problem definition, objectives, main contributions, and finish with the scientific output.

This chapter is organized in six sections. In section 1.1 we present the background of the developed work within the field of quantum information, and also the motivation to develop the presented work in the scope of this PhD thesis. Section 1.2 is devoted to the problem definition followed by the presented motivation. In section 1.3, we present the main objectives of this thesis. The main contributions and the scientific output resulted from this thesis are presented in section 1.4 and in section 1.5, respectively. Finally, in section 1.6 we present the outline of this thesis.

1.1 Background and Motivation

A practical quantum computer has been becoming a reality, which has boosted concerns about the security of current classical public-key cryptography systems. In 1994, Peter Shor proposed a quantum algorithm for integer factorization which runs in polynomial time in a quantum computer, instead of exponential time using classical computation techniques [1]. When applied to public-key cryptography systems, Shor's algorithm will have the ability to break the Rivest-Shamir-Adleman (RSA) cryptosystem and signature schemes used for data confidentiality [2]. In the presence of a quantum computer, a 4096-bit RSA would be broken in a matter of hours in contrast to the best current classical computers that would require billions of years [3]. In this way, the security of today's classical network would be compromised and secrets would be revealed. Later, in 1996, Lov Grover discovered that the searching problem can be solved by a quantum computer performing brute-force inversions of one-way functions with a speed quadratic higher than classical brute-force [4]. This severely compromises the privacy of the digital data store in databases, including our medical and genome data, and the governance citizens data. In response, some post-quantum cryptography schemes have been proposed as an alternative to the public-key cryptography method used nowadays, such as the post-quantum RSA, in which its security is based on other hard and complex computational problems [1]. However, the post-quantum RSA imposes a processing cost many orders of magnitude above the pre-quantum RSA, which will compromises the efficiency of encryption and decryption tasks [5]. Moreover, post-quantum RSA is a recent research topic, and in this way the related problems present more immaturity when comparing with the factorization

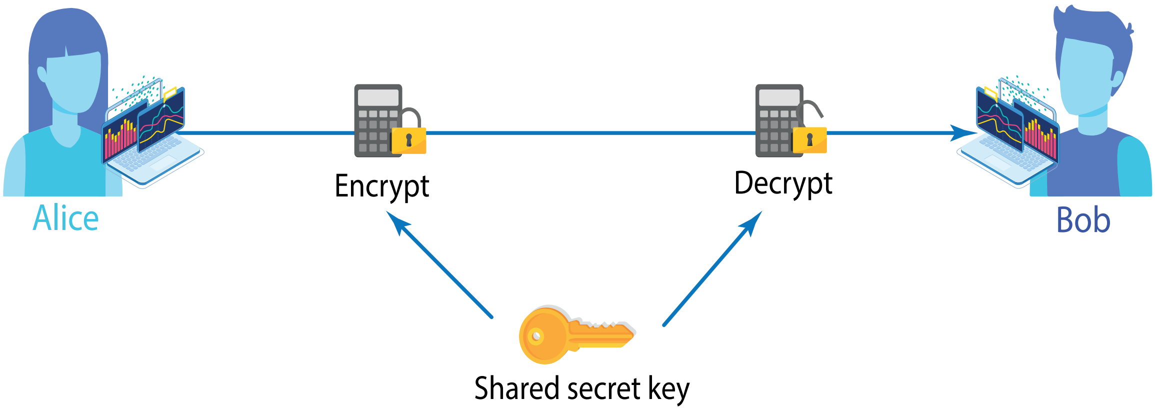


Figure 1.1: Schematic of symmetric key encryption, where one secret key is used to both encrypt and decrypt data. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.

problem that have been being study for decades.

In one hand, the information in classical communication systems can be copied without any disturbance on the system, on the other hand, in quantum communication the information cannot be copied without disturbing the system based on the no-cloning theorem [6]. An identical copy of an unknown quantum state is impossible to be created following the no-cloning theorem. In this way, considering a quantum system free of imperfections whenever the receiver randomly chooses the same basis as the transmitter prepared a quantum state, he obtains a correct measurement [7]. Otherwise, the receiver obtains a random measurement. Note that, besides QKD is recognized as providing theoretic secured information, when implemented in real devices those security can be compromised by the imperfections of real devices.

In [8], Bennet and Bassard reported that using quantum cryptography, the information can be encoded in the transmitter and sent to a receiver in such a way that it is able to decode the information if no eavesdropper is present. In the case of any attempt of an eavesdropper to intercept the information, its presence is detected, and no information is revealed since the transmitted key is discarded. In this way, quantum cryptography schemes are a solution that can provides perfect security of data transmission, even against an eavesdropper with unlimited computation power [9–11]. The BB84 protocol allows the secure key distribution between two distant parties. Those keys supply upper-lower protocols that use symmetric keys, which enables distant parties encrypt and decrypt the a message using the same key as shown in Figure 1.2. Current QKD systems use those prepare and measure protocols, where the transmitter generates the quantum state, which is transmitted through the quantum channel, and measure by a distance receiver. Moreover, the proposal of the BB84 protocol relies on polarization to encode information in single-photons in four different states of polarization using two non-orthogonal basis [12]. Since then, a lot of schemes for quantum key distribution using polarization encoding have been proposed.

Nowadays, quantum cryptography systems can be implemented following two fundamental approaches, depending on the coding basis used to encode the information [13, 14]. In both approaches, the ability of produce, manipulate, transmit and measure quantum signals is required. In this PhD work, we aim to implement the QKD protocol in a standard telecommunication channel, which demands that the quantum signals are always photons and the physical communication channel can be optical fiber. In DV-QKD, the information can be encoded in various degree-of-freedom of individual photons, such as the polarization, which lead to a discrete measurement outcome [15–18]. Alternatively, Continuous-variables quantum key distribution (CV-QKD) systems rely on multi-photon quantum states of light and encode the bits on observables with a continuous spectrum, such as the phase and amplitude of coherent states [14, 15]. A fundamental difference between those two families of protocols lies in the detection scheme. Regarding the degree of freedom used to encode information, the number of options are varied. For instance, a few of those degrees of freedom include polarization, phase, and phase difference between consecutive pulses.

With the increasing need for jointly computing huge quantities of data, current telecommunication networks have two big issues, that have been under discussion by scientific community: security and privacy of the data when it is exchanged between multiple distrusting parties. Quantum cryptography rises as the solution to cryptography systems against attacks even against a quantum computer, since the encryption, transmission and decryption processes security are guaranteed by the laws of quantum mechanics [19]. Quantum key distribution solves the problem of symmetric key distribution, since the protocol is executed at both ends of the quantum channel generating a secret key at those ends, which is only known by the parties that are executing the protocol. The strength of this technique relies on the security assured by the laws of nature described by quantum mechanics, which does not require any computational assumption since the protocol is inherently immune to any attack independently of the eavesdropper computational power. Security can be solved using QKD to implement symmetric cryptography. This is widely accepted in scientific community, since there already are commercial solutions in the market. Furthermore, there is an European project funded with 15 million euros to implement an European test-bed for QKD. On the

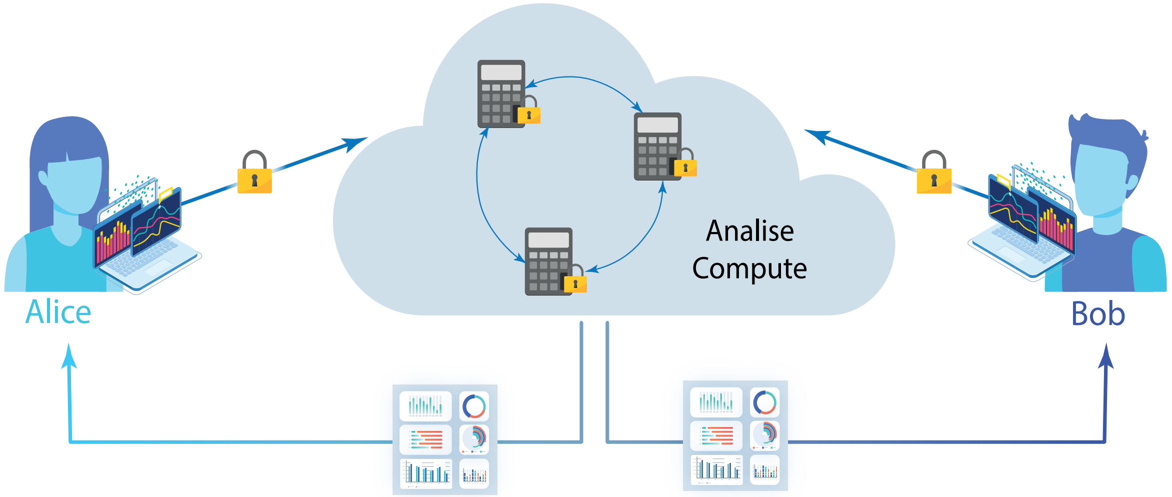


Figure 1.2: Schematic of a secure multiparty computation application, which allows remote interaction between untrusted parties assuring that a malicious entity cannot profit from inputs of others. In secure multiparty computation, each party only knows its input and the obtained output without knowing any information about other parties inputs.

other hand, privacy is a more complex problem to solve. Privacy is crucial in scenarios where multiple parties want to perform statistical analyzes using joint databases but keeping their inputs private. Secure multiparty computation has occurred as a generic tool for computing on private data, since it has a natural advantage in solving security and privacy issues in a wide range of areas such as medical, financial and government applications [20]. Oblivious transfer arises as the cryptography primitive to enable secure multiparty computation [20]. However, classical oblivious transfer is computational implemented using the RSA protocol. Nevertheless, the security of the RSA is based on computational complexity which makes it insecure against a quantum computer. Since quantum computers are becoming a reality current cryptography techniques based on RSA can be broken in real time. Besides that, oblivious transfer based on complex computational implementations is slow, which means that we can only generate a few hundred of secure oblivious transfers per second. In this way, classical oblivious transfer does not provides the required oblivious transfers for instance to obtain a single advanced encryption standard (AES) that requires 1048576 oblivious transfers in a short time [21]. In scenarios where multiple distrusted parties are connected in the same network and want to interact remotely, security, privacy and obviously speed are crucial, which makes the classical oblivious transfer not feasible for secure multiparty computation applications [21, 22]. Another approach is quantum oblivious transfer. Being based on the fundamental laws of quantum mechanics and considering the lack of long-time perfect quantum memories, quantum cryptography technologies assure present and future privacy of personal information. This still stands even considering the expected exponential growth of computational power that forthcoming quantum computers can bring to our society.

1.2 Problem Definition

We are now facing a second quantum revolution, that started in the early 21st century, bringing significant technological advances to science, industry and society. One important topic in the research field of quantum information is the way we distribute keys in order to allow secure communication between distant parties. QKD systems are already in a commercial stage attracting companies and government heavy investment in researching for quantum information technologies. However, there still are open issues to be fulfilled namely the reaching distance of QKD protocols, the transmission rate in order to transmit the maximum number of keys in short-time, and the cost of those systems. Moreover, this work is devoted to the key exchanging using polarization encoded single-photons over standard optical fiber channels, which opens an additional issue regarding the polarization stability of the optical signals. Furthermore, note that in most of the QKD systems based on a discrete-variables approach, the transmission rate is limited by the detection scheme, which is definitely an important topic on quantum information research that has our best attention in this work.

1.3 Objectives

The aim of this thesis is the development of a single-photon polarization encoding based quantum communication system capable of generating, transmitting and detecting qubits information. The work is developed under the scope of the following objectives:

1. The first goal is to study and implement in the laboratory a real-time quantum communication system based on polarization encoded single-photons.

2. Prepare the implemented system to be able to operate outside the laboratory over standard optical fibers.

3. The final goal is to analyze and optimize the DV-QKD system, regarding the reaching distance, achievable performance, and implementation cost.

1.4 Main Contributions

The main contributions this PhD work are the following:

- We have experimentally implemented a quantum communication system based on polarization encoded single-photons. The implemented system supports the generation and measurement in real-time of two sets of two states of polarization orthogonal within each set, and from two non-orthogonal mutually unbiased basis between sets [23–25]. Moreover, we also developed and implement on hardware an algorithm for temporal symbol synchronization to enable prepare-measurement quantum protocols implementation between two distant parties [26].

- Development and implementation of an algorithm to automatically compensate the polarization random drift throughout a standard optical fiber channel of a state of polarization. This algorithm can be applied in any quantum communication system, specially in a communication system that uses polarization encoded single-photons to transmit information [27].

- Later, we extend the polarization drift compensation algorithm for practical long-term quantum key distribution protocols implementation assuring polarization drift compensation for any state of polarization [28], which allows the implementation of the developed DV-QKD system over standard optical fibers.

- We also propose a novel polarization-based discrete-variables quantum key distribution system that combines the use of phase-modulators to state of polarization generation and basis switching with a polarization diversity coherent detection scheme. Moreover, a theoretical model considering system imperfections was developed and implemented in simulation to assess the feasibility of the proposed scheme in a realistic scenario. For that model we consider polarization mode dispersion over the standard optical fiber channel, the polarization dependent loss in phase modulators, a highly attenuated laser source modelled using a Mach-Zehnder to obtain single-photons, as well as the imperfections and noise contributions of the detection system [29].

1.5 Scientific Output

In the scope of this PhD work, the following publications were released:

1.5.1 Journal Papers

- M. F. Ramos, A. N. Pinto, and N. A. Silva, ”Polarization-based discrete variable-QKD via conjugated homodyne detection”, Scientific Reports, Vol. 12, No. 1, pp. 1 - 13, April, 2022.

- M. F. Ramos, N. A. Silva, N. J. Muga, and A. N. Pinto, "Full polarization random drift compensation method for quantum communications", Optics Express, Vol. 30, No. 5, pp. 6907 - 6920, February, 2022.

- N. J. Muga, M. F. Ramos, S. T. Mantey, N. A. Silva, A. N. Pinto, "FPGA-Assisted State-of-Polarization Generation for Polarization-Encoded Optical Communications", IET Optoelectronics, Vol. 14, No. 6, pp. 350 - 355, December, 2020.

- M. F. Ramos, N. A. Silva, N. J. Muga, and A. N. Pinto, "Reversal Operator to Compensate Random Drifts in Polarization-Encoded Quantum Communications", Optics Express, Vol. 28, No. 4, pp. 5035 - 5035, February, 2020.

- Mariano Lemus, Mariana F. Ramos, Preeti Yadav, Nuno A. Silva, Nelson J. Muga, André Souto, Nikola Paunkovic, Paulo Mateus, Armando N. Pinto, "Generation and Distribution of Quantum Oblivious Keys for Secure Multiparty Computation",Applied Sciences (Switzerland), Vol. 10, No. 12, pp. 4080 - 4080, June, 2020.

1.5.2 National and International Conference Papers

- S. T. Mantey, M. F. Ramos, N. A. Silva, A. N. Pinto, N. J. Muga, "Demonstration of an Algorithm for Quantum State Generation in Polarization-Encoding QKD Systems", OSA Optical Fiber Communications - OFC, San Diego, United States, March, 2022

- M. F. Ramos, N. A. Silva, N. J. Muga, A. N. Pinto, "Reference Clock Signal Distribution for Quantum Key Distribution", SBRC Workshop de Comunicação e Computação Quântica WQuantum, Uberlândia, Brazil, August, 2021.

- S. T. Mantey, M. F. Ramos, N. A. Silva, N. J. Muga, A. N. Pinto, "Algorithm for State-Of-Polarization Generation in Polarization-Encoding Quantum Key Distribution", Telecoms Conference ConfTELE, Leiria, Portugal, February, 2021

- Nelson J. Muga, Mariana Ramos, Sara Mantey, Nuno A. Silva and Armando N. Pinto, "Deterministic State-of-Polarization Generation for Polarization-Encoded Optical Communications", accepted for oral presentation in 8th edition of the SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC). Aveiro Portugal, November 2019.

- M. F. Ramos, N. A. Silva, N. J. Muga, and A. N. Pinto, "Fast Polarization Basis Alignment For Quantum Communications". In Frontiers in Optics (pp. JTu3A-53). Optical Society of America. Washington, September, 2019.

- Armando N. Pinto, Mariana F. Ramos, Andoni C. Santos, Nuno A. Silva, and Nelson J. Muga, "The Impact of Fiber Random Birefringence in Polarization-Encoded Quantum Communications", International Conference on Transparent Optical Networks ICTON. Angers, France, July, 2019.

- Armando N. Pinto, Mariana F. Ramos, Nuno A. Silva, and Nelson J. Muga, "Generation and Distribution of Oblivious Keys through Quantum Communications", 20th International Conference on Transparent Optical Networks (ICTON) (pp. 1-3). IEEE. July, 2018.

1.5.3 Awards

The following awards were also achieved:

- S. T. Mantey, M. F. Ramos, N. A. Silva, N. J. Muga, A. N. Pinto, "Algorithm for State-Of-Polarization Generation in Polarization-Encoding Quantum Key Distribution", presented at the 2021 Telecoms Conference (ConfTELE), the 12th conference on telecommunications, held in Leiria Portugal, 11-12 February 2021., 01-02-2021. The award has been attributed for the Best Paper Award.

- M. F. Ramos, N. A. Silva, A. N. Pinto, Best PhD oral communication, "Fast and Secure Multiparty Computation Enabled by Quantum Communication Technologies" presented at Research Summit 2019, held at the University of Aveiro, Portugal, July 3-5 2019. The award has been attributed for the scientific quality and organization of the work.

1.6 Outline

This PhD thesis is divided in six chapters and it is organized as follows:

- Chapter 2 presents the experimental discrete variables quantum communication (DV-QC) system based on single photon polarization encoding implemented on the laboratory. We start presenting the state-of the art under the scope of the experimental implemented system. Moreover, we describe the system general architecture including the physical-layer, middleware layer, and the protocol-layer. The implemented system supports four states of polarization from two mutually unbiased basis, which allows the implementation of QKD and Quantum oblivious Key Distribution (QOKD) protocols based on discrete-variable encoded in polarization. All hardware and software procedures are detailled including the code implemented in field programmable gate array (FPGA)s and the software implemented in the upper-layer.

- Chapter 3 presents the method developed to compensate a single-state polarization random drift in optical fibers by mapping the estimated bit error rate on the Poincaré sphere. In this chapter we present the developed algorithm and demonstrate its impact on systems under heavy external perturbations assuming perfect and realistic receivers.

- Chapter 4 presents a novel heuristic searching method to compensate polarization random drift of the BB84 QKD states of polarization based on the QBER of only two non-orthogonal mutually unbiased states of polarization. The proposed method takes advantage of the usage of quantum frames and implements the algorithm presented in the previous chapter in a more generalized way allowing for the compensation of any state of polarization, which enables the large deployment of polarization encoded based DV-QKD systems.

- Chapter 5 presents a novel polarization-based DV-QKD system that combines the use of phase-modulators for SOP generation and basis switching with a polarization diversity coherent detection scheme. This enables a full implementation of DV-QKD systems using only telecom-grade material. In this chapter, we present the theoretical model developed to simulate the proposed system in different contexts showing the practical improvements opened by those proposal.

- Chapter 6 summarizes the main conclusions resulted from this PhD thesis and discuss on the future work that may be followed.

Chapter 2

Polarization DV-QC System

In this chapter, we describe a DV-QC system based on single photon polarization encoding. This system supports four states of polarization from two mutually unbiased bases. The developed system is upper layer protocol agnostic being able to support namely QKD and QOKD protocols.

This chapter contains 5 sections. In section 2.1, the current DV-quantum communication systems state of the art is presented. In section 2.2, the system's general architecture is detailed. In section 2.3, the transmitter is detailed, the single-photon generation, and the polarization encoding are discussed. In section 2.4, the receiver is detailed, the polarization decoding, basis selection, and parties synchronization are discussed. In section 2.5, we present the experimental results that validate the implemented experimental system. At the end of this chapter, in section 2.6, the final remarks are presented.

2.1 State of The Art

For the past decade we have been witnessing the steady technological development that leads to the deeply integration of the current globalised world, where billions of electronic devices are connected in a worldwide network [30]. Nowadays, communication networks are secured by classical cryptography based on cryptographic protocols that rely on computational complexity [31]. Two kinds of cryptography keys can be distinguished, symmetric and asymmetric. In symmetric cryptography a common secret key is shared by transmitter and receiver [32]. For instance, the transmitter encrypt the plain text with the same key that the receiver decodes it, which demands an efficient method for exchanging secret keys using public communication networks. In that process, the legitimacy of both parties can be guaranteed by authentication. Asymmetric cryptography provides pairs of keys. For instance, transmitter sends the public key to the receiver, who encodes the message with that key and send it back to the transmitter, who is able to decrypt it using a private key. Moreover, Shannon introduced the perfect secrecy and demonstrated that the one-time pad encryption is theoretically secure in message exchanging, which demands the existance of a symmetric key with the same length as the message to be encrypted [33]. Current popular symmetric algorithms include the AES and the data encryption standard (3DES). Besides symmetric cryptography is assumed to be secure, it requires a secure way for key distribution [1]. Assymetric cryptography, for instance the RSA cryptosystem, is computational costly and known insecure since they are vulnerable to attacks after some processing delay, namely "intercept now, decrypt later" attacks [34]. With the imminent emergence of quantum computers this kind of encryption techniques are deeply compromised due the high computation power of a quantum computer [30]. Since 1994, when Peter Shor proposed the polynomial-time quantum algorithm for integer factorization and later in 1996 Grover with the searching algorithm, a lot of research has been made in the field considering the existence of a quantum computer. Considering the existance of a quantum computer Shor's algorithm can break the RSA cryptosystem in a matter of hours [4]. Conventional classical encryption and authentication techniques are not proved secured, and they are vulnerable to Shor's algorithm in the presence of a quantum computer. Post-quantum cryptography is one of the approaches that can be used for encryption and authentication and it may be secured against Shor's algorithm. Besides being believed that post-quantum cryptography is good for short-term security (authentication), but it can't be for long-term security, that is the ability to prevent attacks from a quantum computer [3] [35]. On the other hand, by relying the security on the physical layer, QKD is one of the approaches to move to quantum-safe cryptography resorting to quantum physics laws, which assuming a certain level of trust on the used devices, assures secret correlations unconditionally secure between parties [36].

The exchange of quantum information dates back from 1984, when Bennet and Brassard proposed the first protocol for QKD, the "BB84" protocol [12]. The BB84 protocol is a prepare and measure protocol, which can be divided into two consecutive steps namely the quantum communication followed by classical post-processing. During the quantum communication, the transmitter (usually called Alice) prepares instances of random classical information into encoded orthogonal quantum states (bit 0 and 1 correspond to orthogonal states from the same basis), and send them through a quantum channel (optical fiber or free-space), which is managed by an untrustable eavesdropper (usually called Eve). When Eve tries to steal the encoded quantum information, she measure the qubits. However, she only gets partial information when she disturbs the quantum channel due to the impossibility of clonning such information [14]. At the output of the quantum channel, the receiver (usually called Bob) measures the quantum information using a randomly chosen basis and obtains a random classical variable. After the post-processing, both Alice and Bob come up with the secret key shared by both parties, which contains the random classical variables encoded by Alice and the classical variables resulted from the Bob's measurements. BB84 was proven secure even considering an untrustable third identity with unconditional computational power by various researchers assuming honest Alice and Bob [37] [38]. More recently, huge progresses have been made in this field namely achieving high secret secure key transmission [39] [40], and over long distances [41] of the BB84 protocol. Due the redundance of using four states from two non-orthogonal bases, in 1992, Bennet proposed the B92 protocol where Alice prepares information using only two non-orthogonal states from two mutually unbiased one to the other [42]. Due to the intrissically nature of the observables, it is guaranteed that neither Bob or Eve cannot distinguish between those two states when they measure them with 100% success. The unconditional security of B92 protocol is also proved by Tamaki in the work presented in [43]. However, the performance of B92 is not as good as BB84, since Eve is able to execute a good unambiguous state discrimination measurement of quantum states prepared by transmitter when the states are non-orthogonal but linear independent. The BB84 protocol was extended to a six state protocol from three non-orthogonal bases in 1998. The use of three orthogonal bases creates a difficulty to the eavesdropper, which makes that protocol more secure than the BB84 protocol [44]. However, the drawback of that protocol is to consider the existance of a quantum memory at Bob, since he only performs the measurements after

Alice reveals the preparation bases. Within this line of work, other similar protocols were proposed. The BBM92 protocol, which is the entanglement version of BB84 [45], the E91, where identical random numbers are generated in remote places [46], the T12 protocol which has the same features as BB84 but use decay qubits [47], among others.

QKD protocols can be implemented following two fundamental approaches, depending on the coding basis used to encode information [13] [14]. In discrete variable QKD, the information can be encoded in various degree-of-freedom of individual photons, such as the polarization, which lead to a discrete measurement outcome [15] [16] [17] [18]. A lot of schemes using polarization encoded single-photons have been proposed, not only in the laboratory but also in real field trials, in both optical fiber networks and free-space [48] [49] [50]. Alternatively, it was suggested the use of continuous variable quantum communications systems, which are schemes that use multi-photon quantum states of light and encode the bits using observables with the continuous variables such as the phase and amplitude of coherent states [14] [15]. A fundamental difference between those two families of protocols lies in the detection scheme. Discrete variable QKD demands the use of single photon detectors which tend to be slow and expensive [13], whereas continuous variable QKD demands the use of homodyne detection schemes [51], which are faster and cost-effective. However their performance is limited by classical noise. Both of those schemes were successfully implemented over distances of the order of 421 km for discrete variable QKD [41] and 100 km for continuous variable QKD [52].

Due to the extreme difficult in implementing perfect single-photon sources, which emit only one photon at a time, experimental discrete variable QKD is implemented using coherent state sources heavily attenuated to an average number of 0.1 photons per pulse [13]. Despite all proposed schemes to implement discrete variable QKD, all rely on single-photon detectors to detect the arrival states, which usually set limits on the achievable performance. The most common are the Indium gallium arsenide (InGaAs) avalanche photodiodes (APDs), which operating with a reverse voltage above breakdown generates a strong electron avalanche at photon absorption [53]. Therefore, that avalanche leads to tapped electron charges in the defects that are spontaneously released triggering consecutive avalanches. This event is called after-pulse, and it is usually controlled by operating the detectors on gating mode and imposing a dead-time on the single-photon detector, which limits the detection rate of the system. In order to improve the discrete variable QKD system detection performance, superconducting nanowire single-photon detectors (SPNSPDs) was developed. In contrast to a quantum efficiency of 10% of the APDs, SPNSPDs achieve quantum effiencies in the order of 80% [14].

Discrete-variable QKD can be implemented using various photon degrees of freedom, for instance phase encoding, time-bin, and polarization encoding. In phase encoding, the information is contained in the phase difference between two modes that interfere with each other, whereas in time-bin the information is encoded in qubits that belong to different time slots. One-way discrete variable QKD experimental implementation was reported using phase encoding over a 107 km optical fiber distance in laboratory environment [54]. Another approach was reported in [55] over 20 km optical fiber, where information is encoded into differential phase shift QKD. In 2013 a time-bin based DV MDI-QKD protocol was experimentally demonstrated by several research groups [56] [57] [58]. Moreover, at zero distance and with a over repetition rate of 1 GHz, a secret key rate of 1.6 Mbps was achieved [59], while a secret key rate of 3.2×10^{-4} was reached for a 404 km ultra low-loss optical fiber [60]. In polarization encoding, the information is carried by different states of polarization [61]. The two-decoy-state QKD was demonstrated over 144 km free-space link implementing the BB84 states with polarization encoding [62]. There is always a commitment between reachable distance and secret key rate achieved. Polarization encoding gains advantage over the time-bin implementations on the transmission rate, since for every impulse a qubit of information is transmitted. Besides the unique potential for use in free space, polarization encoding holds the unequivocal advantage of being easily measured, visualized and understood. In this way, a lot of research is being done in this field, and quantum communication systems have been experimental implemented using polarization encoding [61] [63]. Several polarization modulation schemes have been proposed in order to generate stable and fast states of polarization. Polarization modulation can be achieved using N single-photon sources, one for each desired state of polarization. In [64], an experimental BB84 scheme is implemented, where the two polarization bases of that protocol consist of two PBS with a polarization controller (PC) in the diagonal basis in order to provide a rotation of $\pi/4$ from the linear basis. Following the same trend, in [65] a polarization modulation scheme using eigth laser sources is proposed to implement the decoy-state method. Those lasers are organized in four different groups, one for each state of polarization used in the BB84 protocol (horizontal, vertical, 45°, and 135°), where the two lasers in each group are responsible for generating the pulses of the signal state and the decoy state. In order to combine both the signal state and the decoy state in each group a beam-splitter (BS) and a refletor are used, and the pulses are encoded into the four polarization states and combined themselves using PBSs, half-wave plate (HWP), and BS. Alternatively, polarization modulation can be provided by optical interferometers that comprise a PBS, a phase-modulator (PM) in one of the PBS arms and a **FM!** (**FM!**) in three of the PBS arms [48] [66]. Those are intrinsically stable polarization modulation schemes, that provide up to six states of polarization. The states of polarization are chosen by applying different voltage values on the PM , and by interference of the two components of the interferometer input state. Furthermore, polarization modulation schemes based on inherently stable SAGNAC interferometers have been implemented [67] [68]. In these kind of systems, two orthogonal states enter different arms of the interferometer using a PBS, and one of them suffers a phase shift allowing to generate two diagonal and two circular states of polarization. However, the main disadvantage of those systems is regarding the polarization mode dispersion caused by the birefringence of the crystal. For that reason, some polarization modulation schemes present additional polarization maintaining fiber patch cords or faraday mirrors. The SAGNAC interferometers based polarization modulation schemes are free of polarization mode dispersion and calibration. However, its experimental implementation is hard to perfectly align and maintain the required stability. In this way, in [69], the authors propose an in-line simple LiNbO_3 phase modulators based polarization encoding scheme with a single laser source and only two single-photon detectors that compensates intrinsically compensates the polarization mode dispersion induced by the crystals with no need of additional aligment between phase-modulators at transmitter and receiver. Despite the discussed solutions, the use of EPC devices represents a viable solution, since it presents advantages such as the plug and play versatility, the low loss insertion and the low cost and small size [70] [24]. The current state of the art claims discrete variables QKD protocols have reached an average secure key rate of 54.5 kbps after 151.5 km of single-mode optical fiber channel [39]. Moreover, a maximum reachable distance of 421 km for ultra-low loss optical fibers was reported in [41].

2.2 General Architecture

In this section the quantum communication system general architecture is presented and discussed. The quantum communication system is divided on three vertical layers, and on three horizontal layers, see Figure 2.1. The vertical layers comprise the transmitter, namely Alice, the quantum communication channel, and the receiver, namely Bob. The horizontal layers comprise the physical layer, where the information is physically prepared, transmitted and measured, the middleware layer, and the protocol layer. The horizontal layers of the transmitter and receiver are latter discussed in section 2.3 and section 2.4, repectively. On the physical layer, the communication channel includes a wavelength-division multiplexing (WDM) combiner at transmitter output that combines the two individual classical reference signal and the quantum information signal, the standard single-mode optical fiber channel through which both signals are transmitted, and a WDM splitter at receiver's input that separates both combined signals. Furthermore, the communication channel also provides a classical channel on the protocol layer, which connects the transmitter and receiver by ethernet protocol communication.

2.2.1 Physical Layer

The physical layer comprises the experimental system developed to implement polarization encoded single-photons. Such experimental system provides encryption key exchange between two distant parties, namely Alice and Bob. The qubits are implemented using polarization modulation using an EPC of very narrow optical pulses at the transmitter, and they are measured at the receiver using single-photon detectors. Both parties, Alice and Bob, are connected by a standard optical fiber channel. Moreover, two signals are transmitted, the quantum polarization encoded signal and an extra classical signal used for synchronization. Those two signals are generated with different wavelengths to avoid crosstalk between them. The transmitter and receiver are detailled later in this chapter.

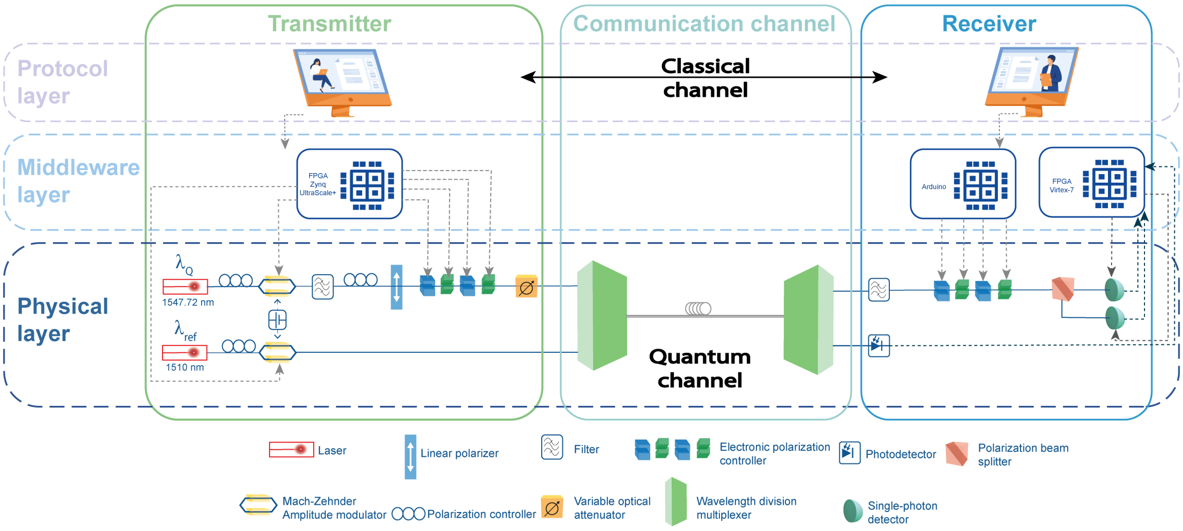


Figure 2.1: Schematic of the developed polarization encoding based quantum communication system.

2.2.2 Middleware Layer

The middleware layer enables the information flow between the physical-layer and the quantum protocol layer. At the transmitter, this layer is responsible for generating the signals to the modulation required by the MZM. The MZM modulates not only the quantum information signal, but also the additional classical signal used for symbol synchronism between parties. Furthermore, this layer also provides the electrical signals for the EPC used to polarization encode the quantum signal. Moreover, on receiver-side this layer assumes the detection procedure including symbol synchronization and the detection circuit scheme. The middleware layer consists solely of a FPGA board in both parties, and the implementation details will be individually presented later in the next sub-sections regarding the transmitter and receiver.

2.2.3 Protocol Layer

Due to the extreme versatility of the implemented quantum communication system, any quantum cryptography protocol that uses polarization encoding single-photons can be implemented on the quantum protocol layer. Once the physical layer provides the usage up to six states of polarization from the three mutually unbiased bases, the quantum protocol layer can implement from the simplest protocol using only two polarization states, for instance the B92, passing by the protocols that require four states of polarization, for instance the BB84, to the most complex protocol that requires six states of polarization. In the protocol layer, Alice and Bob are also connected through an authenticated classical channel to exchange public information needed to run the implemented protocol. In this work, we implemented a simple QBER protocol to calculate the error rate between the information transmitted by Alice and the information received by Bob. A pseudo-random sequence is encoded and sent by Alice, and measured by Bob. Note that, measurements such as no-clicks, double-clicks and measurements performed with different basis at receiver does not are taken into account on QBER calculation, being those measurements simply discarded.

2.3 DV-Quantum Transmitter

In quantum communications, the fundamental information unit is the Qubit being the information carried by it its own state. Analogous to classical communications, the qubit is a two-level quantum system, and can be described by a normalized vector. The developed system implements a qubit using polarization encoded single-photons. In this section, we detail the single-photon based transmitter system including the generation and encoding sections. Also, an additional reference signal is prepared at the transmitter for synchronization purposes. Figure 2.2 shows the transmitter architecture.

2.3.1 Physical Layer

In this sub-section, we present the physical configuration of the polarization modulation scheme at transmitter side. Since the Bob detection system operates in Geiger mode, the signals generated by Alice have a finite time-duration. To achieve that, Alice uses an amplitude modulator such as a MZM modulator driven by electrical analog signals generated by an FPGA board. As shown in Figure 2.2 the optical pulses of the quantum signal are

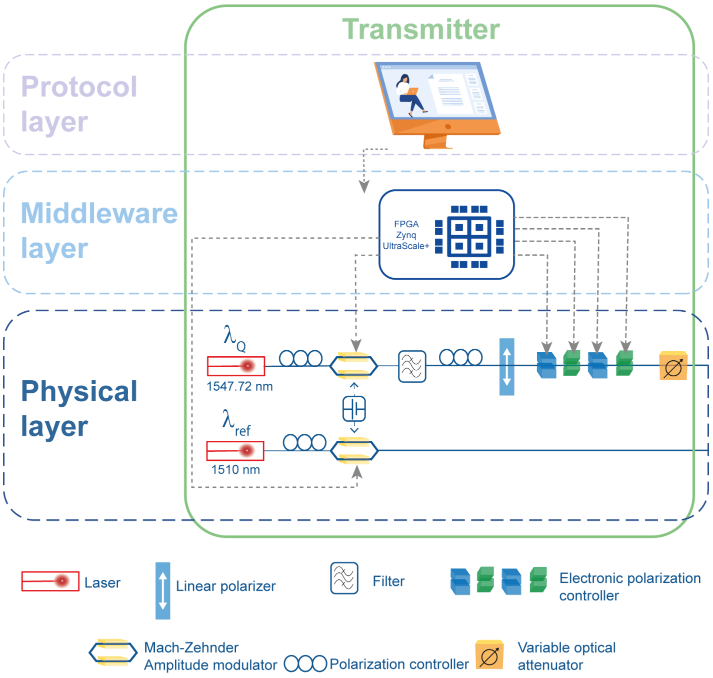


Figure 2.2: Schematic of the DV-Quantum transmitter. λ_Q and λ_{ref} are the laser sources of the quantum and the reference signal, respectively.

generated through MZM1. Moreover the classical signal used to synchronize Alice and Bob system is also a pulsed optical signal with the same repetion rate than the quantum signal, and it is generated by a second MZM2. These two optical signals are generated at different wavelengths (1547.72 and 1510 nm) to avoid signal cross-talk, and are combined in the same optical fiber via a WDM combiner, at the end of the DV-Quantum transmitter. The signals FPGA generation is later detailled in section 2.3.2, as well as the VHDL model implemented for that purpose. In this section, we begin with the photon generation section followed by the polarization encoding section. Later, we detail the topology of the middleware layer whose is responsible for controlling the physical layer, and also assure the information flow between the upper-protocol layer and the physical layer.

Photon Generation

Compared with other implementations, photons provide a good candidate to implement qubits in quantum cryptographic systems. Here, we use polarization to encode single-photon qubits. Unfortunately, the pure single-photon sources are extremely difficult to realize experimentally. Therefore, this practical implementation relies on faint laser pulses implementation in which the photons obey to a Poisson-statistics, therefore existing a small probability of having more than one photon per pulse. A very simple solution to approximate single-photon Fock states is by realizing coherent states with a very low mean photon number, μ. In this way, the probability of finding n photons on a pulse follows the Poisson statistics and can be expressed as

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}. \tag{2.1}$$

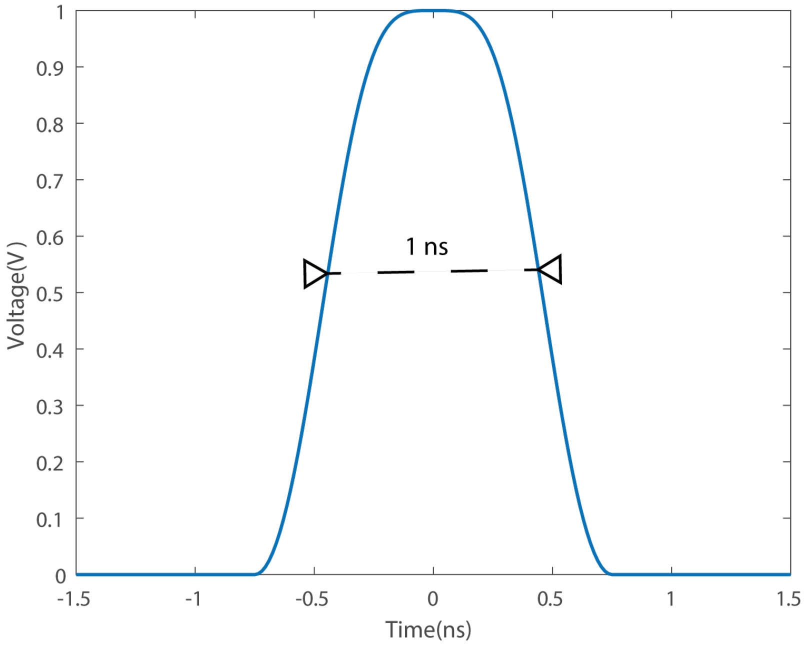


Figure 2.3: Electrical signal generated for amplitude modulation by MZM1.

Accordingly, the probability of a non-empty weak pulse is $P(n > 0, \mu) \simeq \frac{\mu}{2}$. Even though this approach guarantees a very good approximation to single-photon Fock states, when μ is a very small value the use of weak pulses results on decreasing the bit rate since a large number of pulses are empty.

In this work, the narrow laser pulses are previously generated and encoded with a higher number of photons per pulse and only then attenuated to a quantum level that assures unconditional secure communications. The photon source comprises a laser source, a PC, and a MZM as shown in Figure 2.2. The laser source emitts ligth at a wavelength of $\lambda_Q = 1547.72$ nm. The light beam is led to a PC which assures a well aligned input beam with the MZM main axis. The information carried by the optical data is obtained by amplitude modulation using the MZM1 [71]. Figure 2.3 shows the electrical square signal implemented to obtain a very narrow electrical pulse with a 1 ns half height width, and an amplitude of 1 V.

Polarization Encoding

Lets assume the orthogonal basis $\{|H\rangle, |V\rangle\}$, where the state of a qubit can be written as $a_0|H\rangle + a_1|V\rangle$. Hence, a general state of a qubit described in its polarization can be described as

$$|\psi\rangle = \cos\frac{\theta}{2}|H\rangle + \sin\frac{\theta}{2}e^{i\phi|V\rangle}. \tag{2.2}$$

A convenient representation of pure states of polarization is its mapping on the surface of Poincaré sphere, see Figure 2.4. Each pair of antipodal point of the sphere presented in Figure 2.4 corresponds to an orthogonal basis, and four of them can be expressed in relation to the third took as reference. For instance, lets define the state of a qubit defined by its normalized vector C^2 where the orthogonal basis of C^2 is $\{|H\rangle, |V\rangle\}$. In this way, the other

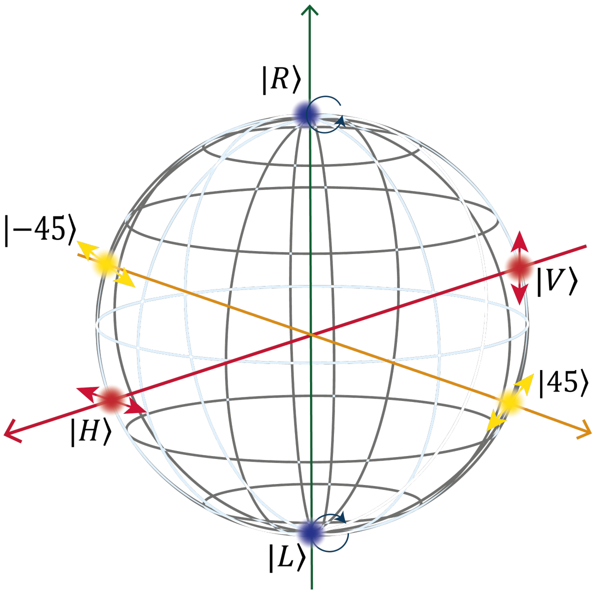


Figure 2.4: Representation on Poincaré sphere of the six states of polarization resulting from three non-orthogonal bases. $|H\rangle$ and $|V\rangle$ are orthogonal to each other and belong to the linear basis. $|45\rangle$ and $|-45\rangle$ are also orthogonal between them and belong to diagonal basis. Finally, $|R\rangle$ and $|L\rangle$ belong to the circular basis and are also orthogonal to each other.

four qubits can be expressed as

$$\begin{aligned} |45\rangle &= \frac{|H\rangle + |V\rangle}{\sqrt{2}} && (2.3)\\ |-45\rangle &= \frac{|H\rangle - |V\rangle}{\sqrt{2}} && (2.4)\\ |R\rangle &= \frac{|H\rangle + i|V\rangle}{\sqrt{2}} && (2.5)\\ |L\rangle &= \frac{|H\rangle - i|V\rangle}{\sqrt{2}}. && (2.6)\end{aligned}$$

In this work, the polarization modulation is performed using an EPC) PolariteIII$^{\text{TM}}$, which comprises four individual wave-plates with a fixed fast angle orientation and a tunable retardation phase. Each wave-plate is driven by a voltage signal, whose preparation is derailed in the next sub-section. The Mueller matrix of a general wave-plate with an orientation angle θ and a retardation δ can be represented by the following equation [23],

$$R(\theta,\delta) = \begin{bmatrix} \cos(2\theta)^2 + \cos(\delta)\sin(2\theta)^2 & -\cos(2\theta)\sin(2\theta)(\cos(\delta)-1) & -\sin(2\theta)\sin(\delta) \\ -\cos(2\theta)\sin(2\theta)(\cos(\delta)-1) & \cos(\delta)\cos(2\theta)^2 + \sin(2\theta)^2 & cos(2\theta)\sin(\delta) \\ \sin(2\theta)\sin(\delta) & -\cos(2\theta)\sin(\delta) & \cos(\delta)\end{bmatrix}. \quad (2.7)$$

Hereinafter, two these two particular cases can be represented as $R_{45}(\delta) = R(\theta = 45°, \delta)$ and $R_0(\delta) = R(\theta = 0°, \delta)$. The schematic of the rotations of each retarded in Poincaré sphere is presented in Figure 2.5-a) considering the two fast angles orientations that are presented in the referred EPC retarders. The schematic diagram of the EPC, which comprises four concatenated wave-plates, is presented in Figure 2.5-b). In the present work, we use an EPC whose the first and third fiber squeezers have 0° fast angle orientation, and the second and four fiber squeezers have a 45° fast angle orientation. The EPC requires a well defined state of polarization at the input of the first wave-plate, which is guaranteed using a fixed-linear-polarizer, LP, see Figure 2.2. The SOPs at the EPC input and output can be represented in the Stokes space as

$$\hat{s}^{\text{in}} = \begin{bmatrix} s_1^{\text{in}} \\ s_2^{\text{in}} \\ s_3^{\text{in}} \end{bmatrix} \tag{2.8}$$

and

$$\hat{s}^{\text{out}} = \begin{bmatrix} s_1^{\text{out}} \\ s_2^{\text{out}} \\ s_3^{\text{out}} \end{bmatrix} . \tag{2.9}$$

The s_i^{in} and the s_i^{out} represent the ith component of the input and output Stokes vector, respectively. The input SOP is sequentially transformed by the four wave-plates, which can be mathematically represented by $R_0(\delta_1)$, $R_{45}(\delta_2)$, $R_0(\delta_3)$, and $R_{45}(\delta_4)$. In order to obtain the electrical analog signals needed for polarization modulation, we use the Zynq UltraScale+ RFSoC ZCU111 Evaluation Kit, from Xilinx. This board provides a set of Digital to Analogue Converter (DAC) interfaces able to generate voltages with 1 V peak-to-peak (around 2.2 V), which allows to complete a full rotation on the Poincaré sphere of the polarization state. Each

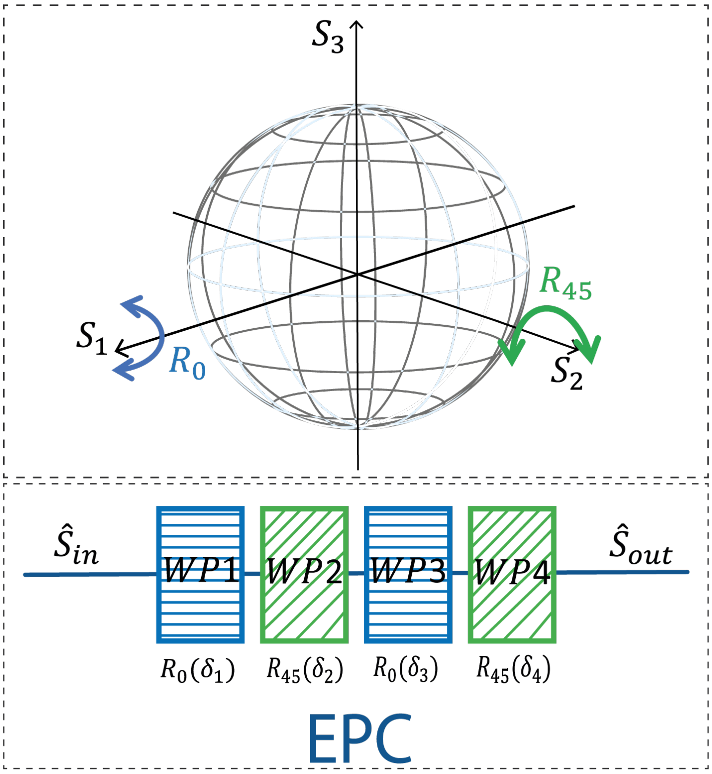


Figure 2.5: Schematic diagram of SOP rotation in Poincaré sphere induced by linear retarder, assuming the two orientations of the fast axis: $\theta = 0°$ and $\theta = 45°$.

SOP results from a set of four voltage values (one for each wave-plate), where each voltage addresses different values for the δ_1, δ_2, δ_3, and δ_4 in such a way that we obtain up to four SOPs. At the FPGA board, the electrical signals are generated at higher frequencies since the sampling rate of the DACs in the board is of the order of GHz. However, as the available EPC is only able to switch between different SOPs at a maximum frequency of 500 Hz (which is bounded by the bandwidth of the high-power RF amplifiers), we down-sample the board DACs clock in order to obtain the desire qubits repetition rate. The optical information pulses pass through the Variable Optical Attenuator (VOA)to be attenuated to 0.1 photons per pulse on average, in order to prevent the *beam splitting attacks*.

2.3.2 Middleware Layer

In this sub-section we detail the main goals of the middleware layer at transmitter side. That layer receives one signal through serial port communication from the protocol layer, which contains information about basis and bit to encode the single-photon, and also generates six analogue electrical signals. Four of those six electrical signals are generated to drive the four wave-plates of the EPC, and each of them have four different values providing four PAM-4 modulated electrical signals, which can vary 1V peak-to-peak. The other two signals are generated to drive the MZM that modulate the quantum information signal, MZM1, and the additional synchronization signal, MZM2. The methods to generate those signals are further detailed bellow.

The general topology of the transmitter implemented at the middleware layer level is presented in Appendix A.1. The transmitter contains the following components: a multi tile synchronization clock (MTS clk), a general purpose input/output (GPIOs), a RAM memory reader (RAM_rd), a signal generator, a pulse generator, and a data converter (USP_rf_data_converter).

The MTS clk produces the clocks for multi tile synchronization assuring perfect clock synchronization between the two DAC tiles, as well as all other components supplied by these clock signals. This component has two reference FPGA internal clock signals: 100 MHz and 122.8 MHz. The GPIOs provide a input/output interface for the information transmission to and from the processing system. However, these components are not fast enough for real-time changes between the processing system and the programmable logic. In this way, the RAM_rd

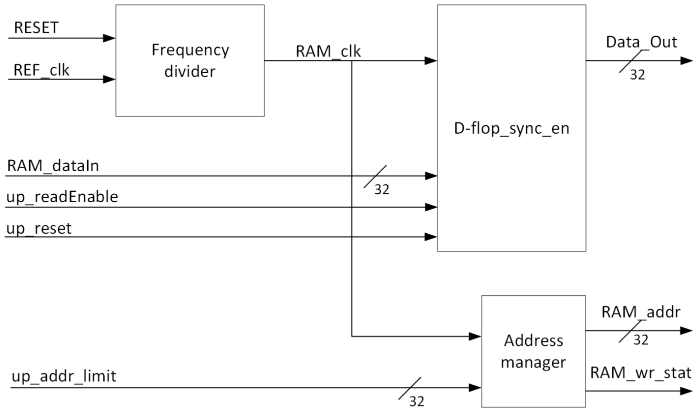


Figure 2.6: Topology of the VHDL block implemented to transmit data from the processing system to the programmable logic (RAM_rd).

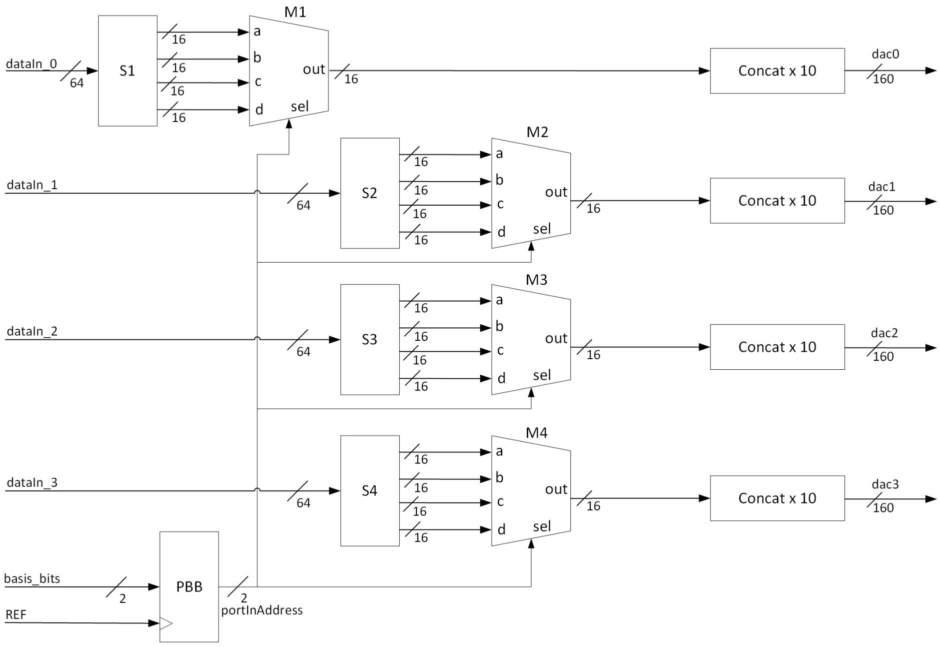


Figure 2.7: Topology of the signal generator VHDL block, implemented to generate the electrical signals to drive each wave-plate of the EPC.

allows the data reading from a configurable memory module created on programmable logic that enables real-time changes from processing system. Figure 2.6 shows the topology of the RAM_rd, which comprises a frequency divider, a synchronous D flip-flop with enable (D-flop_sync_en), and an address manager. The RAM_rd synchronously operates with a REF_clk of 393.216 MHz, which it is shared with the other components. The REF_clk is converted in a 500 Hz clock by a frequency divider, and this clock imposes the refresh memory rate. That component accepts an up_readEnabel that allows the memory reading of the addresses until the address limit defined by the user is reached, which limits the memory length. The address manager controls the memory writing status, and defines the address to be read from the BRAM memory. The D-flop_sync_en works as a synchronous register that changes the Data_out value whenever the up_readEnable is high, the up_reset is low and a rising edge of the RAM_clk is detected. The signal generator component is responsible for implementing the electrical modulation signal to apply on each wave-plate of the EPC in Figure 2.2.

The structure of the signal generator is shown in Figure 2.7. The parse basis and bits (PBB) is a synchronous component that detects a 393.216 MHz clock and divide it in order to read the basis_bit signal at 500 Hz. M1, M2, M3, and M4 are asynchronous multiplexers with a selection signal, sel, that chooses one of the four inputs to be replicated in the out port. The PBB provides the portInAddress signal for each multiplexer selecting the combination of four voltages in dac0, dac1, dac2, and dac3 to apply on the EPC at each symbol period of the 500 Hz clock. The signals dataIn_0, dataIn_1, dataIn_2, and dataIn_3 come from the RAM_rd component. Every one of those signals have four voltages encoded in 16 bit length signals each. In this way, those signals are 64 bit length and they are splitted in four different signals at the component input by S1, S2, S3, and S4. Note that the 16 bit length out multiplexer signal follows to a concat component. The concat makes ten copies of the input signal and

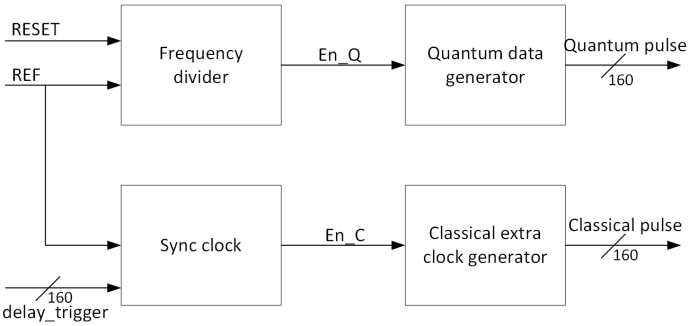


Figure 2.8: Topology of the pulse generator VHDL block, implemented to generate the electrical signals used to drive the MZMs in order to obtain the optical pulses modulated in amplitude.

concatenate those copies in order to provide a 10 samples for the USP_rf_data_converter since it reads 10 samples for each AXI clock cycle.

The pulse generator is implemented to provide the amplitude modulation on both MZM used to modulate the quantum and the additional reference classical signals.

2.3.3 Protocol Layer

In this sub-section we detail the software developed in the transmitter protocol layer in order to implement the QBER protocol proposed in [16]. Here, the main goal of this layer is to generate a pair of bases and bits, send that pair to the transmitter physical layer to provide the encoded qubits to the physical layer, and to send the bases information trough the classical channel to the receiver. Figure 2.9 shows the block diagram of the software implemented on the protocol layer at transmitter. On the transmitter side, the software is divided into two parts: one to randomly generate the bases and data bits (Program 1), and other only to transmit those information to the middleware layer through serial communication (Program 2). The former comprises four blocks: two binary sources set to generate randomly bits, a multiplexer two-to-one (MUX 2:1) to concatenate bases and data bits into the same string, and two blocks of internet protocol tunnel (IP tunnel). One of those IP tunnel sends the information to the second program that runs in the same computer, and the other sends the bases to the receiver's computer through an authenticated classical channel. The second program has an IP tunnel block, which receives the bases and data from the first program, and a serial

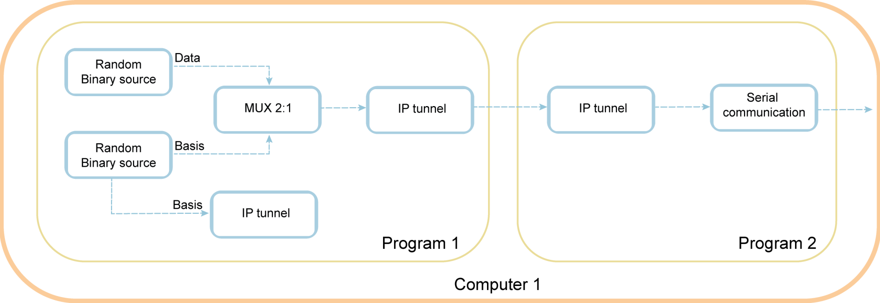


Figure 2.9: Block diagram of the software implemented on the protocol layer at transmitter.

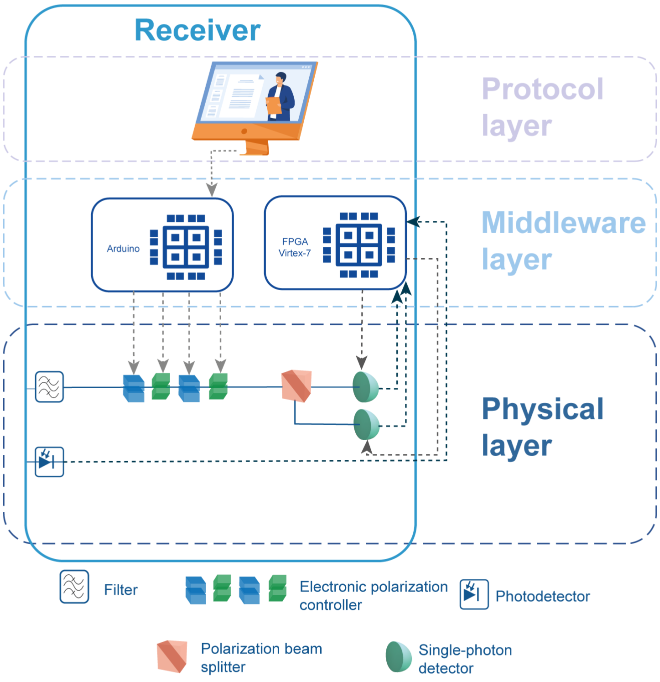


Figure 2.10: Schematic of the DV-Quantum receiver. λ_Q and λ_{ref} are the quantum and the reference signal, respectively.

communication block that formats the received data to send trough serial communication to the FPGA at the middleware layer.

2.4 DV-Quantum Receiver

On the receiver's side the role of Bob is to measure the SOPs and convert the measurements in regular bits. Figure 2.10 shows the schematic of the DV-Quantum receiver. The combined optical signals, namely the quantum signal and the reference clock signal, face a WDM splitter at the receiver's input to separate them into two different optical fiber channel paths. The reference clock signal, λ_{ref} follows directly to a photo-detector to be converted from the optical domain to the electrical domain. That signal is used for synchronization purposes which are later detailed in this section. On the other hand ,the quantum signal goes through an optical filter (XTM-50 Ultrafine, Yenista) to eliminate side-band wavelengths in order to achieve the less noise possible. The quantum filtered signal passes through receiver's EPC, which is responsible for the choice of the measurement basis. The EPC is similar to the one described in section 2.3, but here it is driven by an arduino board (Arduino Due with an AD5669 DAC module). Afterwards, the quantum signal enters in the detection loop composed by a PBS and two single-photon detectors (D1 and D2).

In this section, we begin by describing the polarization decoding scheme implemented to measure four states of polarization from two mutually unbiased non-orthogonal bases. In the final sub-section we detail the synchronization method implemented on the receiver's FPGA.

2.4.1 Physical Layer

In this sub-section, we present the physical configuration of the polarization decoding scheme at receiver side. We detail the detection scheme that provides polarization decoding including the basis selection method.

Polarization Decoding

The deployment of discrete variables based quantum cryptography protocols depends essentially on the capability of successful detect single-photons. The detection scheme relies on the choice of the basis, and on the capability of single-photon detectors effectively detects a photon. In this work, we use two single-photon detectors id210 from Id Quantique, see D1 and D2 in Figure 2.10. The single-photon detectors operate in gated-mode from an external trigger rate of 500 Hz repetition rate. That trigger comes from the FPGA board, and its generation is later detailed in sub-section 2.4.4. The single-photon detectors operate with a time gate width of $\tau_g = 2.5$ ns. Given the inherent differences between the fabrication process of each detector, they have to be set with different efficiency values. The detector D0 in Figure 2.10 has an efficiency of $\eta_0 = 20$ %, and a dark count probability of $P^0_{dc} = 5.59 \times 10^{-6}$ %. For the same gate width as the last, the detector D1 has an efficiency of $\eta_1 = 25$ %, and a dark count probability of $P^1_{dc} = 6.51 \times 10^{-6}$ %. Since the signal period is much higher than the recovering time of the avalanche photo-diode material, the chosen dead-time is not relevant for the current study. That difference was calibrated once taking into account the average counts when a perfect align state is sent to each detector. The receiver's EPC is similar to the one used at transmitter side, therefore it's operation mode can be described as on the previously section according with Figure 2.5-b). In this way, assuming an arbitrary SOP on the receiver input, after the EPC we can describe the SOP as following,

$$|\hat{s}^{\mathrm{B}}_{\mathrm{in}}\rangle = \frac{\sqrt{2}}{2}|H\rangle e^{i\delta_1} e^{i(\delta_3+\delta_4+\delta_5+\delta_6)} + \frac{\sqrt{2}}{2}|V\rangle e^{i\delta_2} e^{i(\delta_3+\delta_4+\delta_5+\delta_6)}, \tag{2.10}$$

where δ_3, δ_4, δ_5, and δ_6 corresponds to the retardation on each of the four wave-plates imposed by the voltages set to choose the basis measurement. The method to find these voltage values is later detailed in sub-section 2.4.1. When the SOP reaches the PBS, it can follows two different paths: the one into D1 direction, or the other into D2 direction. Without loss of generality, lets assume that D1 corresponds to the transmitted path, i.e. horizontal component of the light follows that path, and D2 corresponds to the reflected path, i.e. the vertical component of the light follow that path.

Basis Selecting

As mentioned above, the basis choice is performed by choosing the correct set of voltages to rotate the reference implementation axis, in order to be align with the measurement axis of the PBS. In this work, an automatic method was implemented in order to find the set of voltage values for each basis. Those method does not require additional hardware, and it only needs to be applied when the system is turned. This method calibrates the voltage for each measurement basis according with the bases used to implement the qubits at the transmitter side, and save the values to be used during the QKD protocol that can be run on the system. Moreover, the present method estimates the quantum bit error rate of the quantum signal, and works to minimize it. Likewise the EPC used in the transmitter, the receiver uses the

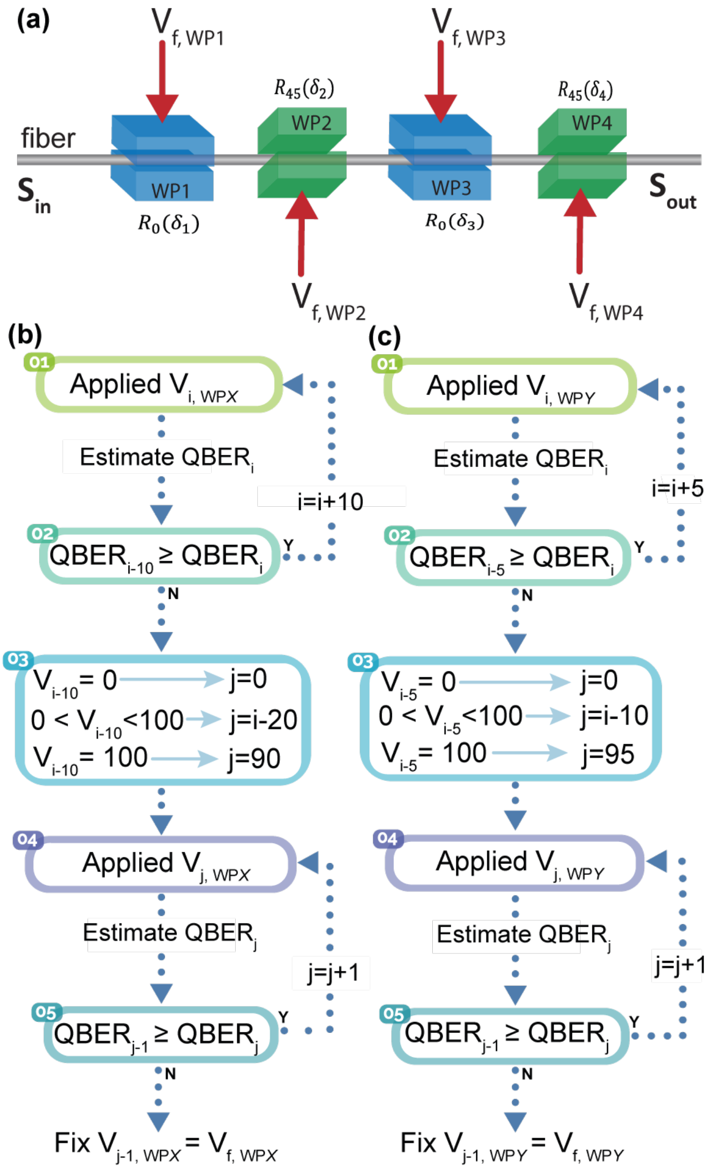


Figure 2.11: (a) Scheme of EPC wave-plates with two orientations for the fast axis: 0° and 45°. Flowchart of the proposed polarization alignment algorithm at the receiver with the steps for (b) the first and second wave-plate (X = 1 or 2), and for (c) the third and fourth wave-plates (Y = 3 or 4). The minimum voltage interval ($V_i - V_{(i-1)}$) is 0.02 V.

---

same EPC that can be represented as shown in Figure 2.11-(a). As mentioned in section 2.3, that controller is based on four fibre squeezers, where the first and third wave-plates have the fast axis oriented at 0Â°, and the second and fourth wave-plates have the fast axis oriented at 45Â°. The input SOP is sequentially transformed by the four wave-plates that are mathematically represented by different Mueller matrices, see 4.12. Figure 2.11-(b) shows the flowchart of the basis calibration method. In order to calibrate a particular basis, the transmitter sends a set of qubits whose are encoded with a polarization stands for bit 0. For instance, the qubits encoded into the horizontal SOP are transmitted to calibrate the linear basis, into the $-45°$ to calibrate the diagonal basis, and into the left circular to calibrate the circular basis. Lets assume the linear basis to be calibrated, and that the receiver previously knows that information. While the transmitter continuously sends the horizontal SOP, the receiver estimates the QBER, and starts scanning the voltage values applied on the wave-plate 1. The first scan is performed between 0 and 2 V, with a 0.2 V increment. The QBER is estimated for each value, until it starts increasing. By that time, the scanning process stops, and the minimum QBER and the corresponding voltage are saved. Depending on the voltage value (step 3 in Figure 2.11-a)), the second scan is performed within a specific range with a smaller increment of 0.02 V. During this last scan, if the QBER increases, the scanning process stops, and the minimum QBER and the respective voltage $V_{(\mathrm{f,WP1})}$ are saved. The $V_{(\mathrm{f,WP1})}$ is fixed, and the scans are repeated for WP2. For the third wave-plate, $V_{(\mathrm{f,WP1})}$ and $V_{(\mathrm{f,WP2})}$ are fixed, and then the steps of Figure 2.11-b) are performed, where the increment for the first scan in 0.1 V. Finally, $V_{(\mathrm{f,WP1})}$, $V_{(\mathrm{f,WP2})}$ and $V_{(\mathrm{f,WP3})}$ are fixed, and it performs again the steps of Figure 2.11-c) for the fourth wave-plate. At the end of these steps, all of the $V_{(\mathrm{f,WP1})}$, $V_{(\mathrm{f,WP2})}$, $V_{(\mathrm{f,WP3})}$ and $V_{(\mathrm{f,WP4})}$ values are saved, and fixed in the EPC. If the QBER is higher than 0.5%, it repeats all the steps. Otherwise, the receiver asks the transmitter to start sending the qubits encoded in the vertical state. If the QBER estimated for the vertical state continues to be lower than 0.5% the algorithm stops, otherwise it repeats the calibration process for the vertical state.

2.4.2 Middleware Layer

The middleware layer at the receiver provides the driven signals for the EPC to allow basis selection, for receiving the measurement data from single-photon detectors and apply a simple post-processing before sending the data to the upper-layer protocol, for receiving the synchronization signal from the physical layer, and for providing the already synchronized clock gate to the single-photon detectors. The generation of the signals to drive the EPC is performed using an Arduino Due combined with an AD5669 module. The reception of the result signals from single-photon detectors is performed using the digital inputs of the FPGA Virtex 7 from Xilinx. This layer outputs to the upper-layer protocol a string with the following values: 1 if the single-photon detector 1 clicks, 0 if the single-photon detector 0 clicks, 2 if both of the single-photon detectors click, and 3 if neither of the single-photon detectors click.

VHDL Model

The topology of the receiver implemented at the middleware layer level is presented in Figure 2.12. The receiver contains the following components: an utility buffer, a coincidence detector, and a general purpose input/output (GPIOs).

The utility buffer generates corresponding buffer to bring an external reference clock signal into the internal circuit. The user_clk_p is the electrical signal that results from the conversion of the λ_{ref} from the optical domain to the electrical domain by the photo-detector in Figure 2.10. The signal user_clk_p is transistor-transistor logic (TTL) 100 ns width square signal with a repetition rate of 500 Hz. Since the reference signal enters through a digital port, a digital high level is set when the voltage level of user_clk_p rises above a certain threshold defined by port characteristics, and it is set as digital low level when the same signal has a voltage bellow another threshold. Nevertheless, this architecture induces errors in the decision

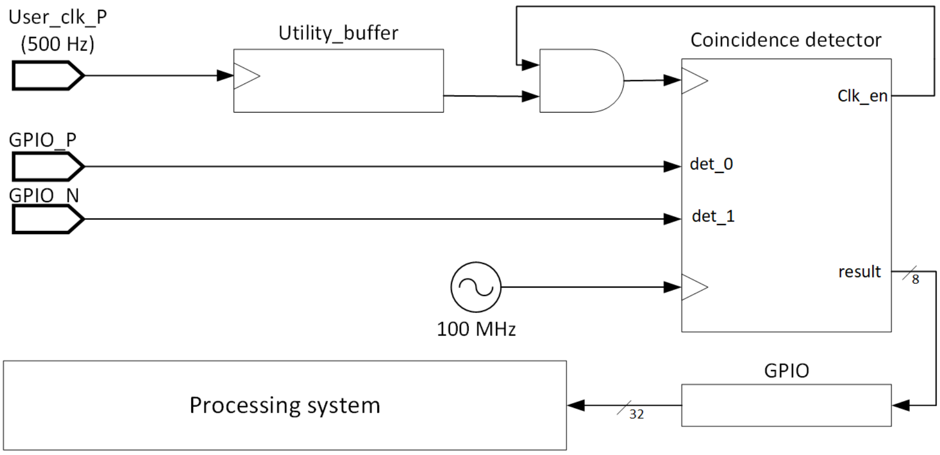


Figure 2.12: Topology of the receiver.

output resulting in a wrong detection of the clock rising edge. A simple algorithm to overcome this problem was developed in VHDL. The coincidence detector component has four input and two output signals. The first input signal is a on board FPGA 100 MHz clock, which defines for each one of the other three inputs a sampling rate of 10 ns. The signals DET_0 and DET_1 correspond to the counts output signals from each single-photon detectors. These are digital signals already, therefore not causing problems in signals reading from FPGA. The coincidence detector outputs the measurement results. That result can take the following values: 0 if the detector 0 outputs an high value for signal DET_0, 1 if the detector 1 outputs an high value for signal DET_1, 2 if both DET_0 and DET_1 have an high value, and 3 if both signals have a low value for a specific measurement time interval. The operation mode of coincidence detector is explained below in the next sub-section.

2.4.3 Protocol Layer

Similar to the transmitter's software description, on the receiver's side, the software is divided in two parts: one that received bases and data in order to estimate the QBER (Program 1); and the second program to receive the data from the middleware layer and

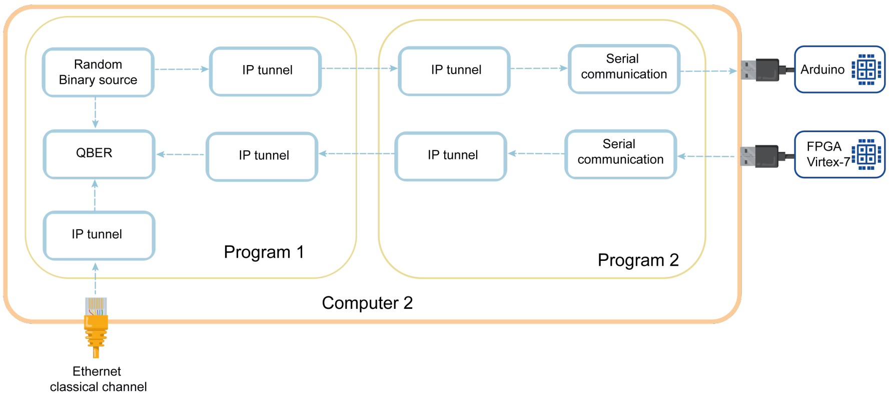


Figure 2.13: Block diagram of the software implemented on the protocol layer at receiver.

transmit it through IP tunnel to the first program (Program 2), see Figure 2.13. The former comprehends three blocks: two IP tunnels (one to receive the bases information from the authenticated classical channel, and other to receive the data from the second program), and one block responsible for estimating the QBER. The QBER estimation algorithm is implemented according with the work presented in [16].

2.4.4 Symbol Synchronization

In this sub-section, we detail the developed method for symbol synchronization implemented in the experimental DV-Quantum communication system proposed in [26]. The method relies on the combination of a WDM scheme to carry the reference clock together with the quantum data signal through the same optical fiber, with a post-processing algorithm to eliminate errors in the reference signal detection process.

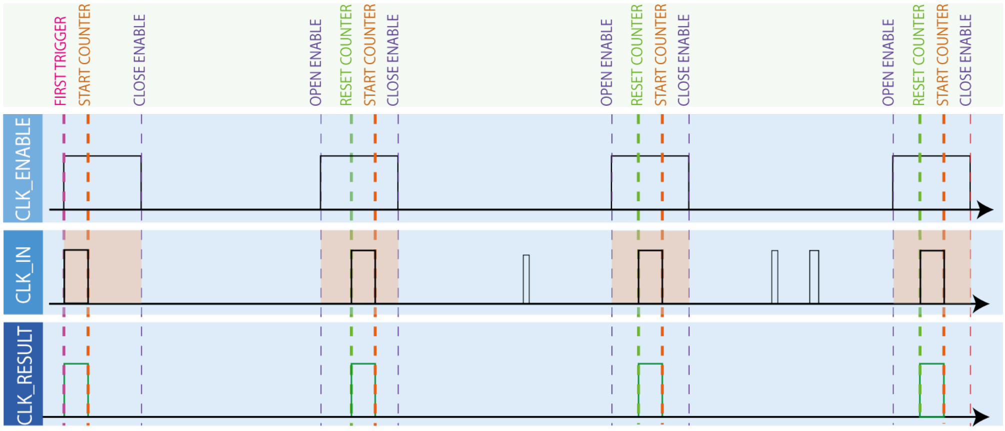


Figure 2.14: Method for reference clock signal post-processing.

Figure 2.14 summarizes the algorithm operation result. The CLK_ENABLE signal starts on an high level. As soon as the CLK_IN is triggered the signal CLK_RESULT changes to an high level, and when a CLK_IN falling edge is detected a counter starts to increment at a rate defined by the 100 MHz clock. The CLK_ENABLE changes to a low level when the counter is equal to a clock enable width value defined by the user. After this first step the counter increments until being equal to other integer value defined by the user to change the CLK_ENABLE signal again to an high level. When the CLK_IN rising edge is detected the counter is reset and the process runs again as previously described. Even if a CLK_IN rising edge is not detected at the instant it is supposed to be triggered, the circuit forces a CLK_RESULT as supposed, working similarly to a regular PLL circuit. The coincidence detector component looks into DET_0 and DET_1 only during the CLK_ENABLE high level. If during this interval one the two signals assumes the high value, the coincidence detector outputs a RESULT equal to the bit associated with each detector, 0 or 1. Otherwise, the RESULT signal assumes the value 3 if none of the two signals assume the high level, and the value 2 if both signals assume the high level during this interval.

The experimental validation of the synchronization method was performed on the implemented experimental DV-Quantum communication system. The figure of merit used to assess the system performance is the QBER, and the method for its calculation was implemented based on the work presented in [16] in the upper-software layer after receives the data from the FPGA carried by signal RESULT, see Figure 2.14-a).

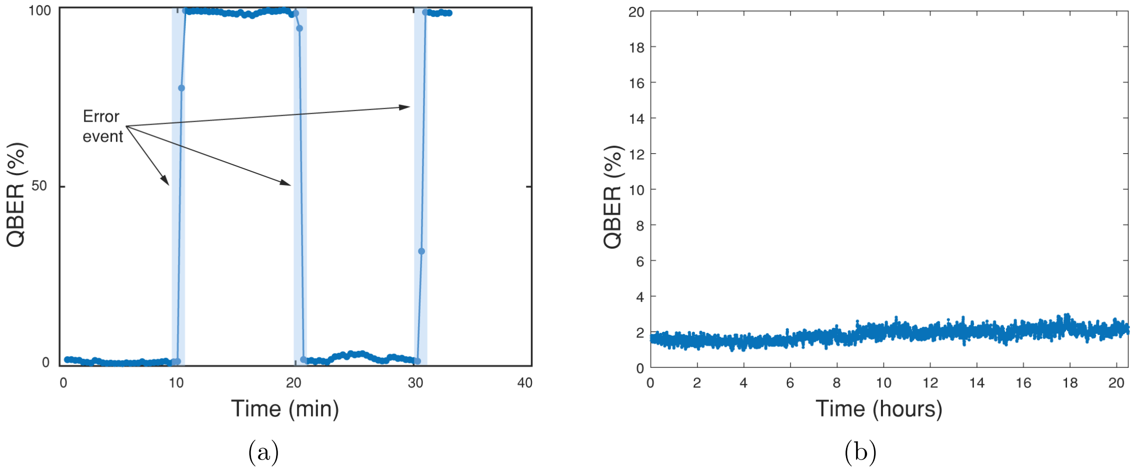


Figure 2.15: (a)-QBER measured for an alternated sequence bits without implementation of the proposed synchronization method. (b) - QBER measured for a pseudo-random sequence with the implementation of the proposed synchronization method.

Figure 2.15-a) shows the QBER measured without signal error correction algorithm for more than half of an hour. In this case, an alternated sequence of bits ”01” prepared with the two orthogonal states $|H\rangle$ and $|V\rangle$ from the same basis was transmitted. As one can see in the figure, at the beginning both stations Alice and Bob were temporally synchronized, although this synchronization is lost after only 10 minutes. This error can occurs due two phenomenons: lost of reference pulse, or detection of a pulse rising edge outside at a wrong instant, see signal CLK_IN in Figure 2.14. In this way, the QBER swaps to a value close to 100% since the sequence changes to opposite values. In Figure 2.15. (b) we present the experimental measured QBER of the same system but we implemented and tested the developed algorithm considering the previous scenario and the error events disappear. Moreover, we went a little further and tested the developed algorithm on a more complex situation considering a pseudo-random sequence longer than the previous alternated sequence. Figure 2.15. (b) shows the QBER measured using the proposed algorithm for clock signal recover for tens of hours considering a 7 qubits pseudo-random sequence to be transmitted. An average QBER = 1.8%, with a minimum $\text{QBER}_{\text{min}} = 0.94\%$ and a maximum $\text{QBER}_{\text{max}} = 3\%$ was measured during the data acquisition.

2.5 Experimental Results

In this section, we present the experimental validation of the implemented DV-QC system based on single-photons polarization encoded, which was presented in [24]. We first demonstrate that the implemented experimental quantum communication system is capable of generating the four SOPs encoded in polarization single-photons used in QKD systems. Figure 2.16 shows a lab photography of the implemented experimental system schematically presented in section 2.2. In our experimental setup, the transmitter and receiver are implemented in different tables in a back-to-back situation.

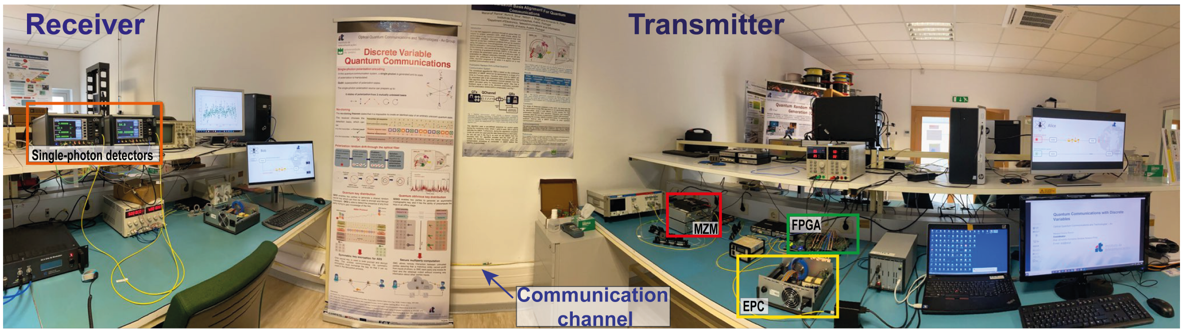


Figure 2.16: Photo of the experimental setup schematically represented in Figure 2.1.

Figure 2.17 shows the schematic diagram of the quantum physical layer system implemented in our laboratory to generate photonic quantum bits (qubits) using polarization degree of freedom of single-photons to encode information. In this section, an additional monitoring block is added in order to acquire data to demonstrate the system is capable of generating the four needed SOPs for QKD. As described in the previous sections, we use an EPC to modulate single-photons in different states of polarization. In order to obtain the four polarization states $|H\rangle$ ($|V\rangle$) for rectilinear basis corresponding to bit 0(1), and $|+45\rangle$ ($|-45\rangle$) for diagonal basis corresponding to bit 1(0), we use the 4-channel EPC from General Photonics (PolaRITE III). Since the available EPC is bounded by the bandwidth of the high-power RF

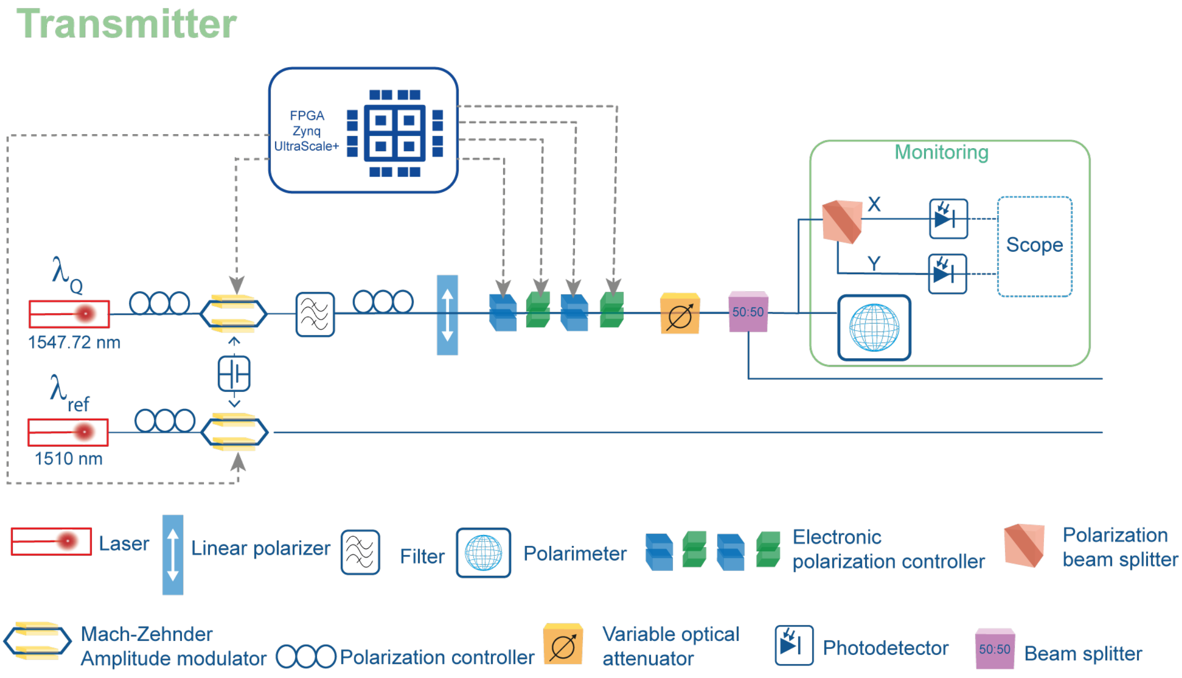


Figure 2.17: Schematic diagram of the polarization-encoding QKD system. The monitoring highlighted block show the devices used to obtain the experimental SOP generation data reported in this section. The monitoring process is performed with a PBS followed by two photo-detectors to measure the projections on the X and Y axis.

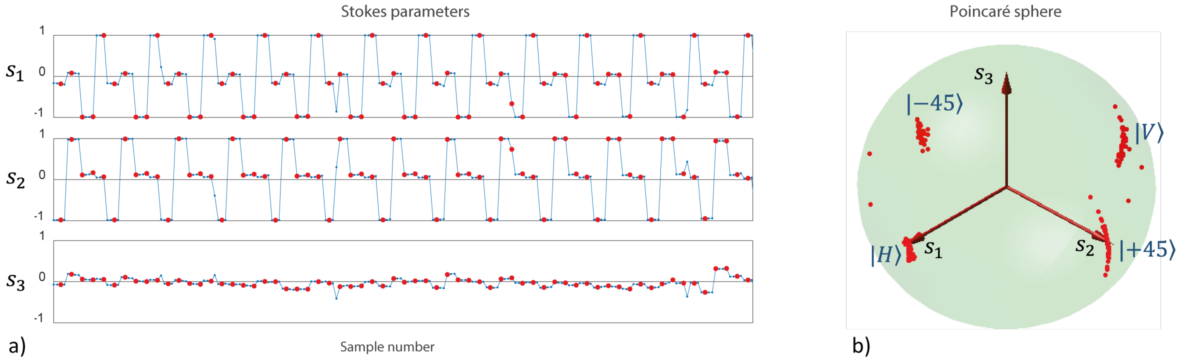


Figure 2.18: Stokes parameters of the different SOPs generated with the implemented experimental system. a) Time evolution of the three signal Stokes parameters, s_1, s_2, and s_3 (small-blue circles); b) Poincaré sphere representation of the SOPs corresponding to the signal samples represented in a) as red dots. The states $|H\rangle$ ($|V\rangle$), and $|-45\rangle$ ($|+45\rangle$) represent the SOPs of the linear basis and diagonal basis used for QKD, respectively, generated by the implemented experimental system.

amplifiers of the device to 650 Hz, we chose to operate the switch SOP frequency at 500 Hz. In order to assess the generation of different states of polarization we have implemented two monitoring systems. Then, the monitoring process was done by a polarimeter from Thorlabs (PAX5710VIS-T), able to measure the three Stokes parameters when using low frequencies, and customized optical photonic system. The customized optical photonic system comprises a polarization beam splitter (PBS) followed by two photo-detectors to measure the projections on the two orthogonal axis. This allows to indirectly verify the effectiveness for higher frequencies SOP modulation. Due to the low bandwidth of the polarimeter we have firstly generated a set of results at lower frequencies (of the order of tens of Hz). After that, we have increased the frequency up to the maximum bandwidth of the EPC (of the order of hundreds of Hz).

Figure 2.18 shows the measured Stokes parameters obtained with the experimental setup described above. The optical signal was collected in the polarimeter with a sampling rate of 200 samples/s, carrying a polarization modulation frequency of approximately 10 Hz. Figure 2.18-a) shows the evolution of the three Stokes parameters as a function of time. Notice that the parameter s_3 takes the value zero for all the selected SOPs. However, results show that this particular Stokes parameters shows a relatively high noisy level when compared with the two other parameters. When the signal symbols are represented in the Poincaré sphere, see Figure 2.18-b), one observes that the four SOP are accurately generated close to the equator. Moreover, this representation identifies the states $|V\rangle$ and —$|+45\rangle$ are the SOPs that are more affected by the noise level observed in a) for the parameter s_3. This is related with the relaxation time of the squeezing process of the EPC when the RF signal from the FPGA board is turned off.

As mentioned above, the usage of the polarimeter is limited to low frequencies. For higher frequencies we have developed a customized optical analyzer in order to check the SOP changes. The experimental results obtained with the customized optical analyzer, comprising a PBS and two photo-detectors, are represented in Figure 2.19. In this set of results, we have increased the coding rate of up to 500 qubit/s, with a sampling rate of 5kHz (i.e., 10 samples per symbol). The photo-detectors output voltages represented in the two plots (Figure 2.19 a) and b)) are proportional to the projections of the optical signal in the two orthogonal axis (Port X and Port Y) of the PBS. Since the system was configured to generate a repeated sequence of four states of polarization, $|H\rangle$, $|V\rangle$, $|+45\rangle$, and $|-45\rangle$, four different output voltages are observed at each port. Moreover, we also observe that the two curves are roughly complementary. To explain the non-exact complementary between curves, it should be pointed out that the SOPs reaching the input of the PBS, see Figure 2.17, are not the same that the ones that reach the input of the polarimeter. This occurs because these optical paths are different. If the SOPs reaching the input of the PBS are equal to the ones at the input of the polarimeter, then only three voltage levels will be observed at the photo-detectors outputs as the states $|+45\rangle$ and $|-45\rangle$ have the same projection. The two other voltage levels will be associated with the SOPs $|H\rangle$ and $|V\rangle$.

Figure 2.20 shows the QBER estimation in function of time over an acquisition time of 21 hours, and the respective histogram. The qubits are encoded in four different SOPs from two

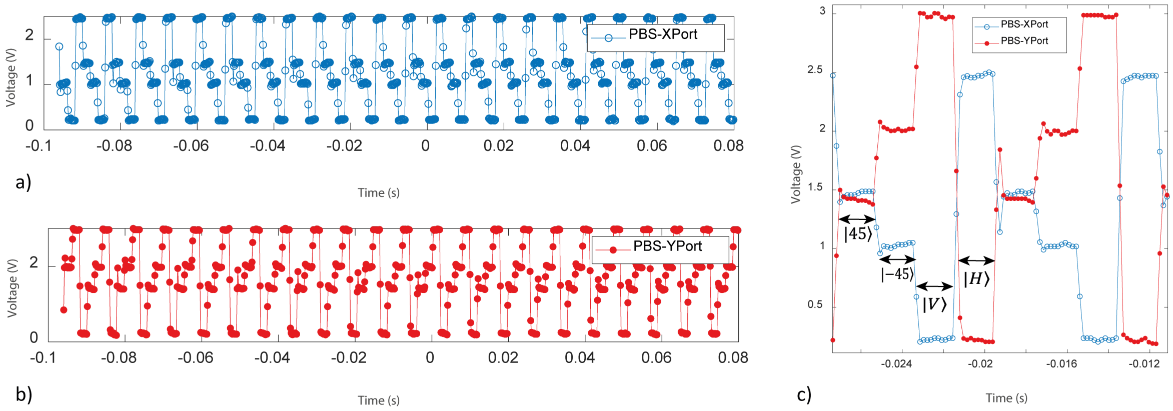


Figure 2.19: Output voltages at the two ports of the PBS. The signal is modulated at 500 qubits/s. a) and b) Voltage as a function of time for the X and Y ports of the PBS, respectively. c) Zoom in of the output voltages of the two ports, showing the sequence of the four different SOPs. Since the two ports correspond to the projection of the two orthogonal polarization, the obtained results are roughly complementary of each other.

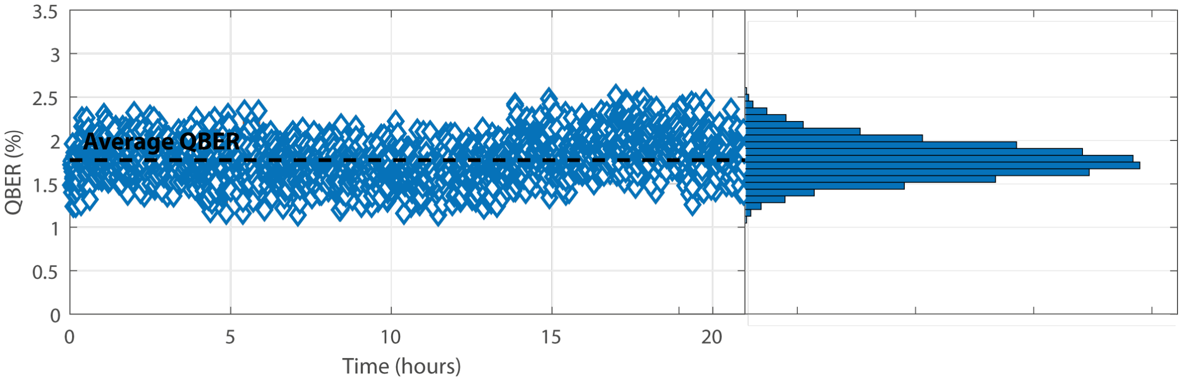


Figure 2.20: QBER estimation in function of time, for a total acquisition time of 21 hours, and the respective histogram. Average QBER=1.8%.

non-orthogonal bases, namely the $|H\rangle$, and $|V\rangle$ (linear basis), $|+45\rangle$, and $|-45\rangle$ (diagonal basis). Therefore, two pseudo-random sequences, namely PRBS-7 sequences, were generated in the protocol layer. Each SOP is encoded based on a pair of basis and bit, which results in a 7 qubit sequence. That sequence was repeatedly transmitted over the total acquisition time. Note that the non-click and double-click events are discarded in QBER calculation being only taken into account valid SOP measurements, i.e. qubits that are measured with the same basis that were encoded. In this experiment, a repetition frequency of 500 Hz was used, a quantum pulse width of 1 ns, a synchronization classical pulse with 100 ns width, a gate width of 2.5 ns, and a dead-time of $0.1\mu s$. Although in the current experiment the dead-time has no impact since it is a time interval lower than the time interval between symbols, the single-photon detectors require a default dead-time value. Different detectors efficiency of $\eta_0 = 20\%$ and $\eta_1 = 25\%$ were defined in order to have similar dark-count probability in both detectors, where η_0 represents the detector efficiency of detector that corresponds to bit 0 and η_1 represents the detector efficiency of the detector that corresponds to bit 1. A dark-count probabilities of $P_{dc}^0 = 5.59 \times 10^{-6}$ ans of $P_{dc}^1 = 6.51 \times 10^{-6}$ were achieved for detector 0 and detector 1, respectively. A maximum error rate of $\text{QBER}_{\text{max}} = 2.6\%$ and an average $\text{QBER} = 1.8\%$ were obtained.

2.6 Final Remarks

A DV-QC system using single-photons polarization encoding to transmit information was experimentally implemented in the laboratory. The implemented system suffers from a few limitations, namely a low transmission rate when compared with the current state of the art. The next improvement steps are naturally related with the increase of the transmission rate, which can be achieved by improving the encoding and decoding schemes. In the presented setup the encoding speed is limited by the bandwidth of the RF power-amplifiers of the EPC being only able to achieve the generation of 500 qubits/s. Following the same encoding scheme using EPCs to switch between different states of polarization, we can replace the current piezoelectric EPCs by acousto-optics EPCs allowing to improve the SOPs switching up to 1 MHz. However, those devices does not allow to achieve state of the art transmission rates. On the other hand, the usage of phase modulators to change the state of polarization present the possibility to achieve SOP generation rates of the order of GHz [39]. Following the pulse amplitude modulation by the MZM, those pulses can be injected into a phase modulator where the input polarization maintaining fiber is oriented at 45Âº in relation to the optical axis. The two orthogonal optical components of the input pulse experience different refractive indices when propagate in the crystal, which is proportional to the applied voltage. Applying different levels of voltage values on the phase modulator we can change the output polarization state between $+45°$, $-45°$, right-handed circular, and left-handed circular. This kind of technique provides optical pulse modulation within the acceptance bandwidth of the phase modulators with high extinction ratio. Even achieving high rates in SOP generation, for instance in the order of GHz, using the current detection system the operation rate of the system is limited by single-photon detectors maximum detection rate of 100 MHz. However, this limit can be exceeded using superconducting nanowire detectors.

Chapter 3

Single-State Polarization Drift

In this chapter, we develop a method to compensate a single-state polarization random drift in optical fibers by mapping the estimated bit error rate on the Poincaré sphere. The developed method solves the problem of finding the appropriate polarization reversal operator of a particular SOP. We show that polarization random drift can be reversed by applying appropriate polarization rotations on the Poincaré sphere, in three iterations at most. This method is able to operate under different external perturbations and it is upper-layer protocol agnostic, it does not need auxiliary classical signals, extra spectral bands, nor additional hardware, and provides polarization basis alignment in less than tens of microseconds, with very low overhead.

This chapter contains five sections. In section 3.1, the current DV-QKD polarization compensation state of the art is presented. In section 3.2, the polarization compensation method for a particular SOP is detailed. In section 3.3, the bit error rate estimation impact on polarization compensation algorithm efficiency is discussed. In section 3.4, the algorithm behaviour is assessed considering a realistic situation. Finally, in section 3.5, the final remarks of this work are summarized.

3.1 State of The Art

The use of polarization to encode and decode quantum information appears natural for the exchange of qubits over optical links [61,63]. Nevertheless, standard single-mode optical fibers do not preserve the SOP, and therefore an active polarization basis alignment (PBA) method is required, to preserve the quantum information [72]. In order to allow the large deployment of polarization encoding QC systems, the PBA scheme must be efficient, simple, upper- layer protocol agnostic, and able to operate in a large variety of environment conditions.

We can consider two generic approaches for PBA, interrupting and real-timing methods. In the interrupting methods basis alignment stops the transmission of quantum information. In real-timing methods auxiliary channels tend to be needed. In [72], the authors quantitatively analyze both methods, using the QBER induced by polarization variations in sensitive QKD systems as a key criteria and considering the polarization drift-time and the tracking speed. For both real-time and interrupting methods a QBER threshold is considered beyond which the QKD procedure is interrupted to perfom polarization basis alignment in the interrupting method. In the real-time method a stronger reference signal is used to feedback the PBA method [72]. They concluded that the interrupting methods should be fast enough to revert the polarization in a time interval much shorter than the drift time. In [73], it was reported that the random polarization drift can induce a QBER exceeding 2.5% in less than 7 ms for aerial-fibers. In [74], also for aerial-fibers, transmission windows as short as 1 ms have been reported in polarization encoding quantum communication systems due to random polarization drifts. The real-timing methods tend to be less critical in terms of time polarization line-width [75], but generally require extra hardware to support the exchange of out-of-band control information [76]. A method that avoids the exchange of out-of-band information, but even still fast enough to operate under heavy external conditions it is clearly desirable [72]. In real-time scenarios, two different approaches have been presented: wavelength-division multiplexing polarization basis alignment (WDM-PBA) [73, 77, 78], and time-division multiplexing polarization basis alignment (TDM-PBA) [17, 79–81]. In [73], SOP tracking is performed using a hill-climbing algorithm in conjugation with a WDM polarization tracking scheme. In [78], a protocol-agnostic scheme is proposed using WDM-PBA in aerial fibers. In [17], it is shown that the achievable reach can be increased by using TDM-PBA based schemes. TDM-PBA may be implemented using classical [79, 80] or quantum reference signals [81]. In classical based TDM-PBA the co-propagation can produce a strong degradation in the weak quantum signals [79]. In [81], a time-division multiplexing (TDM) quantum reference signal is transmitted along with the quantum data signal, also avoiding the need of using both classical and quantum receivers. In [76], a protocol-dependent real-time scheme, free of reference signals is presented, where QKD unveiled bits are used to feed the algorithm to compensate random polarization drifts. That method has the advantage of not add additional overhead, but it is not protocol-agnostic, which can limit its practical implementation. In [16], an accurate QBER estimation method is proposed, and a QBER based PBA method is presented. That method is simple, upper-layer protocol agnostic and able to operate under different external conditions [16]. However, it uses a blind algorithm to align the polarization basis, which makes it quite inefficient, namely under large external condition perturbations [73, 78]. This method uses 12.5% of overhead on average in a laboratory environment, where the polarization remains stable for much longer than in aerial optical fiber installations [16]. In [75], a theoretical polarization drift model, which is able to describe random polarization rotations for installed fibers under different external conditions based on a single parameter is presented. This parameter, named polarization line-width, quantifies how fast the SOP changes with time [75]. This parameter takes into account the installation of the optical fiber and the external perturbations, and it allows to model the polarization random drift speed.

3.2 Algorithm Description

The 3D-Stokes space is a mathematically convenient alternative to represent and easily visualize the SOP of an optical field [75]. We start by showing that it is also possible to map the QBER on the Poincaré sphere, and then find the appropriate polarization reversal operator. We assume the polarization-based quantum communication system is composed by a transmitter, which emits weak laser pulses (approximated single-photon source) from a highly attenuated laser with a well defined particular SOP. After fiber propagation, a single SOP is measured at the detection stage, comprised by an EPC followed by a PBS, and a receiver with two single-photon detectors, see Figure 3.1. Without any loss of generality, we are going to assume that an error at the receiver occurs when for instance a particular horizontally polarized photon at the transmitter output follows the vertical path of the PBS at

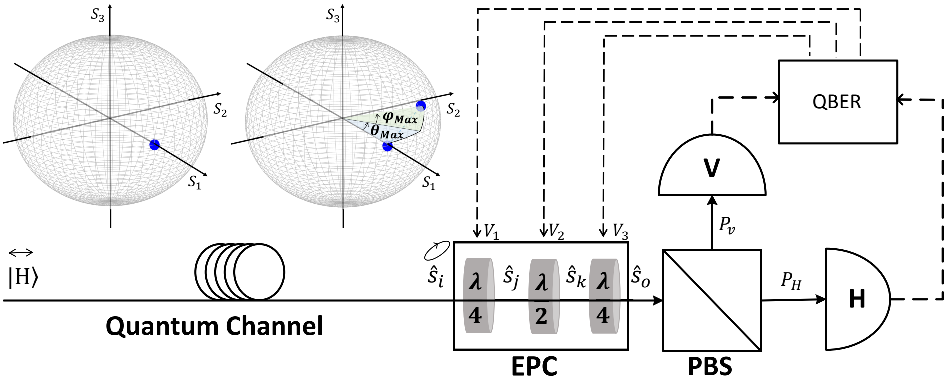


Figure 3.1: Horizontal SOP evolution throughout a quantum channel (optical fiber) which induces random polarization rotations, and detection probabilities at receiver (P_V and P_H). EPC: Electronic Polarization Controller. PBS: Polarization Beam Splitter. V: Single-photon detector in the PBS vertical port. H: Single-photon detector in the PBS horizontal port. V_1, V_2 and V_3: Voltages applied on the EPC to induce a certain rotation.

the receiver, inducing a click on the detector V, see Figure 3.1. Note that even in this chapter we consider the particular SOP a horizontal polarized single-photon, any initial polarization state can be reduced to the previous case by a solid rotation of the Poincaré sphere, in the same way that any SOP can be used as a reference for the null QBER.

In detail, when a photon reaches the PBS it has the probability P_H to follow the horizontal path, and the probability P_V of follow the vertical path [17],

$$P_H = 1 - P_V = \frac{1}{2}(1 + \cos\theta\cos\varphi), \tag{3.1}$$

where angles $\theta/2$ and $\varphi/2$ correspond to the orientation and ellipticity angles of the arriving photon SOP on Poincaré sphere representation, respectively [82]. Considering a horizontal state at the fiber input, we can write

$$\text{QBER}(\theta,\varphi) = 1 - \frac{1}{2}(1 + \cos\theta\cos\varphi). \tag{3.2}$$

Therefore, a QBER specifies a set of possible orientation and ellipticity angles. This set of values define a circle of a sphere on the Poincaré sphere, which corresponds to a QBER with reference to a given initial SOP. In the present case, apart from an horizontal polarized photon at the input of the quantum communication channel, we are also assuming fully polarized light. Therefore, the normalized Stokes parameter s_1 can be written as

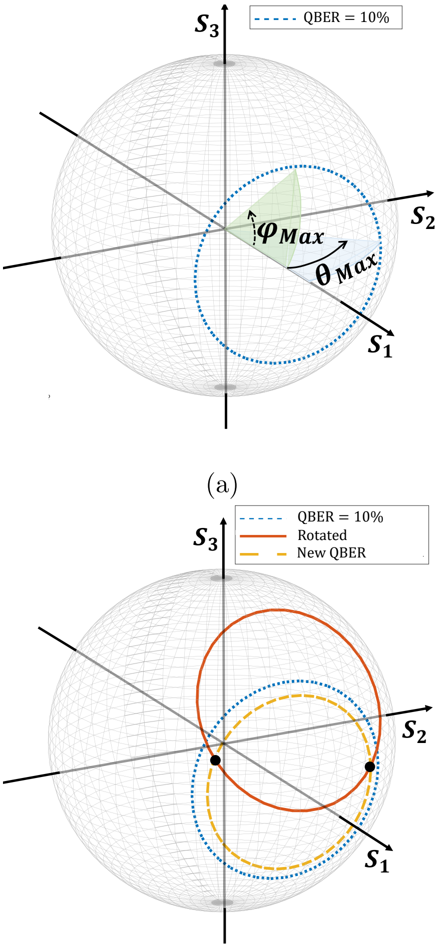
$$s_1 = \cos(\theta)\cos(\varphi), \tag{3.3}$$

where $\theta \in [0, 2\pi]$, $\varphi \in [-\pi/2, \pi/2]$ [83]. The QBER can also be written in terms of s_1 as

$$\text{QBER}(s_1) = \frac{1}{2}(1 - s_1). \tag{3.4}$$

Thus, the circle of a sphere resulting from a QBER value defines a set of possible SOP locations, which are at the same distance from the reference point,

$$d(\text{QBER}) = 2\arcsin\left(\sqrt{\text{QBER}}\right). \tag{3.5}$$



(a)

(b)

Figure 3.2: (a) Circle of a sphere with all possible states on Poincaré sphere that correspond to the QBER = 10%. (b) Circle of a sphere that corresponds to the QBER = 10% rotated considering $\theta_{\max}$ and $\varphi_{\max}$, and circle of a sphere with all possible states on Poincaré sphere that corresponds to the QBER after the previous rotation. The two symbols $\bullet$ represent the intersection points that correspond to the two possible SOP locations.

As we can see in Figure 3.2(a), a single value of QBER has more than one possible polarization reversal operator associated with it, even though a single received SOP leads to a single QBER value. Let us assume that a particular polarization rotation leads to a QBER of 10%, see Fig. 3.2(a). Looking into Figure 3.2(a), we can see that the polarization reversal operator still remains unknown, although it is restricted to rotations that lead the SOP from $(s_1, s_2, s_3)^T = (1, 0, 0)^T$, i.e. a horizontal initial SOP, to a point on the circle of the sphere that represents the 10% QBER. A subsequent deterministic rotation in conjunction with a new QBER calculation allows to reduce the number of possible polarization reversal operators to only two possibilities, see Figure 3.2(b). Note that a rotation can be characterized by the two angles, θ and φ,

$$\mathrm{R_T}(\theta, \varphi) = \mathrm{R}_{\mathbf{1}}(\varphi)\mathrm{R}_{\mathbf{2}}(\varphi)\mathrm{R}_{\mathbf{3}}(\theta), \tag{3.6}$$

where, $\mathrm{R}_{\mathbf{1}}$, $\mathrm{R}_{\mathbf{2}}$, and $\mathrm{R}_{\mathbf{3}}$ are the rotation matrices around the axis S_1, S_2, and S_3, respectively,

$$\mathrm{R}_{\mathbf{1}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{bmatrix}, \quad \mathrm{R}_{\mathbf{2}} = \begin{bmatrix} \cos\varphi & 0 & \sin\varphi \\ 0 & 1 & 0 \\ -\sin\varphi & 0 & \cos\varphi \end{bmatrix}, \quad \mathrm{R}_{\mathbf{3}} = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{3.7}$$

Once a rotation has been performed, as shown in Figure 3.2(b), another calculation of QBER is done. Let us assume the performed rotation was done using the orientation angle $\theta_{\max}/4$ and ellipticity angle $\varphi_{\max}/4$, where $\theta_{\max}$ and $\varphi_{\max}$ are the maximum angles defined by the circle of the sphere corresponding to the first QBER value calculated, see Figure 3.2(a). A new value for QBER allows to draw another circle of a sphere on Poincaré sphere, which intercepts the previous rotated circle in two points, which are shown in Figure 3.2(b) with circle marks. Therefore, the initial infinite number of possible polarization reversal operators is reduced to only two possibilities, which correspond to the reversal operator of the two intersection points. In order to obtain an analytical expression for the two intersection points, we can consider the parametric equations of a 3D circle, see Eq. (3.8). Note that m takes the value 1 for the initial QBER rotated circle, and 2 for the circle of a sphere after the QBER re-calculation,

$$\begin{cases} x^{(m)} = x_c^{(m)} + r_m \cos(\phi) x_{m1} + r_m \sin(\phi) x_{m2} \\ y^{(m)} = y_c^{(m)} + r_m \cos(\phi) y_{m1} + r_m \sin(\phi) y_{m2} \\ z^{(m)} = z_c^{(m)} + r_m \cos(\phi) z_{m1} + r_m \sin(\phi) z_{m2} \end{cases}, \tag{3.8}$$

where ϕ is a real value between 0 and 2π.

In Eq. (3.8), $(x_c^{(m)}, y_c^{(m)}, z_c^{(m)})$ are the center coordinates, and r_m is the radius of each circle m. Note that after measuring the QBER, a circle of a sphere is defined. From Eq. (3.2), $(x_c^{(m)}, y_c^{(m)}, z_c^{(m)})$, r_m, and the plane containing the circle defined by the orthogonal vector $\vec{n} = \vec{v}_{m1} \times \vec{v}_{m2}$, where $\vec{v}_{m1} = (x_{m1}, y_{m1}, z_{m1})$ and $\vec{v}_{m2} = (x_{m2}, y_{m2}, z_{m2})$, can be readily obtained.

The two measured QBER values define two circles of a sphere that intersect in two points, which can be obtained from

$$\begin{cases} x^{(1)} = x^{(2)} \\ y^{(1)} = y^{(2)} \\ z^{(1)} = z^{(2)} \end{cases}, \tag{3.9}$$

and represented in the 3D-Stokes space by,

$$\begin{aligned} s_1^{(n)} &= \cos\theta^{(n)} \cos\varphi^{(n)} \\ s_2^{(n)} &= \sin\theta^{(n)} \cos\varphi^{(n)} \\ s_3^{(n)} &= \sin\varphi^{(n)}, \end{aligned} \tag{3.10}$$

where $n \in \{1, 2\}$. Subsequently, the algorithm chooses a value of n to perform a new rotation. Let us assume that we pick $n = 1$. After applying a rotation with angles $(\theta^{(1)}, \varphi^{(1)})$, the QBER is recalculated, see Eq. (3.2). If the QBER goes bellow an user defined threshold, the polarization random drift has been compensated. Otherwise, the polarization random drift compensation can now be uniquely calculated by the following polarization reversal operator,

$$\mathrm{R_T}(\theta^{(2)}, \varphi^{(2)}) \mathrm{R_T^{-1}}(\theta^{(1)}, \varphi^{(1)}). \tag{3.11}$$

Algorithm for Polarization Random Drift Compensation

Parameters: QBER_{th} value above which the algorithm starts the actuation mode. Integer n, corresponding to the number of bits used to QBER estimation.
Inputs: Single-photon detectors measurements $m_0,\ m_1 \in \{0, 1\}$.

i. From the inputs estimate the QBER. If the estimated QBER is above QBER_{th} start the actuation mode. Map the circle corresponding to the QBER calculated on Poincaré sphere according with Eq. (3.2) (see Figure 3.2(a)).

ii. Perform a rotation with a given θ and φ. A $\theta = \theta_{max}/4$ and a $\varphi = \varphi_{max}/4$ are suitable (see Figure 3.2(b)).

iii. Calculate a new QBER (see Figure 3.2(b)). If the QBER decreases below QBER_{th}, the algorithm stops the actuation mode and goes to (i), otherwise continue to (iv).

iv. Find the two intersection points (see Eq. (3.9) and Eq. (3.11)).

v. Choose randomly one out of the two intersection points computed in (iv) to perform a new rotation (see Eq. (3.6)).

vi. Re-calculate the QBER. If the QBER is bellow QBER_{th}, the polarization random drift has been reverted. Otherwise, perform another rotation following Eq. (3.11), and go to (i).

Figure 3.3: Description of the algorithm to find the reversal operator and compensate the polarization random drifts.

In any of the two scenarios, the algorithm needs only three QBER calculations and three rotations at most to revert the polarization random drift due to birefringence effects along the optical fiber link, after starting the actuation mode. Figure 3.3 summarizes the stages of the algorithm actuation mode to compensate random polarization drifts when the QBER rises above a certain threshold.

Note that the voltages applied on the EPC, V_1, V_2, V_3, can be written in terms of angles θ and φ. These voltages induce a certain phase shift on the wave-plates by changing its orientation, which implies a rotation of the SOP based on a set of rotation angles, χ_1, χ_2, χ_3. These angles can be written in terms of the orientation and ellipticity angles, θ and φ. Looking into Figure 3.1, a random SOP $\hat{s}_i$ inputs the EPC facing the first quarter-wave plate (QWP) that outputs, in turn, the SOP $\hat{s}_j$,

$$\hat{s}_j = \mathrm{R}(\chi_1)\mathrm{M}_{\lambda/4}\mathrm{R}(-\chi_1)\hat{s}_i, \tag{3.12}$$

where $\mathrm{M}_{\lambda/4}$ is the QWP matrix [83] and $\mathrm{R} = \mathrm{R}_{\mathbf{3}}(2\chi_1)$ is the rotation matrix of the wave-plate. The angle χ_1 is given by [83],

$$\chi_1 = \frac{1}{2}\arctan\left(\frac{\sin\theta\cos\varphi}{\cos\theta\sin\varphi}\right). \tag{3.13}$$

The second wave-plate is a HWP, and transforms the linear SOP $\hat{s}_j$ into another linear SOP [83], which in practice means a rotation by θ around S_3 when $\varphi = 0$,

$$\hat{s}_k = \mathrm{R}(\chi_2)\mathrm{M}_{\lambda/2}\mathrm{R}(-\chi_2)\hat{s}_j, \tag{3.14}$$

where, $\mathrm{M}_{\lambda/2}$ is the HWP matrix, and $\hat{s}_j = (s_{1j}, s_{2j}, 0)^T$ defined by Eq. (10) in [83]. In this way,

$$\chi_2 = \frac{1}{4} \arctan\left(\frac{s_{2j}}{s_{1j}}\right), \tag{3.15}$$

where, s_{1j}, s_{2j} are defined by Eq. (3.16) and Eq. (3.17), respectively.

$$s_{1j} = s_{1i} \cos^2(2\chi_1) + s_{2i} \cos(2\chi_1) \sin(2\chi_1) + s_{3i} \sin(2\chi_1), \tag{3.16}$$

$$s_{2j} = s_{1i} \cos 2\chi_1 \sin(2\chi_1) + s_{2i} \sin^2(2\chi_1) - s_{3i} \cos(2\chi_1), \tag{3.17}$$

In addition, $s_{1i} = \sin\theta \cos\phi$ and $s_{2i} = \cos\theta \sin\varphi$, see Eq. (3.11). Finally, the EPC output SOP is defined as,

$$\hat{s}_o = \mathrm{R}(\chi_3)\mathrm{M}_{\lambda/4}\mathrm{R}(-\chi_3)\hat{s}_k, \tag{3.18}$$

where,

$$\chi_3 = \frac{1}{2} \arctan\left(\frac{s_{2k}}{s_{1k}}\right). \tag{3.19}$$

From a practical implementation point of view, we can not use all the qubits to estimate the QBER. In a practical scenario, one expects to use as few as possible number of qubits to compensate the random polarization rotations inside the optical fiber, leaving the most number of qubits for quantum communication purpose. In this scenario, the QBER is estimated taken into account a certain number of received qubits, N_r using

$$\widehat{\mathrm{QBER}} = \frac{e_r}{N_r}, \tag{3.20}$$

where e_r is the number of errors in N_r qubits [16].

This estimation is performed with a certain confidence interval which depends on the number of qubits that we use to perform it. In this section, we are assuming that N_r is large enough to provide an accurate estimation of the QBER. In the next section, we are going to consider and assess the impact of N_r during the algorithm's running. We also assume that our quantum communication system can operate with a QBER threshold of $\mathrm{QBER}_{\mathrm{th}} = 5\%$. Above this threshold value, the quantum communication system cannot operate. The goal of the presented algorithm is to force the QBER to be below the threshold. Figure 3.4 shows eight different cases corresponding to different initial conditions, where it is shown that regardless the respective initial QBER, the final QBER is always below the threshold. The inset in Figure 3.4 shows the location of the different SOPs on the Poincaré sphere, where each one is on the circle of a sphere corresponding to the QBER measured. In Figure 3.4 every case starts from an initial QBER estimation, i.e the first marker. The algorithm starts from this initial QBER estimation and performs the first rotation. The second marker is the QBER estimation after the first rotation. Here, the algorithm chooses one of the two intersection points, see Eq. (3.9). After that, we wait for a 5 errors event, or for 100 qubits received to estimate the new QBER. Note that more than 5 errors implies an estimated QBER larger than the threshold, in this case where a 5% threshold was assumed. When it wrongly chooses the intersection point, the next marker is a QBER above the $\mathrm{QBER}_{\mathrm{th}}$. On the other hand, when it rightly chooses the intersection point, the next marker is a QBER below threshold, and the following. A final marker with high accuracy on QBER estimation is also included in Figure 3.4, to show the proper operation of the algorithm. In Figure3.4, we have shown

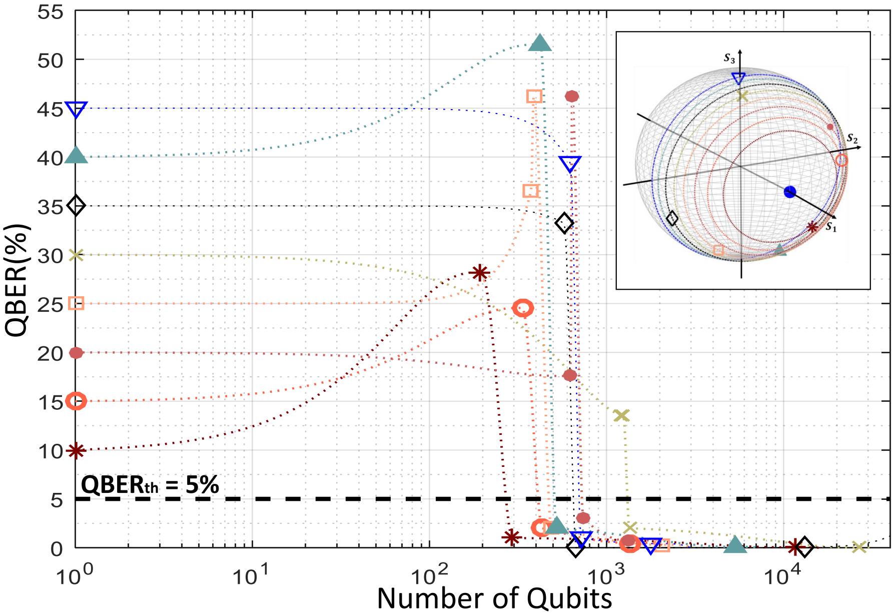


Figure 3.4: QBER evolution during the random polarization random drift compensation algorithm running. Markers represent QBER measurements for different initial QBER values. The initial SOP are represented on the Poincaré sphere shown in the inset, where the reference SOP is represented as a blue dot.

that the algorithm finds the appropriate polarization reversal operator and compensates any polarization random drift leading the initial QBER to a value below the threshold after two or three rotations, at maximum.

A complete and general polarization compensation algorithm should be able to find and reverse any SOP drift. We have described a method to compensate a particular SOP, nonetheless, our SOP drift compensation method can be generalized to any polarization drift suffered by an arbitrary SOP. In order to generalize the operation of the algorithm for an arbitrary channel input SOP, at least two canonically conjugated non-orthogonal states should be compensated [77, 79]. The generalization of the proposed algorithm for multi-state polarization random drift compensation is presented in chapter 4.

3.3 Impact of QBER Estimation Accuracy

In order to assess the impact of the QBER estimation accuracy in the algorithm performance, we are going to use a new coordinate γ, such that

$$\cos(\gamma) = \cos\theta\cos\varphi, \tag{3.21}$$

where γ is the angle between the axis S_1, and the Stokes vector of the SOP. In this way, the QBER in Eq. (3.2) can be written in terms of γ as

$$\mathrm{QBER}(\gamma) = \frac{1}{2}(1-\cos\gamma). \tag{3.22}$$

The number of qubits required for each algorithm iteration is the number of the qubits used for each QBER estimation, occurring in stages (i), (iii) and (vi), see Figure 3.3. The last

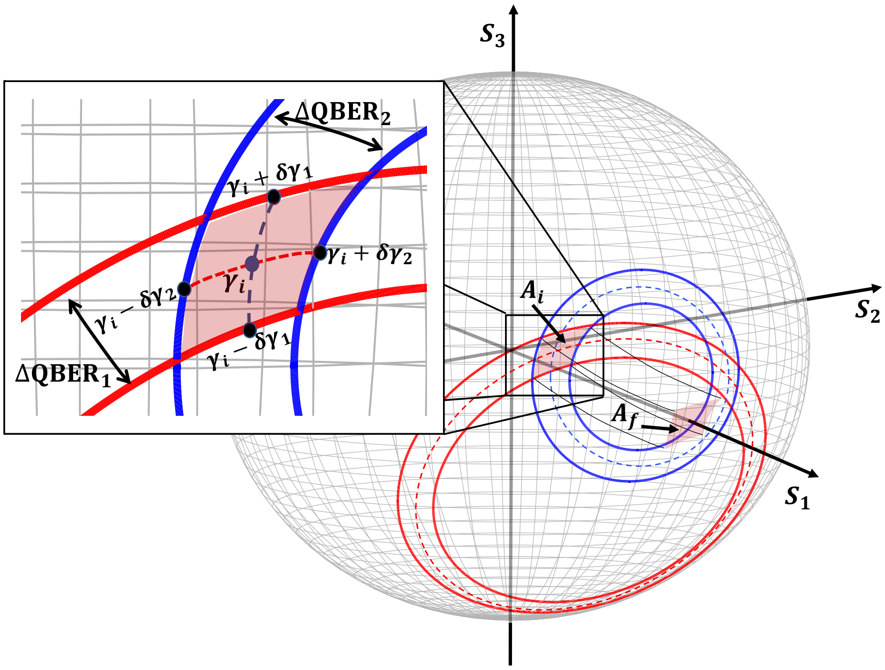


Figure 3.5: Representation of the area defined by the uncertainties of the first and second QBER estimations on the Poincaré sphere surface, A_i. This area is preserved after the final rotation, i.e. $A_i = A_f$. Inset shows a zoom in of the area resulted from the uncertainties of the two QBER estimations.

QBER estimation, at stage (vi), does not lead to any rotation, and therefore does not require high accuracy. In this way, we can assume that

$$n_1, n_2 \gg n_3, \tag{3.23}$$

where n_1, n_2 and n_3 are the number of qubits used in QBER estimations at (i), (iii), and (vi) defined in Figure 3.3, respectively. Therefore, the total number of qubits required to compensate the polarization random drift can be written as, see Eq. (15) from [16],

$$n_b \quad \simeq \quad n_1(\Delta\mathrm{QBER}_1, \mathrm{QBER}_1, \alpha) + n_2(\Delta\mathrm{QBER}_2, \mathrm{QBER}_2, \alpha), \tag{3.24}$$

where $\Delta\mathrm{QBER}_1$ and $\Delta\mathrm{QBER}_2$ are the uncertainty associated with the QBER_1 and QBER_2 estimations at stage (i) and (iii) of the algorithm, respectively, and $1 - \alpha$ is the confidence interval.

Note that the QBER estimation uncertainty, at stages (i) and (iii), can be written as

$$\Delta\mathrm{QBER}_i = \mathrm{QBER}(\gamma_i + \delta\gamma_i) - \mathrm{QBER}(\gamma_i - \delta\gamma_i), \tag{3.25}$$

where $\delta\gamma_i$ is the maximum deviation on γ_i, see Fig. 3.5. At stage (iv) of the algorithm, i.e. after two QBER estimations, an area can be defined due to the QBER estimation uncertainties, see inset on Figure 3.5.

From Eqs. (3.22) and (3.25), the uncertainty $\Delta\mathrm{QBER}_i$ at stages (i) and (iii) can be related to the corresponding γ_i, as well as to $\delta\gamma_i$, using

$$\Delta\mathrm{QBER}_i \approx \delta\gamma_i \sin\gamma_i. \tag{3.26}$$

Table 3.1: **Number of qubits required for estimation of QBER in terms of $\mathbf{QBER_{th}}$ for a confidence level of 99%.**

$\text{QBER}_{\text{th}}(\%)$	0.1	1.0	2.0	3.0	5.0	10.0
n	6743	699	357	243	150	79

The induced rotation into the SOP associated with the QBER estimations, at stage (v), is going to place the uncertainty area, A_i, around the target SOP, preserving its shape, A_f, as shown in Figure 3.5. Note that the final QBER, QBER_f, is null at $\gamma_f = 0$, therefore from Eq. (3.22) we obtain

$$\Delta\text{QBER}_f = \text{QBER}(\delta\gamma_f) \approx \frac{\delta\gamma_f^2}{4}. \tag{3.27}$$

The final QBER estimation uncertainty depends on the first and second QBER estimations, and as a consequence, the ΔQBER_f, see Eq. (3.27), depends on the $\delta\gamma_1$ and $\delta\gamma_2$. Note that the uncertainties ΔQBER_1 and ΔQBER_2 define an area that remains constant after the final rotation, see Figure 3.5. In the worst case scenario, $\delta\gamma_f$ will be the sum of both uncertainties $\delta\gamma_1$ and $\delta\gamma_2$,

$$\delta\gamma_f \leq \delta\gamma_1 + \delta\gamma_2. \tag{3.28}$$

For a given confidence interval $(1-\alpha)$, the algorithm satisfies

$$P(\text{QBER}_f \geq \Delta\text{QBER}_f) \leq 2\alpha. \tag{3.29}$$

Following this discussion, we can calculate the number of qubits required for QBER estimation at stages (i) and (iii) of the algorithm, so that the polarization control random drift algorithm assures a QBER_f below a certain QBER threshold, QBER_{th}, with a certain probability. Note that in a small rotation regime in stage (ii), we can also assume that $\delta\gamma_1 \approx \delta\gamma_2 \approx \delta\gamma$, and $\gamma_1 \approx \gamma_2 \approx \gamma$, which implies $\Delta\text{QBER}_1 \approx \Delta\text{QBER}_2$. Therefore $n_1 \approx n_2 \approx n$, and so that the total number of required qubits will be $n_b = 2n$.

Table 3.1 shows the number of qubits used to perform each QBER estimation, n, calculated given a certain QBER_{th}, using Eqs. (3.27) and (3.28) to calculate $\delta\gamma$, and using Eq. (3.22) to obtain γ in order to obtain the initial QBER uncertainty. Using the initial QBER uncertainty, the initial QBER, and for a given confidence level using Eq. (3.24), we can obtain the total number of required qubits, n_b, and subsequently n, the number of qubits to estimate QBER in stage (i) and (iii). The final QBER threshold has a high impact on the number of qubits required to estimate QBER during protocol execution, since the number of qubits is inversely proportional to the QBER threshold, as one can see in Table 3.1, i.e for smaller QBER_{th} a larger number of qubits is required [16]. This indicates that, in order to achieve a lowest QBER the performed rotation must be precise, and so that the estimated QBER should be as accurate as possible, which is obtained using a large number of qubits for the estimate. In order to assess the algorithm performance, we perform a simulation for a QBER threshold of 3%, considering two initial values for QBER, 10% and 40%. The SOP at the receiver input is randomly chosen between all possible SOP on the circle of a sphere corresponding with the desirable initial QBER. Following Table 3.1, and considering the 3% threshold, we use 243 qubits to estimate each QBER, at stages (i) and (iii) of the algorithm. We run 1000 simulations for each initial QBER. Moreover, the reached QBER estimation was performed with a high accuracy, 3500 qubits were used. Note that this estimation is not part of the algorithm, and it was only performed here to assess the algorithm performance. The obtained results show that for an initial QBER of 10% and 40%, the reached QBER is above the QBER_{th} only in 1.3% and 1.8% of the cases, respectively, which is in good agreement with Eq. (3.29), considering a confidence level of 99%, i.e. $2\alpha = 2\%$.

3.4 Algorithm Overhead

We performed numerical simulations, where the proposed algorithm was applied to a system developed to model a quantum communication system using polarization encoding of a single-state of polarization transmission. We assumed that the system operates at 100 MQubit/s, considering current avalanche photo-diodes based on single-photon detectors technology [84].

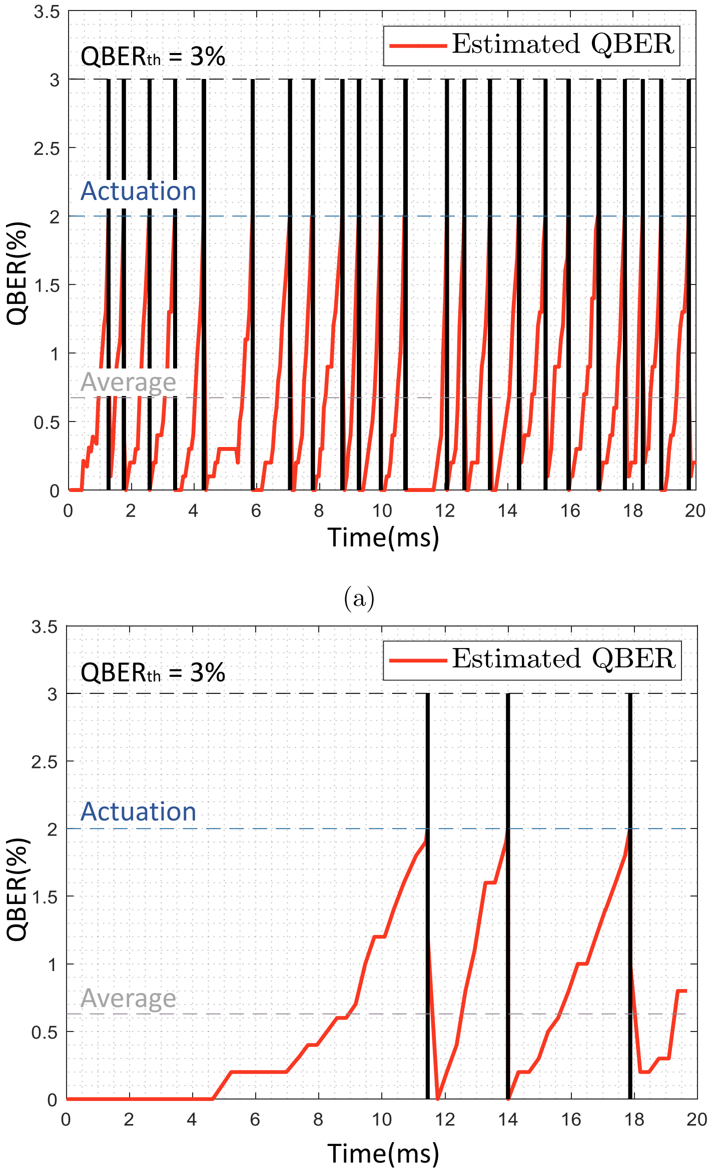
3.4.1 Assuming an Ideal Receiver

In a first instance, we only assess the algorithm actuation impact on a quantum communication system considering perfect devices, i.e. an EPC that actuates instantaneously, perfect single-photon sources, and single-photon detectors with unitary efficiency. The random polarization rotations were induced numerically simulating a polarization scrambler, based on [75]. We assume a QBER threshold imposed by the upper-layer protocols equal to 3%. This value should allow current quantum communication protocols to operate smoothly [85, 86].

We consider two scenarios for the impact of polarization drift. A first case, with an average transmission window of 0.8 ms, and another with a 8 ms average transmission window. We should note that transmission windows of 1 ms have been reported for very turbulent aerial fibers [74]. Buried fibers typically present transmission windows in the order of at least tens of seconds [72], and in the laboratory results have been reported with transmission windows of several minutes [16]. Therefore, both considered scenarios, 0.8 and 8 ms, can be seen as "worst case" scenarios. To model the polarization drift, we follow [75]. To obtain the desired transmission windows we use a polarization line-width, Δ_p [75], of 20 μHz and 0.2 μHz, respectively. Note that we refer to polarization line-width as the parameter used to measure the speed of the drift suffered by the SOP, and it has units of s^{-1}.

The polarization control system comprises two operation modes: a monitoring mode and an actuation mode. In the monitoring mode the QBER is estimated every 100 control received qubits and with a maximum sliding window of one thousand qubits. For polarization line-width of 20 μHz and 0.2 μHz, we assume 1 control qubit per 100, and per 500 transmitted qubits, respectively. From the defined QBER threshold and using Table 3.1, an actuation QBER can be obtained such that the upper-boundary QBER estimation does not exceed the user defined threshold. This QBER actuation value leads to the commutation between the monitoring and the actuation mode. We use a 2% value for the actuation QBER. When the algorithm enters in the actuation mode, it follows the steps presented in section 3.2. In this mode, all transmitted qubits are used for polarization control. After the algorithm actuation, the QBER estimation window is reset.

In order to assess the algorithm's performance, we measured the algorithm's overhead, the actuation time, actuation frequency, average QBER, and maximum QBER for both situations, corresponding to the polarization line-width of 20 and 0.2 μHz. The algorithm's overhead is defined as the ratio between the number of qubits used for polarization monitoring and control, and all transmitted qubits. The algorithm's actuation time is the average time that the algorithm takes to compensate the polarization drift, and leads the QBER to a value below the actuation QBER. The algorithm's actuation frequency is defined as the number of times that the algorithm actuates per unit of time. The average and maximum QBER are calculated considering the data qubits. To assess the algorithm performance, we run



(a)

(b)

Figure 3.6: (a) - QBER monitoring with actuation of the proposed algorithm for polarization random drift compensation in an extreme scenario, where polarization line-width is 20 μHz. (b) - QBER monitoring with actuation of the proposed algorithm for polarization random drift compensation in scenario considering a polarization line-width of 0.2 μHz. Vertical black lines represent the actuation time that the algorithm takes to find the polarization reversal operator and reverse the polarization drift.

simulations during 20 ms time windows on the specified scenarios.

Figure 3.6(a) and 3.6(b) show the evolution of QBER for the two considered scenarios using the proposed algorithm to find the polarization reversal operator to compensate the drift. As it is shown, whenever the QBER rises above the actuation QBER, 2.0%, the algorithm actuates being able to reestablish the qubits data transmission in 12 μs on average for polarization line-width of 20 μHz, see Figure 3.6(a), and in 7.39 μs on average for 0.2 μHz, see Figure 3.6(b). The actuation times are represented by vertical lines in the plots, where the width of the lines correspond to the algorithm actuation time. On average, the algorithm actuates 1.15 times per millisecond, imposing a transmission window of 0.8 ms on average with an overhead of 2.54% in the case represented in Figure 3.6(a). For the case presented in Figure 3.6(b) the algorithm actuates 0.15 times per millisecond, imposing a transmission window of 8 ms on average with an overhead of 0.31%. Note that during monitoring mode, the QBER estimation demands 1% and 0.2% overhead in 20 μHz and 0.2 μHz polarization line-width scenarios, respectively. The remaining overhead is used by actuation mode. The average QBER during data qubits transmission remained below the 3% threshold, and a maximum QBER of 2.1% was obtained in both scenarios.

3.4.2 Assuming a Realistic Receiver

Now, we will assess the algorithm's performance considering off the shelf imperfect devices and its technical limitations. We consider a highly attenuate laser, i.e. a source with a Poisson statistics, a 0.2 dB/km fiber channel attenuation [87], and 25% single-photon detectors efficiency [88]. In order to overcome the issues related with no-click events, and reduce its impact on algorithm's performance, the number of photons in control qubits is optimized. By increasing the number of photons in each control qubit, we also increase the double-click events when the photons polarization is not perfectly aligned due to polarization random drift. Double-clicks can also be caused by the detectors dark-counts, which we assumed a value of 5×10^{-4} for each detector [88]. Both, no-click and double-click events will impact the overhead used by the algorithm, since the qubits measured in that situation are discarded, and not taken into account for QBER estimation. An average number of photons per pulse of 0.1 at the transmitter output was assumed [42]. Two optical channel lengths were defined to perform this analysis, 40 km and 80 km. Figure 3.7 shows the overhead according with the average number of photons per control qubit at the transmitter output. We change the number of photons in the control qubits in order to find the optimum number photons at the receiver input, which we found to be around 5. Note that, for 40 km optical channel length, the number of photons needed at transmitter output is much lower than for 80 km optical channel length. The four curves placed above 4% overhead correspond to a 20 μHz polarization line-width, where the transmission window is on average 0.8 ms, and it is shown that the overhead does not depend significantly on the optical channel length, as well as the optimum number of photons per control qubits.

Due to technological limitations, the EPC does not induce an instantaneous rotation, and it demands a certain time interval to stabilize the output SOP. In this way, the EPC actuation time should be considered in the system assessment. An EPC actuation time of 20 μs was assumed [78], which corresponds to increase the overhead by 2000 qubits in each performed rotation for a transmission rate of 100 MQubits/s. Fig. 3.7 also shows the overhead resulted from adding the EPC actuation time for both optical channel lengths. Even though the overhead increases due this technological limitation, it remains below 9% even for the 0.8

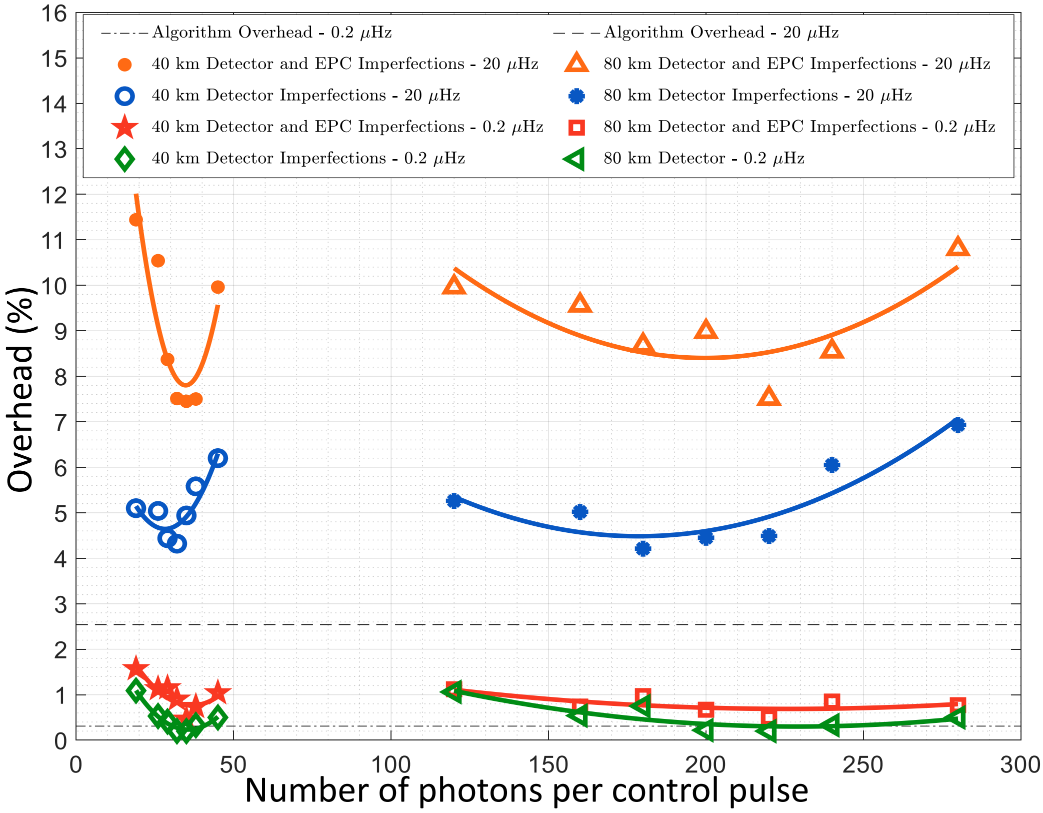
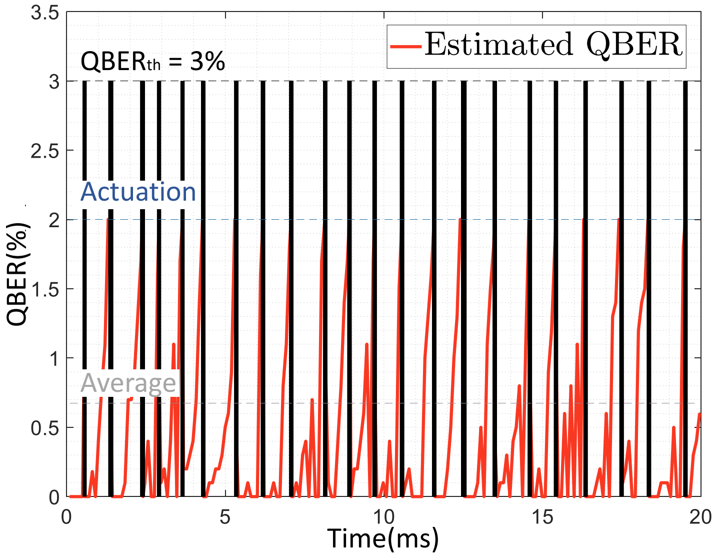


Figure 3.7: Overhead for different average number of photons per control pulse, considering two different optical channel lengths (40 and 80 km). For each fiber length, the overhead was measured considering both a perfect and an imperfect EPC. Two values for polarization line-width were considered, 0.2 μHz and 20 μHz. Dashed and dashed-dot lines represent the intrinsic overhead values considering perfect devices for 20 and 0.2 μHz values of polarization line-width, respectively.

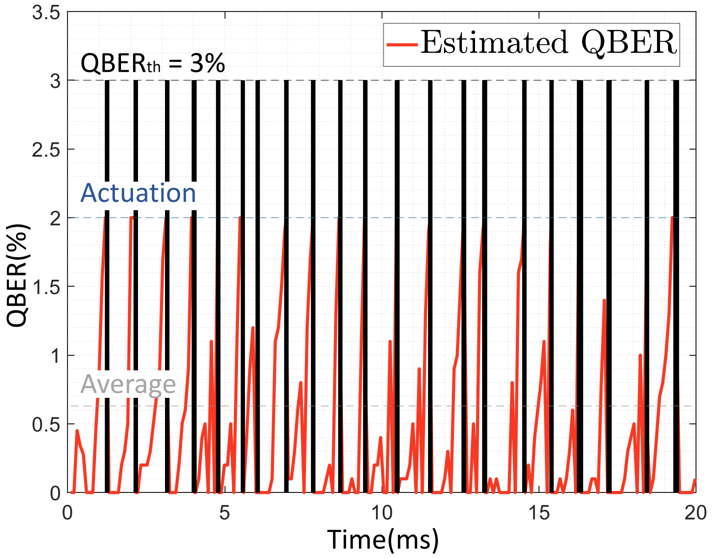
transmission window, which nevertheless is lower than the value presented in [16] for a larger transmission window.

The overhead obtained for both ideal scenarios previously considered is also shown in Figure 3.7 corresponding to 2.54% and 0.31% for a polarization line-width of 20 μHz and 0.2 μHz, respectively. Moreover, according with the number of photons per control qubit the overhead was also calculated for both optical channel lengths considering a 0.2 μHz polarization line-width, that imposes a transmission window of 8 ms on average. As shown in Figure 3.7, the overhead remains below 1.5% for every number of photons considered, even taken into account imperfect devices.

Figures 3.8(a) and 3.8(b) show the QBER monitoring for a polarization line-width of 20 μHz considering both lengths for the communication channel, 40 km and 80 km, respectively. In this case, the number of photons per control pulse was adjusted aiming to achieve the minimum overhead. In this way, according with Figure 3.7, we chose 32 photons for the 40 km situation and 200 photons for the 80 km situation. We consider that the EPC takes $10\mu s$ to apply a single rotation. Comparing Figure 3.8(a) with 3.6(a), we can see that now the vertical black lines tend to be wider, due to EPC actuation time. Even so, it is able to



(a)



(b)

Figure 3.8: QBER monitoring taking into account the actuation time of the EPC besides the detector imperfections. Data obtained for a 20 μHz polarization line-width. Vertical black lines represent the actuation time that the algorithm takes to find the polarization reversal operator and reverse the polarization drift. (a) 40 km optical fiber length. (b) 80 km optical fiber length.

reverse the drift in $20\mu s$, in average, and with an overhead lower than 3% in both cases.

3.5 Final Remarks

We presented an algorithm to automatically compensate a single-state polarization random drift in polarization-encoding based quantum transmission systems. This algorithm is based on QBER estimation and on its representation on the Poincaré sphere, allowing to find the appropriate polarization reversal operator in order to minimize the algorithm overhead. From the estimated QBER, a circle on the Poincaré sphere is defined leading to a set of possible polarization states. By performing a deterministic rotation, the algorithm reduces this set of polarization states to only two possible SOP. From this two possible states of polarization the algorithm is able to compensate the polarization random drift in a very short time. Note that the presented algorithm compensates a particular single-state of polarization.

It was shown that the proposed algorithm is always able to force the QBER to a value below a threshold suitable to implement the BB84 protocol in three iterations, at most. In addition, the uncertainty in the final QBER was related with an area calculated in the Poincaré sphere surface based on two QBER estimation uncertainties. From this area, we obtain the number of qubits required in the QBER estimations to guarantee a final QBER below the threshold.

Moreover, the proposed algorithm was assessed considering two different scenarios. It was assumed two values for polarization line-width, 20 μHz, which imposes a transmission window of around 0.8 ms, and 0.2 μHz, which imposes a transmission window of around 8 ms. In both situations, the algorithm was capable of maintain the QBER below the 3% threshold using only 2.54% of overhead, and 0.31% of overhead, respectively. Furthermore, when imperfect devices limitations are taken into account, namely the EPC actuation time, a highly attenuated laser source, optical channel attenuation, and single-photon detectors efficiency, the overhead slightly increases but remains well below the values reported by blind algorithms. For a transmission window of 8 ms, the overhead is still below 1%, even considering the impact due to device imperfections.

The proposed method actively aligns the polarization basis of a particular SOP with very low overhead, and without using out-of-band signals. Due to its low overhead, it can be used even in scenarios where the fiber is subjected to heavy external perturbations, such as buried fibers in highway, railways, or even aerial fibers, where transmission windows are very short due to the random polarization drift. The presented results show the possibility to revert the polarization drifts of a particular SOP in tens of microseconds.

Chapter 4

Polarization Drift Compensation

In this chapter, we propose a novel heuristic searching method to compensate polarization random drift of any state based on the QBER of only two non-orthogonal mutually unbiased states of polarization. By compensating two states of polarization belonging to two non-orthogonal mutually unbiased bases, we are able to compensate any state of polarization. Through the use of quantum frames, the proposed method continuously monitors the QBER of two states of polarization being able to maintain a real-time drift tracking.

This chapter contains 6 sections. In section 4.1 the current state of the art is presented. In section 4.3,we detail the implemented system model. In section 4.2, the method to compensate polarization random drift of the SOPs to be used in BB84 QKD through fiber-optics quantum channel is proposed. In section 4.4, we present the numerical validation for the method to compensate polarization random drift of any arbitrary SOP. In section 4.5, we assess the performance of BB84 protocol in a finite-key size implementation using the proposed algorithm in a discrete variable polarization encoding quantum communication system. Finally, in section 4.6 the final remarks are summarized.

4.1 State of The Art

Photonic qubits are generally encoded using polarization [19]. Nevertheless, the state of polarization that carries quantum information can be affected when goes through a transmission channel that does not preserves the polarization state, such as the standard optical fibers [13]. Furthermore, the information flow may even be interrupted when the error rate among the legitimate users of quantum channel rises to a value that makes it unsuitable for a reliable information transmission [89, 90].

The polarization mode dispersion is commonly considered a serious obstacle on polarization based communication systems over optical fiber networks [91]. It results in SOP changes with time in a random fashion, which compromises the accuracy of the SOP measurements at the receiver [75]. Such random behaviour represents a real challenge for controlling in practical field polarization based QKD systems, which demands the employment of a polarization control scheme. In addition, in the case of BB84 protocol it is required the usage of two non-orthogonal mutually unbiased bases to generate four states of polarization [92, 93]. Also, a complete and general polarization compensation method for any arbitrary input SOP should at least compensate two of the three non-orthogonal mutually unbiased bases [79]. For instance, and without loss of generality, one can compensate the horizontal and the +45° linear polarization states, which are canonically conjugated non-orthogonal, thus achieving the compensation of all Poincaré sphere SOPs [77]. One possible approach for full polarization random drift compensation in real-time requires additional classical signals containing two non-orthogonal polarization states that must follow the same optical fiber path in order to experience the same random fashion behavior as the quantum polarization states that carry information. However, the intensity of those additional classical signals are usually orders of magnitude higher than the magnitude of the quantum signal, which induces high noise levels hindering the transmission of quantum signals. One of the simplest methods to compensate polarization random drift in real-time requires time multiplexed additional reference signals tuned at the same wavelength [72, 77]. However, this approach limits the transmission rate of secure information. On the other hand, the WDM technique require additional spectral bands [78]. By using WDM techniques, the reaching distance between parties is also limited since the information decorrelation between the two wavelengths increases with distance [17].

An alternative approach is the use of feedback algorithms free of additional classical reference signals [73]. Moreover, in [94] the suitability of the use of quantum frames in QKD systems with polarization encoding was demonstrated. In [76], a protocol-dependent method to compensate polarization drift using the unveiled bits was proposed. Even though this method does not require additional reference signals neither additional dedicated bits, it depends on the implemented protocol which limits its large deployment. Despite being a blind searching algorithm, in [16] the authors proposed an upper-layer agnostic polarization compensation method. In [95] a feedback loop is used to also implement a blind stochastic searching algorithm, which finds the set of voltage values to apply on the electronic polarization controller to minimize the QBER. This method achieves a QBER as lower as 3%. However, the use of blind searching methods increases the required bandwidth consumption, which issue can be overcome using heuristic searching methods. In [27] a heuristic search method is presented, where the reversal operator to compensate polarization random drift in standard fiber-optics channels of a particular SOP is found based on the QBER value. This method is capable of finding the reversal operator for a particular SOP that has suffered polarization random drift, and compensate it in less than tens of microseconds with a very low overhead.

In order to enable the large employment of polarization based QKD protocols, a generalization of the heuristic method to compensate a particular SOP presented in [27] can solve the problem of the random drift polarization behaviour of polarized single-photons when transmitted over standard single-mode optical fibers. Moreover, as far as we know there is still no heuristic searching method to simultaneously compensate the BB84 QKD states of polarization until now.

4.2 Heuristic Polarization Compensation Method

In this section, we propose a method to compensate arbitrary SOP drifts induced by birefringence through a fiber-optics based quantum channel. The method is based on the estimation of the QBER computed from a set of quantum frames encoded in non-orthogonal mutually unbiased bases. [77]. The method starts by compensating the SOP whose its QBER first rises above a user defined QBER threshold. In this context, it is not relevant which state is first compensated. The polarization random drift compensation is performed applying reversal rotations on the SOP that arrives at receiver with a misaligned polarization compared

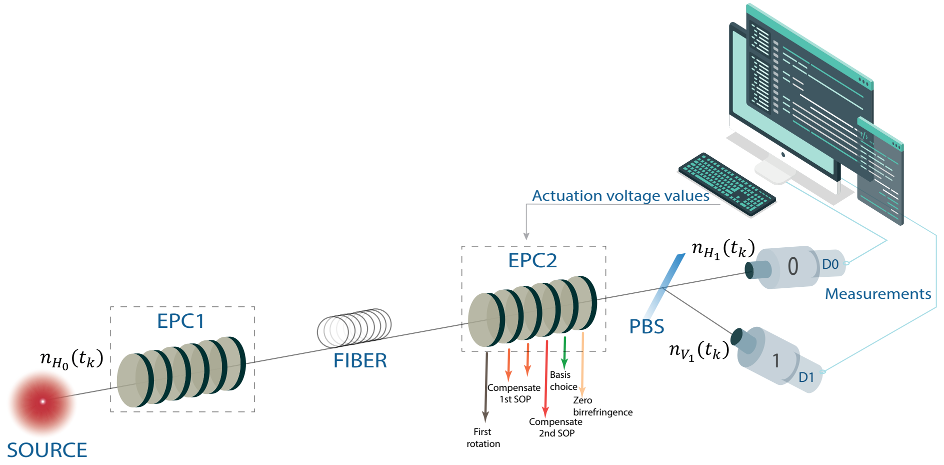


Figure 4.1: Schematic of the QKD system configuration using polarization encoded single-photons in two non-orthogonal basis, with active polarization drift compensation. EPC: Electronic polarization controller. D1 and D2: single-photon detectors.

with the one it had when left the transmitter. Nevertheless, it is crucial that the rotation applied to compensate the non-orthogonal SOP does not impact the one already compensated. In this way, the more important consideration is to guarantee that the rotation applied to compensate the non-orthogonal SOP is performed around the axis on which the already compensated one is placed on.

Lets detail the operation mode of the polarization drift compensation method. The communication between parties is performed using quantum frames [94]. The transmitted frame is divided in two quantum frames: control frame and data frame. The proposed method continuously keep track on the QBER of the control qubits individually, which are known in advance by both parties, and these values are continuously compared with a previously defined threshold above which starts the compensation method.

Without loss of generality, we choose for the control qubits the $|H\rangle$ and the $|45\rangle$ polarization states. Lets assume a threshold value above which the method must be applied, QBER_{th}. By continuously monitoring both QBER values, $\text{QBER}_{|H\rangle}$ and $\text{QBER}_{|45\rangle}$, the algorithm starts the operation mode as soon as one of them crosses the threshold. The first SOP whose QBER rises above the threshold is the first to be compensated. We assume a six wave-plate EPC, where four of the six wave-plates are used to induce the required rotations, one is used for basis selection and the last one is connected to zero birefringence and has no impact in the system. Regardless of which one is the first SOP to be compensated, the first wave-plate of the EPC is responsible for a first small arbitrary rotation as suggested in the algorithm presented in [27]. With that rotation we aim to change the QBER value on the physical system, and simultaneously we apply the same rotation in software on the first circle of a sphere drawn due the first estimated QBER. Next, a new QBER is estimated, and the two possible locations of the SOP result from the intersection between those two circles. In order to fulfill this step of the algorithm, two angles must be chosen to induce a small rotation on the first wave-plate of the EPC, α and δ. The transformation matrix of a linear retarder with fast angle, α, and retardation, δ, is given by $R(\alpha, \delta)$ [82],

$$\mathrm{R}(\alpha,\delta)=\begin{bmatrix} e^{i\delta/2}\cos\alpha^2+e^{-i\delta/2}\sin\alpha^2 & e^{i\delta/2}-e^{-i\delta/2}\sin\alpha\cos\alpha \\ e^{i\delta/2}-e^{-i\delta/2}\sin\alpha\cos\alpha & e^{-i\delta/2}\cos\alpha^2+e^{i\delta/2}\sin\alpha^2 \end{bmatrix}. \tag{4.1}$$

Note that the angles used in this rotation do not depend of which state is being first compensated,

$$\alpha = \pi/4 - \alpha_{\mathrm{max}} \tag{4.2a}$$

$$\delta = -2\delta_{\mathrm{max}}, \tag{4.2b}$$

where α_{max} and δ_{max} are the rotation and ellipticity angles, respectively, defined by the circle of a sphere corresponding to the estimated QBER with relation to the reference state of polarization, see Fig. 4.2 [27]. The second and third wave-plates of the EPC are used to compensate the control qubit of which its QBER first crossed the threshold with the transformation matrix $R(\alpha_1, \delta_1)$ and $R(\alpha_2, \delta_2)$, respectively. In this way, the transformation matrix used to compensate the first SOP is the concatenation of three matrices,

$$R_1 = R(\alpha_2, \delta_2)R(\alpha_1, \delta_1)R(\alpha, \delta). \tag{4.3}$$

For instance, lets assume the first state to be compensated is the $|45\rangle$, and the following must be guaranteed,

$$R_1\mathrm{R_F}\,|45\rangle = |45\rangle\,, \tag{4.4}$$

where $\mathrm{R_F}$ is a Jones matrix that represents the random rotation induced by the standard fiber-optics channel. Fig.4.3 (a) shows the Stokes representation of the rotations induced by

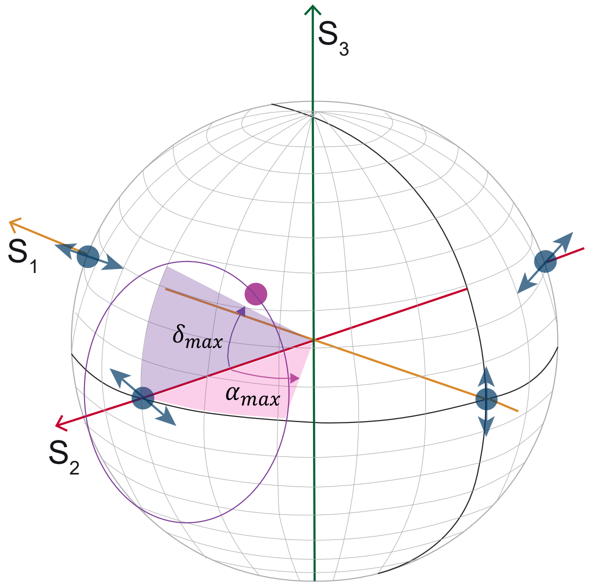
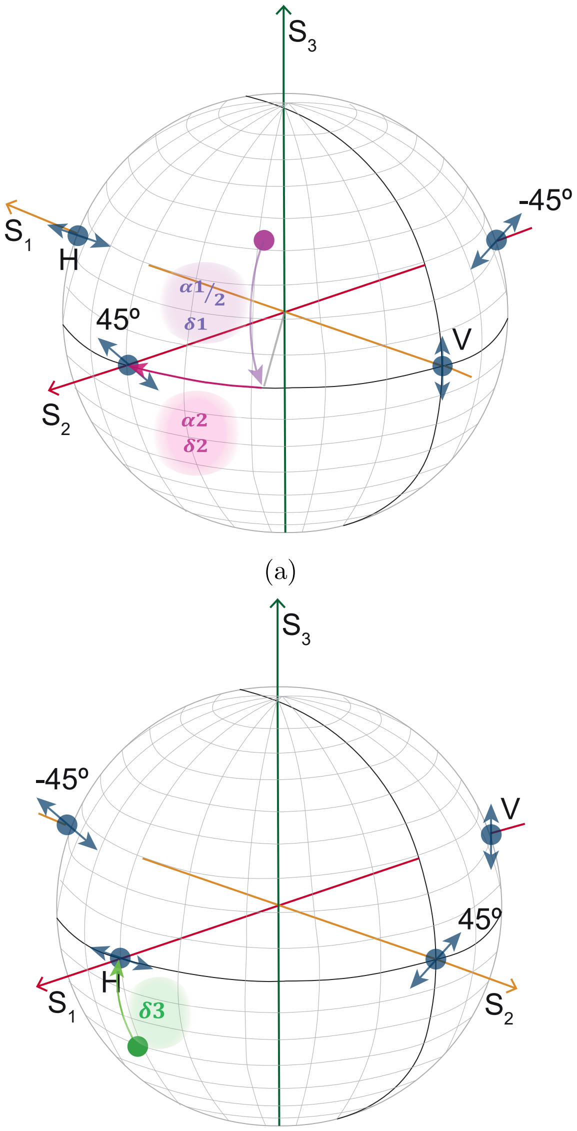


Figure 4.2: Circle of a sphere defined by all possible states of polarization corresponding with the QBER of the control qubits that first rises above the threshold. α_{max} and δ_{max} correspond to the rotation and ellipticity angles defined by the circle of a sphere, respectively.



(a)

(b)

Figure 4.3: Stokes space representation of the rotations induced by R_1 and R_2. (a) Rotations induced at wave-plate 2 and 3 to compensate the first SOP. At this point both angles α_i and δ_i can vary. (b) Rotation induced by wave-plate 4 to compensate the second SOP without influence the first SOP already compensated. At this point α is maintained constant and aligned with the axis on which the first SOP is on. Only δ_3 varies.

$R(\alpha_1, \delta_1)$ and $R(\alpha_2, \delta_2)$. According to Fig. 4.3 (a), the first rotation must be performed such that,

$$\alpha_1 = 2\arctan\left(\frac{S_1/S_2}{2}\right) \tag{4.5a}$$

$$\delta_1 = \arcsin(S_3), \tag{4.5b}$$

where $(S_1, S_2, S_3)^T$ are the stokes parameters corresponding to the intersection points found

Method for full QKD states of polarization random drift compensation

Parameters: $\mathrm{QBER}_{\mathrm{th}}$ value above which the algorithm starts the actuation mode. Integer n, corresponding to the number of bits used to QBER estimation. Integer L, corresponding to frame length. Integer c, corresponding to control frame length, and integer d, corresponding to data frame length. The values of the angles α and δ that lead to the initial rotation and can be calculated using (4.2a) and (4.2b), respectively.
Inputs: Single-photon detectors measurements $m_0,\ m_1 \in \{0, 1\}$.

i. From the inputs individually estimate the QBER of each of the two canonically conjugated control non-orthogonal states. As soon as one of these values is above QBER_{th} start the actuation mode. Apply the first rotation on the EPC2 (see Fig. 4.1) first wave-plate, $R(\alpha, \delta)$.

ii. Run the algorithm proposed in [27] for the first SOP to be compensated, and apply the rotations on EPC2 (see Fig. 4.1) wave-plates 2 and 3, $R(\alpha_1, \delta_1)$ and $R(\alpha_2, \delta_2)$.

iii. The QBER of the first compensated SOP should approach the zero boundary and the other SOP should have a certain QBER value. The last rotation should be applied on the 4th wave-plate, $R(\alpha_3, \delta_3)$, in such a way that do not have influence on the first compensated SOP. To guarantee this requirement the rotation angle of the wave-plate, α, must be aligned with the axis over which the first compensated SOP is placed on.

Figure 4.4: Description of the method for QKD states of polarization random drift compensation.

by the polarization compensation method. Thereafter, the second state to be compensated is $|H\rangle$, and the fourth wave-plate is responsible for performing the polarization drift compensation of this state with no influence on the first which is already compensated. In this way, the main rotation axis of the fourth wave-plate must be aligned with the SOP already compensated. Before inducing any rotation, the QBER of each control qubit is again estimated, see Fig. 4.4 step (iii). The $\mathrm{QBER}_{|45\rangle}$ should approaches the zero bound. At this stage, the transformation matrix to be applied to decrease this QBER to a value close to the zero bound is

$$R_2 = R(\alpha_3, \delta_3), \tag{4.6}$$

which must guarantee that,

$$R_2 \, |45\rangle = |45\rangle \, . \tag{4.7}$$

Since we assumed the first state to be compensated is the $|45\rangle$, the non-orthogonal state of polarization to be compensated now is the $|H\rangle$. Fig.4.3 (b) shows the rotation performed using the fourth wave-plate, and at this point the α_3 must be maintained constant and coincident with the axis S_2 such that the rotation induced does not have influence in the first compensated SOP. Note that, in any case the matrix $R(\alpha_3, \delta_3)$ can only vary one of the angles and maintain the other. In the case we are currently analyzing, the α_3 angle must be constant and coincident with the axis S_2 therefore the induced rotation has no influence on the first SOP already compensated $|45\rangle$, since the performed rotation is around the axis which it is on. In this way,

$$\alpha_3 = \pi/4, \tag{4.8}$$

and δ_3 can assume two different values, $\pi - \delta_k$ or $\pi + \delta_k$, where δ_k is defined as following,

$$\delta_k = \arccos\left(2(1 - \mathrm{QBER}_{|H\rangle}) - 1\right). \tag{4.9}$$

The polarization compensation method chooses one of the two possible δ_3 and estimates the QBER. If the QBER does not approaches zero another rotation is induced using the other angle. Otherwise, the compensation procedure stops and runs as initially, i.e. monitoring the QBER using quantum frames. The concatenation of both transformation matrices R_1 and R_2 must compensate the polarization drift induced in $|H\rangle$ by $\mathrm{R_F}$,

$$R_2 R_1 \mathrm{R_F} \, |H\rangle = |H\rangle \,. \tag{4.10}$$

Once assuring (4.4), (4.7) and (4.10) the polarization random drift compensation method compensates two non-orthogonal states of polarization from two mutually unbiased bases, which implies the compensation of the BB84 QKD states of polarization on the Poincaré sphere.

4.3 System Description

A conventional physical system to implement QKD is shown in Figure 4.1. To support any QKD upper-layer protocol assuring unconditional security, the physical layer system must allow to encode the photons in four states of polarization using two non-orthogonal bases [12]. In this work, we use the two non-orthogonal linear bases: rectilinear basis, $|H\rangle$ and $|V\rangle$, and diagonal basis, $|45\rangle$ and $|-45\rangle$.

4.3.1 Transmitter

In the transmitter side, it is assumed a well defined horizontal polarized state at the input of the EPC1, which is obtained from a strongly attenuated laser source whose optical pulses have an average number of photon per pulse of $n_{\mathrm{H}_0}(t)$. In this way, the number of photons per pulse is randomly generated from a Poisson distribution,

$$n_{\mathrm{H}_0}(t) \sim \mathrm{Poisson}(\mu), \tag{4.11}$$

where μ is the average number of photons per pulse. The EPC1 is responsible for encoding any state of polarization applying a rotation on the input state, for instance the four required for QKD implementation. For that purpose only one wave-plate of the EPC1 is required, and its transformation matrix is assumed to be described as a rotation imposed by a wave-plate [82],

$$\mathrm{R_{EPC1}} = \begin{bmatrix} R_{11}(\delta_{\mathrm{in}}(t), \alpha_{\mathrm{in}}(t)) & R_{12}(\delta_{\mathrm{in}}(t), \alpha_{\mathrm{in}}(t)) \\ R_{21}(\delta_{\mathrm{in}}(t), \alpha_{\mathrm{in}}(t)) & R_{22}(\delta_{\mathrm{in}}(t), \alpha_{\mathrm{in}}(t)) \end{bmatrix}, \tag{4.12}$$

where R_{ij} is the element of a rotation matrix induced by a wave-plate [82], see (4.1), α_{in} represents the orientation of the wave-plate, and δ_{in} represents the wave-plate retardation angle [96]. After the EPC1 the number of photons in horizontal and vertical component can be written as

$$\begin{aligned} n_{\mathrm{H}_1}(t) &= n_{\mathrm{H}_0}(t) \mid R_{11}(\delta_{\mathrm{in}}(t), \alpha_{\mathrm{in}}(t)) \mid^2 \\ n_{\mathrm{V}_1}(t) &= n_{\mathrm{H}_0}(t) \mid R_{21}(\delta_{\mathrm{in}}(t), \alpha_{\mathrm{in}}(t)) \mid^2 . \end{aligned} \tag{4.13}$$

4.3.2 Fiber-optic Quantum Channel

The fiber-optic quantum channel is modeled based on the work presented in [75], and we represent it as a random matrix parameterized by the random parameters $\gamma_k = (\gamma_1, \gamma_2, \gamma_3)$,

$$\mathrm{R_F}(\gamma(t)) = \mathbf{I}\cos\psi - i\mathbf{a}\cdot\vec{\sigma}\sin\psi, \tag{4.14}$$

where $\vec{\sigma}$ is the tensor of Pauli matrices, $\mathbf{I}$ is a 2×2 identity matrix, $\gamma(t) = \psi\mathbf{a}$, with length $\psi = \|\gamma(t)\|$, denoting $\|\cdot\|$ the euclidean norm [75]. Furthermore, $\mathbf{a} = (a_1, a_2, a_3)$ denotes the direction defined in a unitary sphere. The randomness of rotations is defined by γ_k parameters obtained from a normal distribution with mean zero and standard deviation $\sigma^2 = 2\pi\Delta_p T$, being T the total acquisition time and Δ_p the polarization line-width that defines the velocity of the random drift [75]. Therefore, the temporal drift evolution is modelled by concatenating consecutive matrices $\mathrm{R_F}$ with different random generated $\gamma(t)$ at each instant. Moreover, it is worth noticing that we are assuming a quantum channel free of depolarization and dispersion. The average number of photons per pulse in horizontal and vertical components at the optical fiber channel output is given by:

$$\begin{cases} n_{\mathrm{H}_F}(t) = & n_{\mathrm{H}_0}(t) \mid \mathrm{R_{F(11)}}(\gamma(t)) R_{11}(\delta_{\mathrm{in}}(t), \alpha_{\mathrm{in}}(t)) \\ & \quad + \mathrm{R_{F(12)}}(\gamma(t)) R_{21}(\delta_{\mathrm{in}}(t), \alpha_{\mathrm{in}}(t)) \mid^2 e^{-\alpha_F L_F} \\ n_{\mathrm{V}_F}(t) = & n_{\mathrm{H}_0}(t) \mid \mathrm{R_{F(21)}}(\gamma(t)) R_{11}(\delta_{\mathrm{in}}(t), \alpha_{\mathrm{in}}(t)) \\ & \quad + \mathrm{R_{F(22)}}(\gamma(t)) R_{21}(\delta_{\mathrm{in}}(t), \alpha_{\mathrm{in}}(t)) \mid^2 e^{-\alpha_F L_F}, \end{cases} \tag{4.15}$$

where $n_{\mathrm{H}_F}(t)$ is the average number of photons per pulse in horizontal component at the instant t_k, $n_{\mathrm{V}_F}(t)$ is the average number of photons per pulse in vertical component at the instant t_k. Moreover, in (4.15), α_L is the attenuation coefficient, and L_F is the length of the fiber-optic quantum channel.

4.3.3 Receiver

In the receiver side, the first optical component the polarization encoded single-photons face is EPC2. The EPC2 is the head device of our system, since it is the one responsible for actuating in the modelled system as a compensation of the polarization random drifts occurred throughout the quantum channel. This component is modelled as a concatenation of five wave-plates similar to (4.12), and can be represented as

$$\mathrm{R_{EPC2}} = \begin{bmatrix} J_{11}(t) & J_{12}(t) \\ J_{21}(t) & J_{22}(t) \end{bmatrix}, \tag{4.16}$$

where $J_{ij}(t)$ are the elements of the rotation matrix at each time instant t, resulting from the concatenation of the six wave-plates of EPC2 in Figure 4.1. The first four wave-plates of the EPC2 are used to compensate the polarization random drift suffered by any SOP, while it travels over fiber-optics channel represented by $\mathrm{R_F}$. The fifth wave-plate is used to choose the receiver measurement basis, and the sixth wave-plate is connected to birefringence zero. Besides optical fiber birefringence we also consider the attenuation suffered throughout the fiber-optics quantum channel, and in this way the number of photons in each main axis after EPC2 can be written as

$$\begin{bmatrix} n_{\mathrm{H}_1}(t) \\ n_{\mathrm{V}_1}(t) \end{bmatrix} = e^{-\alpha_L L_F} \mathrm{R^H_{EPC2}} \mathrm{R_{EPC2}} \mathbb{E}\left[\mathrm{R^H_F}(t)\mathrm{R_F}(t+1)\right] \mathrm{R^H_{EPC1}} \mathrm{R_{EPC1}} \begin{bmatrix} n_{\mathrm{H}_0}(t) \\ 0 \end{bmatrix}, \tag{4.17}$$

where n_{H_1} and n_{V_1} represent the average number of photons per pulse at polarization beam splitter output, see Figure 4.1, and $\mathbb{E}\left[\cdot\right]$ denotes the expected value.

$$\begin{cases} \sigma^2_{H_1} & = \langle \hat{c}^\dagger_H(t)\hat{c}_H(t)\hat{c}^\dagger_H(t)\hat{c}_H(t)\rangle - \langle \hat{c}^\dagger_H(t)\hat{c}_H(t)\rangle^2 \\ \sigma^2_{V_1} & = \langle \hat{c}^\dagger_V(t)\hat{c}^{(}_V t)\hat{c}^\dagger_V(t)\hat{c}^{(}_V t)\rangle - \langle \hat{c}^\dagger_V(t)\hat{c}^{(}_V t)\rangle^2 \end{cases}, \tag{4.18}$$

where $\hat{c}^\dagger_{[\cdot]}$ denotes the creation operator and $\hat{c}_{[\cdot]}$ the annihilation operator. Since $[\hat{c}(t), \hat{c}^\dagger(t)] = 1$,

$$\hat{c}(t)\hat{c}^\dagger(t) = 1 + \hat{c}^\dagger(t)\hat{c}(t), \tag{4.19}$$

and 4.18 can be written as

$$\begin{cases} \sigma^2_{H_1} & = \langle \hat{c}^\dagger_H(t)\hat{c}^\dagger_H(t)\hat{c}_H(t)\hat{c}_H(t)\rangle + \langle \hat{c}^\dagger_H(t)\hat{c}_H(t)\rangle - \langle \hat{c}^\dagger_H(t)\hat{c}_H(t)\rangle^2 \\ \sigma^2_{V_1} & = \langle \hat{c}^\dagger_V(t)\hat{c}^\dagger_V(t)\hat{c}_V(t)\hat{c}_V(t)\rangle + \langle \hat{c}^\dagger_V(t)\hat{c}_V(t)\rangle - \langle \hat{c}^\dagger_V(t)\hat{c}_V(t)\rangle^2 \end{cases}. \tag{4.20}$$

In detail,

$$\begin{aligned} \langle \hat{c}^\dagger_H(t)\hat{c}^\dagger_H(t)\hat{c}_H(t)\hat{c}_H(t)\rangle = & \langle \mid [\mathrm{R}_{\mathrm{EPC2}}\{1,1\}(t)\mathrm{R}_{\mathrm{F}}\{1,1\}(t) + \mathrm{R}_{\mathrm{EPC2}}\{1,2\}(t)\mathrm{R}_{\mathrm{F}}\{2,1\}(t)] \\ & \mathrm{R}_{\mathrm{EPC1}}\{1,1\}(t)[\mathrm{R}_{\mathrm{EPC2}}\{1,1\}(t)\mathrm{R}_{\mathrm{F}}\{1,2\}(t) + \mathrm{R}_{\mathrm{EPC2}}\{1,2\}(t) \\ & \mathrm{R}_{\mathrm{F}}\{2,2\}(t)]\mathrm{R}_{\mathrm{EPC1}}\{2,1\}(t) \mid^4 \langle \hat{a}^\dagger_H(t)\hat{a}^\dagger_H(t)\hat{a}_H(t)\hat{a}_H(t)\rangle, \end{aligned} \tag{4.21}$$

and

$$\begin{aligned} \langle \hat{c}^\dagger_V(t)\hat{c}^\dagger_V(t)\hat{c}_V(t)\hat{c}_V(t)\rangle = & \langle \mid [\mathrm{R}_{\mathrm{EPC2}}\{2,1\}(t)\mathrm{R}_{\mathrm{F}}\{1,1\}(t) + \mathrm{R}_{\mathrm{EPC2}}\{2,2\}(t)\mathrm{R}_{\mathrm{F}}\{2,1\}(t)] \\ & \mathrm{R}_{\mathrm{EPC1}}\{1,1\}(t)[\mathrm{R}_{\mathrm{EPC2}}\{2,1\}(t)\mathrm{R}_{\mathrm{F}}\{1,2\}(t) + \mathrm{R}_{\mathrm{EPC2}}\{2,2\}(t) \\ & \mathrm{R}_{\mathrm{F}}\{2,2\}(t)]\mathrm{R}_{\mathrm{EPC1}}\{2,1\}(t) \mid^4 \langle \hat{a}^\dagger_H(t)\hat{a}^\dagger_H(t)\hat{a}_H(t)\hat{a}_H(t)\rangle. \end{aligned} \tag{4.22}$$

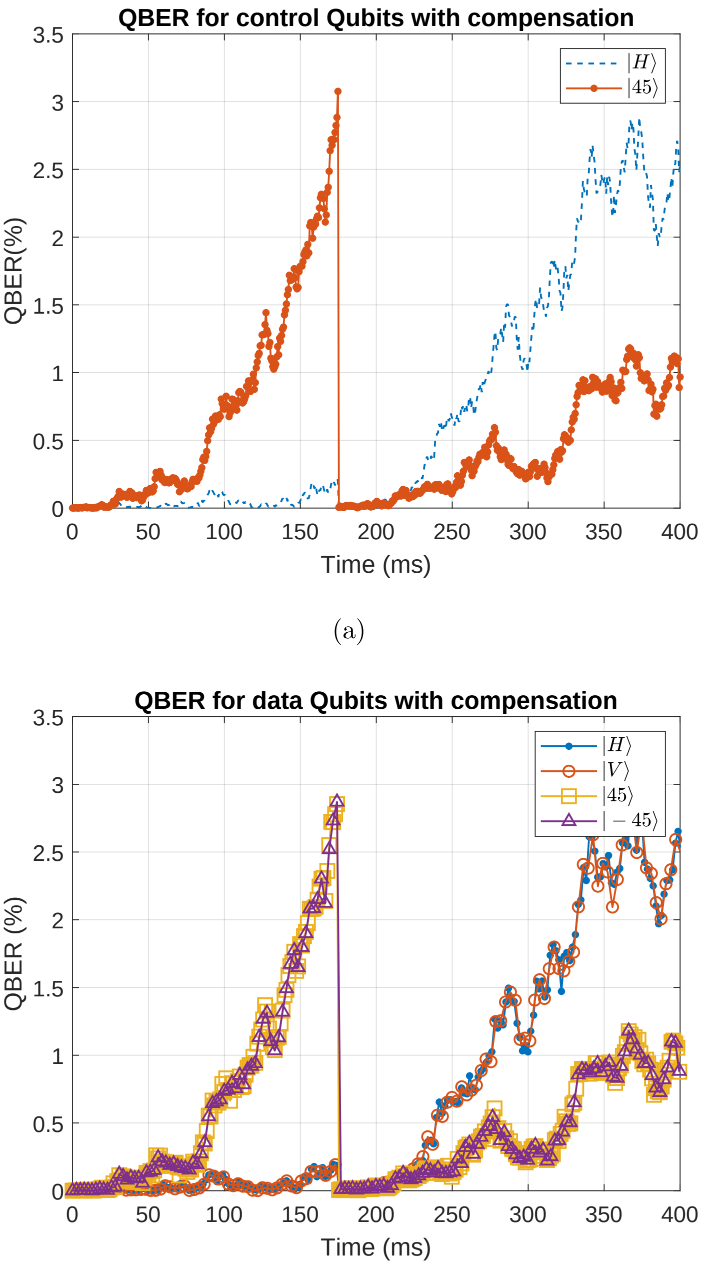
Considering that $\langle \hat{a}^\dagger_H(t)\hat{a}^\dagger_H(t)\hat{a}_H(t)\hat{a}_H(t)\rangle = \phi_0^2$, (4.20) can be written as the average number of photons per pulse at each time instant,

$$\begin{cases} \sigma^2_{H_1} & = \langle \hat{c}^\dagger_H(t)\hat{c}_H(t)\rangle^2 = \langle \hat{n}_1(t)\rangle \\ \sigma^2_{V_1} & = \langle \hat{c}^\dagger_V(t)\hat{c}_V(t)\rangle^2 = \langle \hat{n}_2(t)\rangle \end{cases}. \tag{4.23}$$

In chapter 3, an algorithm to find the reversal operator for a particular SOP was presented [27]. Here, we present a more comprehensive method for compensating the drift of any arbitrary SOP during continuous transmission of polarization states while a QKD protocol is running. The proposed method assures that polarization rotations induce by matrix R_{F} are reverted after the EPC2, see Figure 4.1. Every wave-plate has a particular role in the measurement scheme, assuring the polarization drift compensation by the first four wave-plates as described in Figure 4.4, and the basis choice by the fifth wave-plate.

4.4 Method Validation

In this section, we present numerical results to demonstrate the effectiveness of the proposed method to compensate the polarization random drift suffered by an arbitrary SOP along the fiber-optics quantum channel.



(a)

(b)

Figure 4.5: (a) QBER for two non-orthogonal states with the random drift compensation method as a function of time. (b) QBER evolution with time for the data qubits for each of the four SOPs.

4.4.1 Assuming an Ideal Receiver

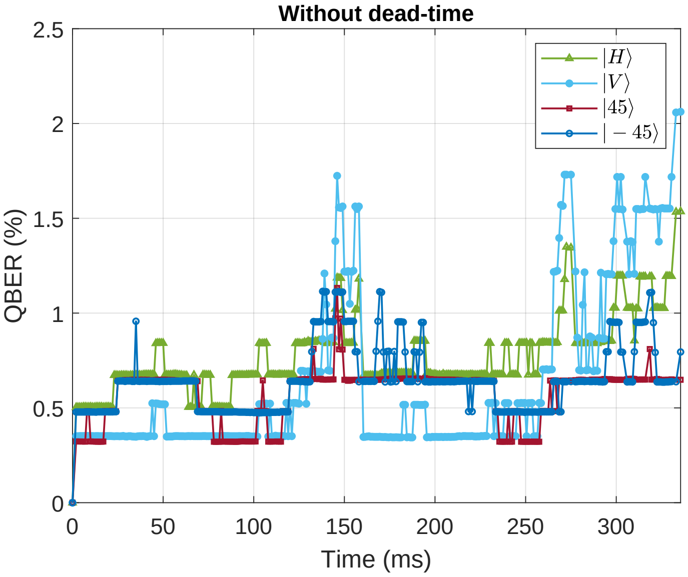
The QBER has two main contributions, the QBER resulted from channel errors induced by polarization random drift (QBER$_{pol}$) [27] [78], and the QBER resulted from single-photon detectors imperfections such as dark-counts, detectors efficiency or after-pulses (QBER$_{det}$) [13].

Lets start taking only into account the QBER resulted by polarization random drift, in order to demonstrate that with the proposed method we can compensate the polarization drift of any SOP looking only into the QBER calculated for two of the four required SOPs, since they belong to mutually unbiased bases [77]. Control frame is composed by the two mutually unbiased states of polarization $|H\rangle$ and $|45\rangle$, and the data frame is composed by the four random states of polarization belonging to two non orthogonal bases considering in the simulation. Considering the study case presented in Figure 4.1, we present numerical results for polarization drift compensation method validation. Note that the control qubits are chosen by the user with a determined position on the frame and previously known by both parties. The data and control qubits are both implemented using a 0.2 average number of photons per pulse. In this subsection, we use a $\Delta_p = 4 \times 10^{-8}$, a symbol repetition rate of 100 MHz, and a QBER$_{th} = 3.0\%$.

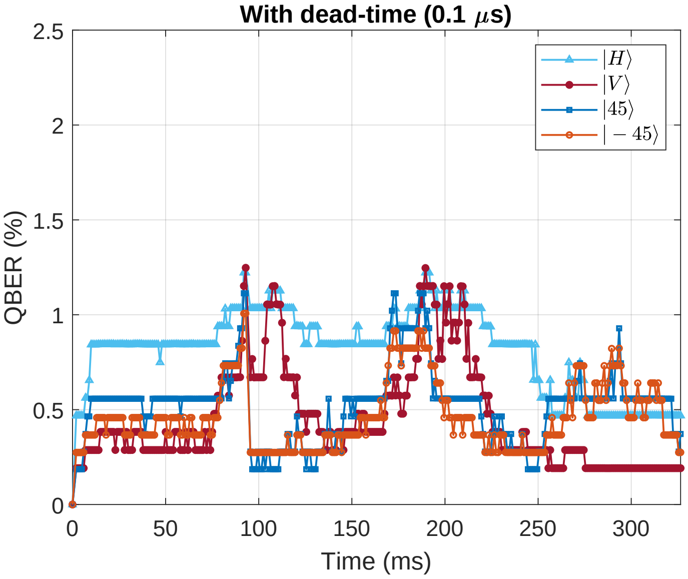
Figure 4.5 (a) shows the individual QBER evolution for control qubits, $|H\rangle$ and $|45\rangle$. The first SOP to be compensated was $|45\rangle$ since, as one can see in Figure4.5, the QBER associate with this SOP is the first to reach the predefined QBER$_{th}$. The polarization random drift compensation occurred at 175 ms, and one can see that both QBER$_{|H\rangle}$ and QBER$_{|45\rangle}$ decrease approaching the zero bound. Also, looking into Figure4.5 (b), where the QBER of the four BB84 SOP are presented, they also decrease approaching zero at the time of polarization compensation.

4.4.2 Assuming a Realistic Receiver

Once the effectiveness of the proposed polarization drift compensation method has been demonstrated considering a perfect receiver, we will now consider the effects of the single-photon detectors dark-counts, and detection efficiency. Besides polarization random drift, we also consider the fiber-optic channel attenuation of 0.2 dB/km. In this subsection we consider an average number of photons per pulse of 0.2 at transmitter output for data qubits, and at receiver input for control qubits, a channel length of 40 km, a polarization line-width of $\Delta_p = 2 \times 10^{-8}$, a symbol repetition rate of 100 MHz, and a QBER$_{th} = 1.0\%$ on control qubits. Note that the length of control and data frames had to be increased since with the addition of the dead time later, the number of photons that are effectively measured decreased. In this way, a lower threshold had to be also defined to guarantee a QBER on data qubits is maintained bellow 2.1%. We divided the transmitted frame in 50000 control qubits and 50000 data qubits. Again, the control qubits frame is a predefined sequence of $|H\rangle$ and $|45\rangle$, and the data frame is a random sequence that includes the four SOP. Figure 4.6 (a) shows the data qubits QBER of each one of the four SOP used in this work, considering single-photon detectors efficiency of 25% and a dark-count probability of 5×10^{-4}. The polarization compensation method actuated three times in this session. The QBER does not returned to zero since there are other error sources apart from the polarization random drift. Figure 4.6 (b) shows the QBER of each one of the four SOP considering a 0.1μs dead-time of single-photon detectors. In this case, the average QBER is higher than the previous case as expected, since one more error source was added because the correlation time between samples was decreased. Nevertheless, in both cases presented in Figure 4.6 we observe the robustness of our algorithm, since in both cases we observe a QBER for the data qubits lower than 2.1%. Furthermore, a system parameter that has impact on the polarization random drift compensation method performance is the single-photon detectors dead-time. We consider the single-photon detectors are operating in gated mode, and the dead-time holds-off consecutive



(a)



(b)

Figure 4.6: QBER time evolution for data qubits, considering a dark count probability of 5×10^{-4} , a detection efficiency of 25%, and a dead-time of: a) - dead time null; b) - dead time equal to $0.1\mu s$. An average QBER of 0.59% and 0.65% was calculated in a) and b), respectively.

gates maintaining the bias voltage of the avalanche photo-diode well bellow the breakdown voltage [53]. The dead-time increases the time interval between consecutive samples, which can lead to uncorrelated consecutive samples [17].

4.5 Case Study: BB84

In this section, we include the polarization random drift compensation method in a realistic QKD system, where the BB84 protocol is implemented [12].

4.5.1 Comparative Analysis With a Non-automatic Compensation Method

Lets assume a system that implements the BB84 protocol with polarization encoded single-photons using the linear and diagonal bases. In this case, we use a 5×10^4 qubits control frame with an alternated sequence of two mutually unbiased states of polarization, $|H\rangle$ and $|45\rangle$, and a 5×10^4 qubits data frame with the four randomly generated states of polarization from two non-orthogonal bases. For the method actuation boundary we chose a $\text{QBER}_{th} = 1\%$. The sifted key is obtained from the events in which both Alice and Bob prepare and measure the qubits with the same basis, i.e. the sifted key is the key generated after basis reconciliation. The polarization control algorithm uses M bits of the sifted key (obtained after basis reconciliation) to estimate the sifted key QBER, and we call this procedure data check. After data check and discard the bits used for that step, a secret key is obtained. Figure 4.7 shows the QBER estimated using 1000 bits of the obtained sifted key when 50000 data qubits are transmitted. The qubits are prepared using an average of $\mu = 0.2$ photons per pulse and were exchanged throughout a quantum channel with $L = 40$ km length. The qubits measurement is performed using single-photon detectors with 25% efficiency, a dark-count probability of $P_{\text{dc}} = 5 \times 10^{-4}$ and a dead-time of $0.1\mu s$. As we can see in Figure 4.7, the QBER without the proposed polarization compensation method increases with time, readily surpassing the security bound for the BB84 protocol which is close to 11% [97].

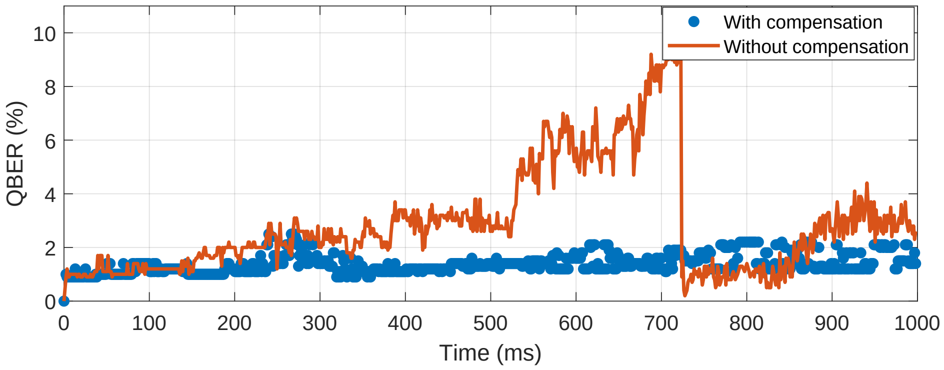


Figure 4.7: QBER estimated using 1000 bits extracted from the sifted key with and without the actuation of the polarization random drift compensation method over time. The average number of photons per pulse at transmitter output is $\mu = 0.2$. The channel length between transmitter and receiver is $L = 40$ km with attenuation of 0.2 dB/km. The dark-count probability of single-photon detectors is $P_{\text{dc}} = 5 \times 10^{-4}$, and the dead-time of $0.1\mu s$.

We assume here that as soon as the QBER reaches the security boundary imposed by the protocol, an instantaneous compensation occurs. This is the best scenario we can consider for a compensation method, i.e. an instantaneous compensation time. On the contrary, the QBER using the proposed compensation method remains stable with a QBER lower than 2%. In this way, even consuming 50% of extra bandwidth, the proposed method provides long-term key exchange between parties with an error bellow 2%.

4.5.2 Impact of Finite-key Size Effects on Compensation Method Performance

We now analyze the length of the secret key as a function of the total number of transmitted qubits, including control and data qubits. For each session that produces non-zero secret key, we recorded the length of the sifted key, the number of control and data transmitted qubits, and the sifted key error rate. Finite-key unconditional security boundaries are used for the BB84 protocol for a practical prepare and measure implementation [98].

A set of sessions was recorded considering three different distances for the fiber-optics quantum channel, with and without the polarization random drift compensation method. We now analyze the numerical results taking into account the finite-key unconditional security boundaries defined for BB84 protocol prepare and measure implementations [99]. We adapt the equation (4.24) presented in [100] to our case study, being the length of the final secret key defined as

$$\ell \leq NA\left(1-\mathcal{H}\left(\frac{\tilde{E}}{A}\right)\right)-N\text{leak}_{\text{EC}}-7N\sqrt{\frac{1}{N}}\log_2\left(\frac{2}{\bar{\varepsilon}}\right)-2\log_2\left(\frac{1}{\varepsilon_{\text{PA}}}\right)-\log_2\left(\frac{2}{\varepsilon_{\text{EC}}}\right), \quad (4.24)$$

where N is the sifted key recorded length before error correction, and $\mathcal{H}$ denotes the binary Shannon entropy. The security parameter $\varepsilon = \varepsilon_{\text{PE}} + \tilde{\varepsilon} + \varepsilon_{\text{PA}} + \varepsilon_{\text{EC}}$ is considered to be 10^{-10} during all recorded sessions [100], and each term is optimized during simulation [97]. Note that $\tilde{\varepsilon}$ denotes the probability that Eve's information is underestimated, ε_{PA} is the collision probability of an hash function, and ε_{EC} is the probability of failure in error correction leaves non-zero number of errors. Lets assume the QBER estimated from the sifted key with size N may have deviated from the actual value, and it is defined as

$$\tilde{E} = \text{QBER}_{\text{sifted}} + \frac{1}{2}\sqrt{\{2\ln(1/\varepsilon_{\text{PE}}) + 2\ln(N+1)\}(1/N)}, \quad (4.25)$$

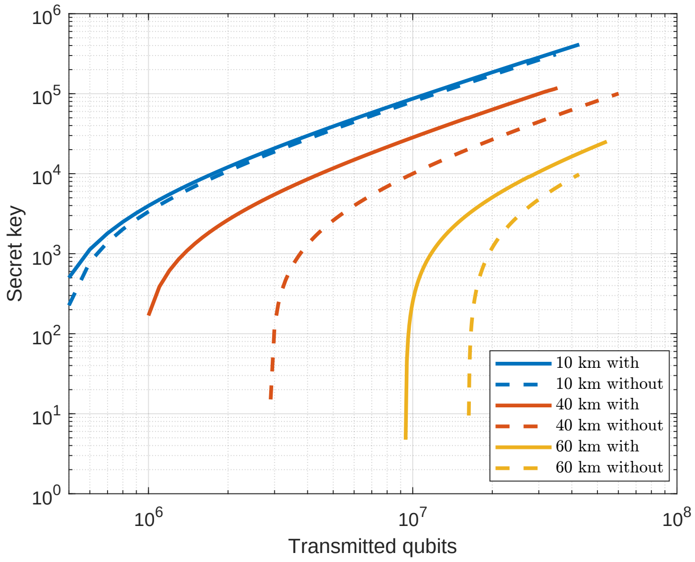
where ε_{PE} is the probability of deviation occurrence, and $\text{QBER}_{\text{sifted}}$ is the observed QBER estimated from part of the sifted key [100]. Lets also consider the probability of having more than one photon in a weak laser pulse prepared by Alice during raw key exchange, p_{multi}. A correction term for the weak laser multi-photon probability should be added in single-photon detection probability

$$A = (p_{\text{det}} - p_{\text{multi}})/p_{\text{det}}, \quad (4.26)$$

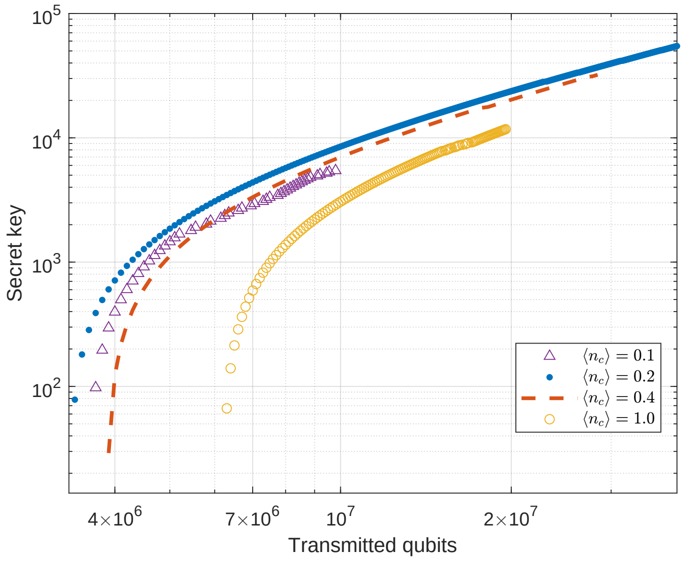
where p_{det} is the single-photon detection probability [97]. Another parameter of interest is the the estimated portion of key disclosed during error correction,

$$\text{leak}_{\text{EC}} = f_{\text{EC}}\mathcal{H}(\text{QBER}_{\text{sifted}}), \quad (4.27)$$

where $\mathcal{H}(\text{QBER}_{\text{sifted}})$ is the minimum part of the key with an error rate of $\text{QBER}_{\text{sifted}}$ required to be disclosed to correct all the errors. A $f_{\text{EC}} = 1.16$ as practical efficiency of error correction is considered [97].



(a)



(b)

Figure 4.8: Secret key length versus total number of transmitted qubits. (a) Numerical results for different fiber-optic channel lengths with and without polarization compensation method. (b) Numerical results for different average number of photons per pulse in control frame at the receiver input for a 40 km fiber-optics quantum channel.

Figure 4.8 (a) shows the secret key length versus the total number of transmitted qubits for three different distances, with and without the actuation of the polarization random drift compensation method. As the fiber-optics quantum channel length increases the secret key generation is less efficient. However, for higher distances such as 40 km and 60 km the use of the polarization random drift compensation method considerably improves the efficiency of secret key generation since the average quantum bit error rate decreases. Figure 4.8 (b) shows the secret key length versus the total number of transmitted qubits for different average number of photons per pulse in control qubits at the receiver input for a 40 km fiber-optic quantum channel. From the results in Figure 4.8 (b), we can see that for $\mu = 0.2$ in the data qubits, the most efficient average number of photons in the control bits at receiver input is $\langle n_c \rangle = 0.2$. Note that all curves in Fig. 4.8 (a) and (b) were obtained over the same time window acquisition. In Fig. 4.8 (a), the curves that represent the "with compensation" correspond to scenarios where the QBER never reaches the limit defined by BB84 to produce a secret key, which means that even increasing the time window under analysis a secret key is continuously produced over long time. On the contrary, the curves that represents the "without compensation" correspond to scenarios where the QBER eventually reaches the limit imposed by BB84 to produce a secret key, and with an increasing of the time window the system eventually stops to produces a secret key even the qubits are transmitted over long time. In this way, a secret key improvement can be calculated taking into account a certain time window.

4.5.3 Bandwidth Consumption Analysis

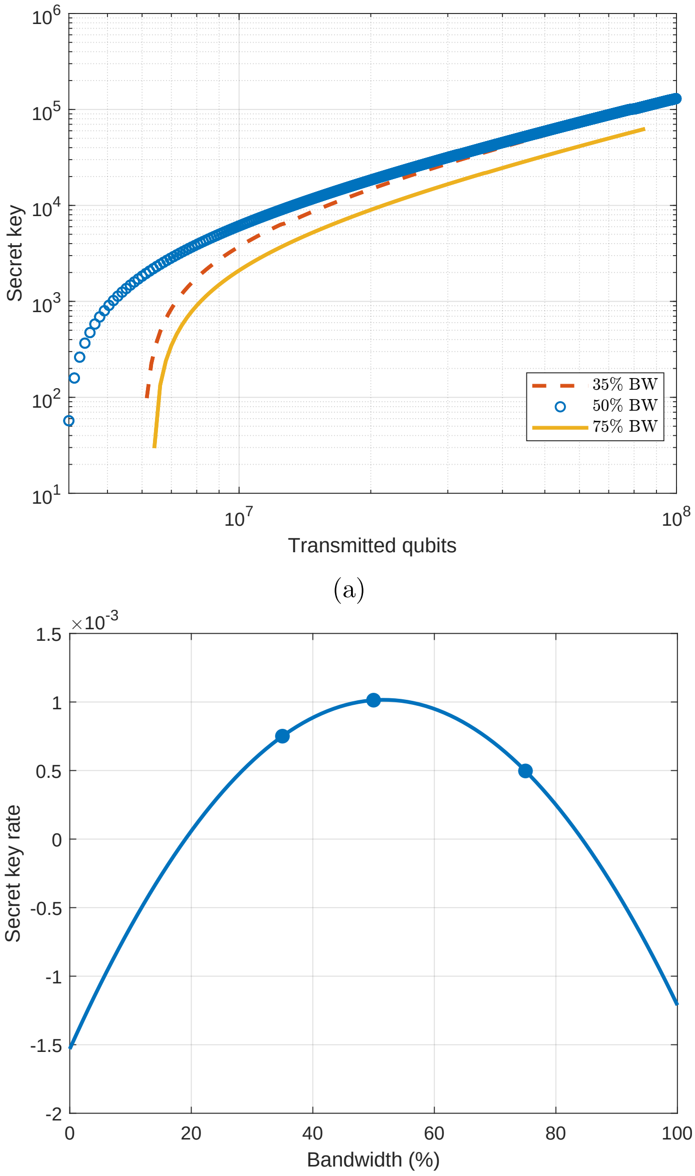
One important assessment measurement is the bandwidth consumption of the proposed polarization random drift compensation method. Here, we also present the final secret key length versus the total transmitted qubits. Figure 4.9 (a) shows the secret key length as a function of the total transmitted qubits for different polarization random drift compensation method bandwidth consumption. The bandwidth consumption of 50% is the most advantageous since the secret key generation is more efficient requiring less transmitted qubits to generate a final secret key with the same size. Figure 4.9 (b) shows the secret key ratio, calculated by dividing the secret key length by the total transmitted qubits required to generate it, versus the bandwidth consumption. Similarly, the most advantageous is the 50% bandwidth consumption since provides the highest secret key ratio. The reason for this is related to the polarization compensation method capacity of maintaining the lowest QBER when comparing with other bandwidth consumption. Even consuming 50% bandwidth less qubits needed to be transmitted to generate a secret key because the error correction codes are more efficient requiring less qubits to correct the errors.

4.6 Final Remarks

We presented a polarization random drift compensation method able to compensate arbitrary SOP time drifts of any SOP induced by the propagation over standard fiber-optic channel. We demonstrated that only monitoring the QBER induced by two qubits prepared in mutually unbiased bases, the proposed method is able to compensate the BB84 QKD SOPs.

Moreover, we have shown that the implementation of the proposed method in discrete-variables polarization encoded based systems assures a long-term key exchanging between parties with a QBER lower than 2%. Furthermore, the compensation method provides an average QBER bellow 2% for a realistic system with a 40 km fiber-optics quantum channel, and average number of photons per pulse of 0.2 at the transmitter output in the data frame, and 0.2 at receiver's input in the control frame. This QBER value is lower than a half of a system with no compensation method, which strongly impacts the secure key generation efficiency in BB84 protocol.

We have demonstrated that by employing the proposed method in a finite-key implementation, the secret key rate generation is improved in 82%, even consuming part of the transmission bandwidth for polarization random drift compensation. To obtain this result, we divided the average secret key length, resulted from the case where no polarization compensation method was applied, by the average secret key length, resulted from the case where the proposed method was applied. Note that to obtain the secret key length in all situations we always used the same time transmission window. Regarding the bandwidth consumption, we analysed the secret key ratio for different bandwidths, and this analysis allowed us to



(b)

Figure 4.9: (a) Secret key length versus total transmitted qubits for three different polarization random drift compensation method bandwidth consumption. A fiber-optics quantum channel with 40 km is considered. (b) Secret key ratio versus bandwidth. The secret key ratio is calculated in relation to the total transmitted qubits.

conclude that the optimum value for bandwidth consumption is 50%, being the efficiency of BB84 higher for this value.

Chapter 5

Coherent Detection for DV-QKD

In this chapter, we propose a novel polarization-based DV-QKD system that combines the use of phase-modulators to SOP generation and basis switching with a polarization diversity coherent detection scheme. This enables a full implementation of DV-QKD systems using only telecom-grade material.

This chapter contains 6 sections. In section 5.1 the current state of the art is presented. In section 5.2, we detail the theoretical model of the proposed polarization based DV-QKD system. In section 5.3,we detail the DV-QKD BB84 protocol implementation in the proposed system. In section 5.4, the method for polarization compensation is detailed and assessed. In section 5.5, we assess the performance of BB84 protocol in a finite-key size implementation using thresholds to operate the proposed system in counting mode. Finally, in section 5.6 the final remarks are summarized.

5.1 State of The Art

QKD protocols can be implemented following two fundamental approaches. In DV-QKD, information is encoded in one (or more) degree-of-freedom of individual photons, which leads to a discrete measurement outcome [15]. Assuring compatibility with current telecommunication infrastructures, CV-QKD schemes use multi-photon quantum states of light encoding the bits using observables with the continuous variables such as the phase and amplitude of coherent states [14]. DV-QKD schemes have been experimentally demonstrated over long distances [41] [61], and present more mature security proofs taking into account system imperfections and finite data size effects [97]. On the other hand, CV-QKD schemes allow to achieve higher transmission rates at short distances on current telecommunication metro networks [52].

Despite some disadvantages of CV-QKD arise mainly from the complexity of information reconciliation steps [14], their compatibility with classical detection hardware poses a major advantage against current single-photon avalanche based detection schemes required for the DV-QKD, which limits on the achievable performance and work at very-low temperatures demanding additional cooling systems [53]. More recently, a detection scheme to determine the photon number statistics of an input quantum state using conjugate homodyne detection without controlling the phase of the input quantum state was proposed [101]. The photon number statistics is one of the research tasks on quantum tomography [102], where homodyne detection has been being implemented for that purpose [103]. Later, a DV-QKD implementation was presented using a conjugate homodyne detection scheme that operates in counting mode. This detection scheme consists on a PBS followed by two optical homodyne detectors, which allows the measurement of a pair of quadratures of the input quantum state [104]. Although most of the homodyne detection schemes used to decode single-photons assume ideal single-photon sources, an hybrid solution based on decoy-state and homodyne detection was proposed in [105], where the local oscillator phase is randomised being no need to distribute a common phase reference between transmitter and receiver. Due to the non-practical conditions required to create ideal single-photon sources, experimental DV-QKD is implemented using coherent state sources highly attenuated to an average number of 0.1 photons per pulse [13]. Moreover, the switching between SOPs using phase modulators allows SOP generation rates in the order of GHz [39]. Current state-of-the-art reports a BB84 quantum states generation at 5 GHz pulse repetition rate over 151.5 km using a phase modulator to encode quantum information on single-photons polarization, achieving a final secret key rate of 54.5 kbps [39]. This kind of technique provides optical pulse modulation only limited by the acceptance bandwidth of the phase modulators and its extinction ratio [106].

5.2 DV-QKD Polarization Diversity Coherent Detection

In this section, we propose the quantum communication system shown in Figure 5.1 to implement the BB84 protocol. The proposed system combines the usage of phase modulators to generate quantum polarized states with a polarization diversity coherent detection scheme. Moreover, we also present the theoretical model of the proposed polarization based DV-QKD system considering the equipment imperfections, such as the birefringence over the optical fiber channel, non-ideal single-photon sources, and thermal and shot noise in the detection scheme. The transmitter, usually known as Alice, randomly generates the BB84 states using phase-randomised weak coherent pulses. On the other hand, the receiver, usually known as Bob, performs random quadrature measurements. Figure 5.1 shows the schematic representation of the proposed polarization based DV-QKD transmission system, which is divided in

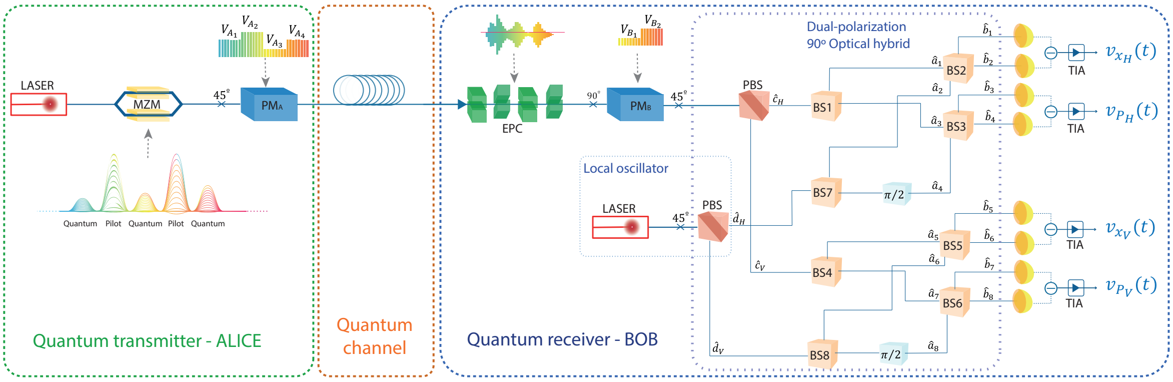


Figure 5.1: Schematic representation of the DV-QKD system based on polarization diversity coherent detection. [MZM] denotes the Mach-Zehender amplitude modulator, [PM$_\mathrm{A}$] and [PM$_\mathrm{B}$] the phase-modulators of Alice and Bob, respectively, [EPC] the electronic polarization controller, [PBS] the polarization beam-splitters, [BS] the beam-splitters, and [TIA] the trans-impedance amplifiers.

three parts namely Alice, the quantum channel, and Bob. This section is divided in three sub-sections comprising the three main parts of the system. In the first sub-section, we present the theoretical model that describes the polarization state preparation by Alice. Next, we briefly describe the theoretical model used to simulate the polarization mode dispersion over the quantum channel. Finally, in the last sub-section we describe the theoretical model that describe the polarization state measurements technique used by Bob.

5.2.1 Polarization State Preparation

Alice generates the BB84 polarization states by combining a weak coherent optical signal source, as an approximation to a true single-photon source, with a phase-modulator to switch between the four possible states of polarization. In order to increase security avoiding for instance photon number splitting attacks to this photon source, the security could be increased significantly if we also implement a decoy-state protocol. Please note that, in literature it was already proved that the use of a weak-coherent optical signal in the DV-QKD BB84 protocol implemented together with a decoy-state protocol leads to an unconditional secure QKD implementation. The polarization state preparation scheme consists of a single-laser source followed by a Mach-Zehender (MZM) amplitude modulator, and a phase modulator ([PM$_\mathrm{A}$). Alice applies time-division multiplexing techniques to transmit pulses with different amplitudes by switching between two voltage levels on consecutive pulses of the signal that drives the MZM, see Figure 5.1. One of those levels correspond to the high power pilot tone, which is sent to enable the use of a locally generated local oscillator and to reverse the polarization random drift that the photons suffers during its evolution over the quantum channel. The other voltage level corresponds to the weak coherent optical signal in such a way to obtain 0.1 photons per pulse on average, which corresponds to the information carried by the quantum state. The MZM outputs a well defined horizontal polarized optical pulse that can be defined by [107],

$$\hat{a}_{\mathrm{in}_H}(t) = \sqrt{\eta_{\mathrm{MZM}}(t - nT_s)}\hat{a}_{0_H} e^{i(\omega_s t + \phi_{s_N}(t))} h(t - nT_s), \tag{5.1}$$

where $\eta_{MZM}(t - nT_s)$ is the MZM efficiency over the symbol duration (T_s) of each pulse with symbol number n, $\hat{a}_{0_H}$ denotes the annihilation quantum operator of a coherent state of a single-mode laser [108], ω_s is the optical frequency of the quantum signal, $\phi_{s_N}(t)$ is the initial unknown optical phase of the laser, and $h(t - nT_s)$ denotes the impulse response of MZM [109]. Please note that we consider that the polarization state at the laser optical signal output is a well defined horizontal polarization state. In this work we consider a return-to-zero pulse with 50% duty cycle. From (5.1), we can define the the average number of photons per quantum pulse, $\langle n_Q \rangle = \langle \alpha_L | \hat{a}^\dagger_{\mathrm{in}_H}(t) \hat{a}_{\mathrm{in}_H}(t) | \alpha_L \rangle$ being $|\alpha_L\rangle$ the coherent state describing the laser field [108], given by

$$\langle n_Q \rangle = |\alpha_s|^2 \eta_{MZM}(t - nT_s) \int_{\frac{T_s}{2}(2n-1)}^{\frac{T_s}{2}(2n+1)} dt |h(t - nT_s)|^2, \tag{5.2}$$

where, $|\alpha_s|^2 = P_s/(\hbar\omega_s)$ is the time-independent optical photon flux at laser output, being P_s the optical power at laser output and $\hbar$ the reduced Plank constant. Note that for $\eta_{MZM}(t - \ nT_s) \ = 1$ implies that we are generating a pilot tone. However, for $\eta_{MZM}(t - nT_s) \ll 1$, we are operating in a quantum regime and in that case we are generating the quantum signals for QKD implementation.

Following the MZM in Figure 5.1, the PM$_A$ which represents the phase modulator and is responsible for polarization modulation. The phase modulator has at the input polarization maintaining optical fiber oriented ate 45° with respect to the optical axis, which results in the two orthogonal equal amplitude polarization components of the electromagnetic field to propagate in the crystal experience different refractive indexes, which are proportional to the voltage applied on the phase modulator [69]. We can switch between four states of polarization by applying four different voltages, in particular 0, V_π, $V_{\pi/2}$, $-V_{\pi/2}$ to obtain $|45°\rangle$, $|-45°\rangle$, $|RC\rangle$, and $|LC\rangle$, respectively [69]. In this work we assume the polarization dispersion loss (PDL) effects in the phase modulator, which is defined as the ratio between the maximum over the minimum optical transmission coefficient, ϵ_{PDL}. The maximum transmission is assumed to be 1. In this way, ϵ_{PDL} corresponds to the minimum transmission, with $\text{PDL}_{dB} = 10 \log 1/\epsilon_{\text{PDL}}$ [110]. The two orthogonal amplitude polarization components of the electromagnetic field at Alice output can be defined in terms of quantum operator as [82, 107, 108],

$$\begin{cases} \hat{a}_{A_H}(t) = \frac{1}{\sqrt{2}} e^{i\frac{V_A(t-nT_s)}{V_\pi}\pi} \Big(\hat{a}_{in_H}(t) - \hat{a}_{in_V}(t)\Big) \\ \hat{a}_{A_V}(t) = \frac{1}{\sqrt{2}} \Big(\hat{a}_{in_H}(t) - \hat{a}_{in_V}(t)\Big) \sqrt{\epsilon_{\text{PDL}}}, \end{cases} \tag{5.3}$$

where $V_A(t - nT_s)$ is the voltage applied on the phase-modulator PM$_A$ to generate one of the four BB84 polarization states, V_π is the voltage needed to apply a phase difference of π on the phase-modulator, and $\hat{a}_{in_V}$ corresponds to annihilation operator for the vertical polarization state at phase modulator output, which is in a vacuum state since, the laser is assumed to emit photons only over the horizontal polarization state.

5.2.2 Transmission of the Polarization States over an Optical Channel

The quantum channel is assuming to be a standard optical fiber. We consider the polarization mode dispersion (PMD) following the work presented in [75]. The PMD degrades the transmitted state of polarization inducing random drift polarization due birefringence inherent of the standard optical fiber channel. Polarization states change accordingly with a random matrix parameterized by the random parameters $\gamma_n = (\gamma_1, \gamma_2, \gamma_3)$ generated at each instant, where $\gamma_n = \psi \mathbf{a}$, with length $\psi = \|\gamma_n\|$, denoting $\|\cdot\|$ the euclidean norm. The randomness of rotations is defined by γ_n parameters obtained from a normal distribution with mean zero and standard deviation $\sigma^2 = 2\pi\Delta_p T$, being T the total acquisition time and Δ_p the polarization line-width that defines the velocity of the random drift [75]. Therefore, the temporal drift evolution is modelled by concatenating consecutive matrices,

$$\text{M}_\text{F}(\gamma_n) = \mathbf{I} \cos \psi - i \mathbf{a} \cdot \vec{\sigma} \sin \psi, \tag{5.4}$$

where $\vec{\sigma}$ is the tensor of Pauli matrices, $\mathbf{I}$ is a 2×2 identity matrix [75], and $\mathbf{a} = (a_1, a_2, a_3)$ denotes the direction defined in a unitary sphere. We also consider the optical fiber channel losses, which are modelled using the beam-splitter model. The transitivity of the channel is defined as $\tau_{ch} = 10^{-\alpha_L/10}$, where α_L is the dB attenuation coefficient.

5.2.3 Polarization States Measurement

The states of polarization enter on Bob measurement setup and pass through an EPC, that is used to compensates the polarization random drift suffered over the transmission channel. In order to compensate the polarization PDL in PM$_A$, we apply a 90° rotation to the light field before entering in PM$_B$ that follows the EPC in Figure 5.1. The component that passes through the ordinary axis in PM$_A$ crystal follows the extraordinary axis in PM$_B$, and vice-versa [69]. The phase modulator output optical fiber is spliced at 45° applying an inverse rotation of the one performed at PM$_A$ input allowing Bob to decipher the received information correctly [69]. In this work, we assume equal phase modulators in Alice and Bob considering the same characteristics including the same PDL in both. Moreover, Bob must apply two voltage levels on the phase modulator for choosing the measurement basis for turning the states into horizontal and vertical. For instance, $V_{B_1} = 0$ V for measuring in the diagonal basis, and $V_{B_2} = V_{\pi/2}$ V for measuring in the circular basis. After this passing thought PM$_B$ the two annihilation operators for the two orthogonal polarization states Bob's phase modulator output can be written as [82, 107, 111],

$$\begin{aligned}\hat{a}_{B_H}(t) = -\sqrt{\frac{\tau_{ch}}{2}}\left[\mathbf{Z}_{21}(t-nT_s)e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi} + \mathbf{Z}_{11}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\right]\hat{a}_{A_H}(t) - \\ \sqrt{\frac{\tau_{ch}}{2}}\left[\mathbf{Z}_{22}(t-nT_s)e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi}\right. \\ \left. + \mathbf{Z}_{12}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\right]\hat{a}_{A_V}(t) - (\text{terms associated with vacuum operators}), \quad (5.5)\end{aligned}$$

$$\begin{aligned}\hat{a}_{B_V}(t) = -\sqrt{\frac{\tau_{ch}}{2}}\left[\mathbf{Z}_{21}(t-nT_s)e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi} - \mathbf{Z}_{11}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\right]\hat{a}_{A_H}(t) - \\ \sqrt{\frac{\tau_{ch}}{2}}\left[\mathbf{Z}_{22}(t-nT_s)e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi}\right. \\ \left. - \mathbf{Z}_{12}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\right]\hat{a}_{A_V}(t) - (\text{terms associated with vacuum operators}), \quad (5.6)\end{aligned}$$

where $\mathbf{Z}$ is the concatenation of the EPC matrix with M_F, see equation 5.4, τ_{ch} is the transmissivity of the optical fiber which accounts for the fiber loss, and V_B is the voltage applied on PM$_B$ for changing the measurement basis. The terms associated with the vacuum operator are hidden since they do not contribute for the average value neither for variance calculations. At the input of the dual-polarization optical hybrid in Figure 5.1, the quantum signal is mixed with a strong local oscillator for quadrature measurement. The quantum operator for this second laser source that generates the local oscillator can be defined as

$$\hat{a}_{Lo_H}(t) = \left|\bar{a}_{lo_H}\right| e^{i(\omega_{lo}t + \phi_{lo_N}(t))}, \quad (5.7)$$

where $\bar{a}_{lo_H}$ is the (classical) amplitude of the local oscillator laser, ω_{Lo} is the optical frequency of the local oscillator, and ϕ_{Lo} is the optical phase of the local oscillator.

Optical Hybrid Input/Output Relations

Now, we detail the input/output relations of the optical hybrid. Lets detail the relations to obtain the current $\hat{i}_{x_H}(t)$ from the top photo-detectors in Figure 5.2. In this way, the

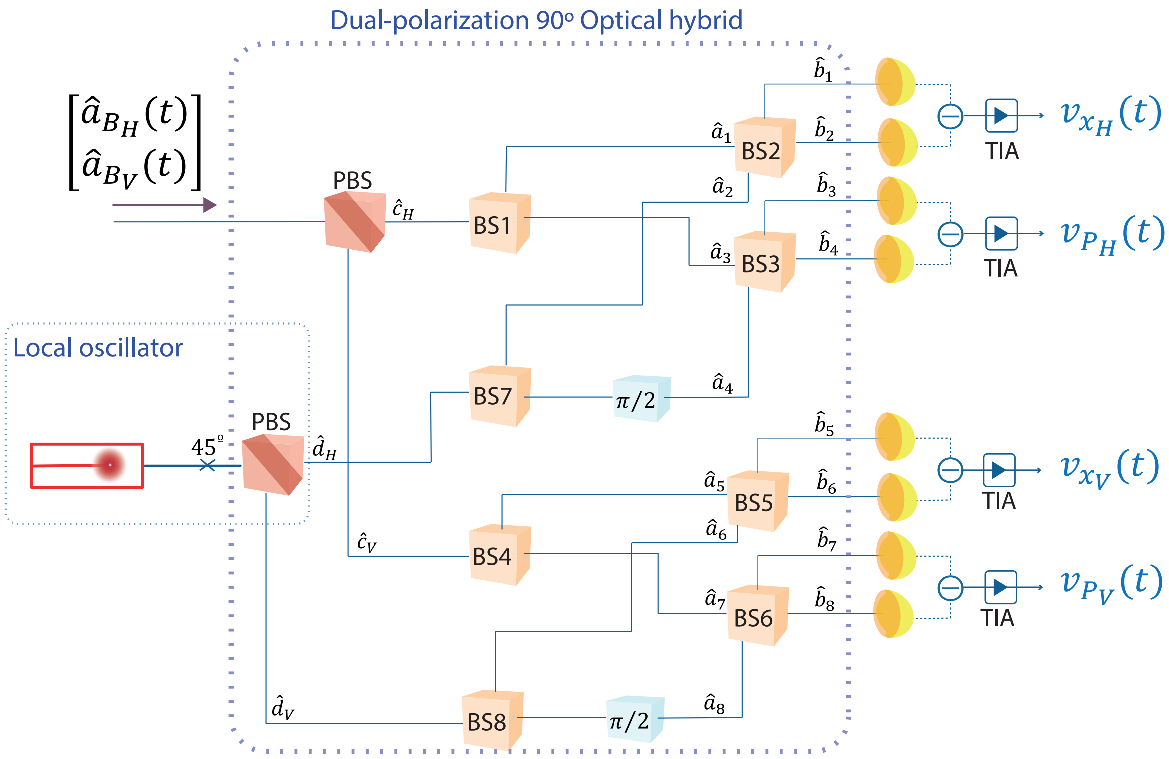


Figure 5.2: Schematic representation of the optical hybrid input/output relations. [PBS] the polarization beam-splitters, [BS] the beam-splitters, and [TIA] the trans-impedance amplifiers.

following relation can be defined

$$\begin{cases}\hat{b}_1(t) = \frac{1}{\sqrt{2}}\left(\hat{a}_1(t) + \hat{a}_2(t)\right)\\ \hat{b}_1(t) = \frac{1}{\sqrt{2}}\left(\hat{a}_1(t) + \hat{a}_2(t)\right).\end{cases} \tag{5.8}$$

From those relations, the current $\hat{i}_{x_H}(t)$ can be given by

$$\hat{i}_{x_H}(t) = q_e\left(\hat{b}_1^\dagger(t)\hat{b}_1(t) - \hat{b}_2^\dagger(t)\hat{b}_2(t)\right) \tag{5.9}$$

$$= q_e\left(\hat{a}_1^\dagger(t)\hat{a}_2(t) + \hat{a}_2^\dagger(t)\hat{a}_1(t)\right). \tag{5.10}$$

Note that the currents $\hat{i}_{P_H}(t)$, $\hat{i}_{x_V}(t)$, and $\hat{i}_{P_V}(t)$ can be readily obtained replacing in 5.2.3 the $\hat{b}_i$ and $\hat{a}_i$ operators by the correspondent ones. For instance, to obtain $\hat{i}_{P_H}(t)$ we should use the $\hat{b}_3$, $\hat{b}_4$, $\hat{a}_3$, and $\hat{a}_4$ operators; to obtain $\hat{i}_{x_V}(t)$ we should use the $\hat{b}_5$, $\hat{b}_6$, $\hat{a}_5$, and $\hat{a}_6$ operators; and finally to obtain $\hat{i}_{P_V}(t)$ we should use the $\hat{b}_7$, $\hat{b}_8$, $\hat{a}_7$, and $\hat{a}_8$ operators. Lets consider the balanced 50:50 beam-splitter model illustrated in Figure 5.3 and the following input/output relations

$$\begin{cases}\hat{b}_1 = \sqrt{\eta}\hat{a}_1 + \sqrt{1-\eta}\hat{a}_2\\ \hat{b}_2 = \sqrt{\eta}\hat{a}_2 - \sqrt{1-\eta}\hat{a}_1\end{cases} \tag{5.11}$$

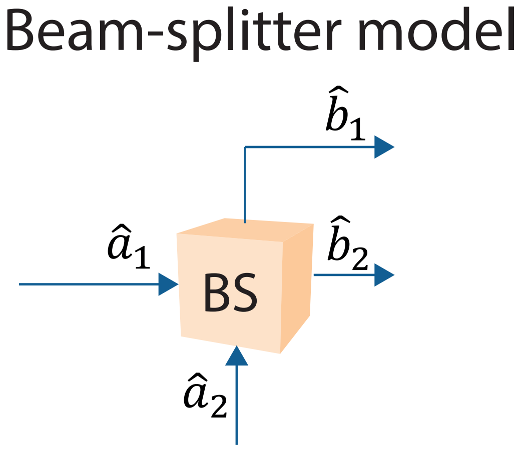


Figure 5.3: Schematic representation of the beam-splitter model.

In detail, and considering the beam-splitter model, the operators $\hat{a}_i$ with $i = 1, 2, 3, 4, 5, 6, 7, 8$ can be given by

$$\begin{cases} \hat{a}_1(t) = \frac{1}{\sqrt{2}} \left(\hat{b}_{v_1}(t) - \sqrt{\eta_d}\hat{c}_H(t) - \sqrt{1-\eta_d}\hat{b}_{v_{\eta_d H}}(t) \right) \\ \hat{a}_2(t) = \frac{1}{\sqrt{2}} \left(\hat{b}_{v_7}(t) - \hat{d}_H(t) \right) \end{cases} \tag{5.12a}$$

$$\begin{cases} \hat{a}_3(t) = \frac{1}{\sqrt{2}} \left(\sqrt{\eta_d}\hat{c}_H(t) + \sqrt{1-\eta_d}\hat{d}_H(t) + \hat{b}_{v_1}(t) \right) \\ \hat{a}_4(t) = \frac{1}{\sqrt{2}} \left(\hat{d}_H(t) + \hat{b}_{v_7}(t) \right) e^{i\pi/2} \end{cases} \tag{5.12b}$$

$$\begin{cases} \hat{a}_5(t) = \frac{1}{\sqrt{2}} \left(\hat{b}_{v_4}(t) - \sqrt{\eta_d}\hat{c}_V(t) - \sqrt{1-\eta_d}\hat{b}_{v_{\eta_d V}}(t) \right) \\ \hat{a}_6(t) = \frac{1}{\sqrt{2}} \left(\hat{b}_{v_8}(t) - \hat{d}_V(t) \right) \end{cases} \tag{5.12c}$$

$$\begin{cases} \hat{a}_7(t) = \frac{1}{\sqrt{2}} \left(\sqrt{\eta_d}\hat{c}_V(t) + \sqrt{1-\eta_d}\hat{b}_{v_{\eta_d V}}(t) + \hat{b}_{v_4}(t) \right) \\ \hat{a}_8(t) = \frac{1}{\sqrt{2}} \left(\hat{d}_V(t) + \hat{b}_{v_8}(t) \right) e^{i\pi/2}, \end{cases} \tag{5.12d}$$

where

$$\begin{cases} \hat{c}_H(t) = \hat{a}_{B_H}(t) \\ \hat{c}_V(t) = -\hat{a}_{B_V}(t), \end{cases} \tag{5.13}$$

and $\hat{b}_{V_i}$ with $i = 1, 4, 7, 8$ denotes the vacuum states inputs of the beam-splitters BS1, BS4, BS7, and BS8 in Figure 5.2. Furthermore, the operators $\hat{d}_H(t)$ and $\hat{d}_V(t)$ in 5.2.3 are given by

$$\begin{cases} \hat{d}_H(t) = \frac{1}{\sqrt{2}} \left(\hat{a}_{Lo_H}(t) - \hat{a}_{Lo_V}(t) \right) \\ \hat{d}_V(t) = -\frac{1}{\sqrt{2}} \left(\hat{a}_{Lo_H}(t) + \hat{a}_{Lo_V}(t) \right), \end{cases} \tag{5.14}$$

where $\hat{a}_{Lo_H}(t)$ and $\hat{a}_{Lo_V}(t)$ denote the orthogonal components of the local oscillator electric field after the 45° rotator at the input of the optical hybrid.

Voltages at Bob Homodyne Detection Outputs

After being detected by each pair of photo-diodes, the electrical signals are subtracted and amplified by a TIA following a standard homodyne detection scheme. The four voltages after the TIA obtained at the Bob homodyne detection scheme output in Figure 5.1 for a given symbol n are given by [107, 108, 112, 113],

$$v_{q_p}^{(n)}(t) = g_{\text{TIA}} \int_{-\infty}^{\infty} d\tau' \langle \hat{i}_{q_p}(t-\tau') \rangle r_{\text{TIA}}(\tau'), \tag{5.15}$$

where $q = \{X, P\}$ denotes the quadrature, and $p = \{H, V\}$ denotes the corresponding polarization, and $\hat{i}_{q_p}(t)$ represents the current generated by the homodyne detector [112]. Moreover, in (5.15) g_{TIA} is the TIA's gain, and $r_{\text{TIA}}(t)$ denotes the Fourier transform of the impulse response function considering a Butterworth filter of order n and bandwidth B_e given in frequency domain by [112]

$$H(\omega) = \frac{1}{\left[1 + \left(\frac{\omega}{2\pi B_e}\right)^{2\pi}\right]^{1/2}}. \tag{5.16}$$

In this work, we assume ideal digital signal processing for phase and frequency carrier recovery. The expected value of the current at the output of the difference operator between each pair of detectors in Figure 5.1, for each transmitted symbol n, is given by,

$$\begin{aligned}\big\langle \hat{i}_{x_H}(t) \big\rangle = q_e \big\langle \hat{a}_1^\dagger(t)\hat{a}_2(t) + \hat{a}_2^\dagger(t)\hat{a}_1(t) \big\rangle = -\frac{1}{2\sqrt{2}} q_e \sqrt{\eta_d}\sqrt{\tau_{ch}}\sqrt{\eta_{MZM}(t-nT_s)}\big|\alpha_{Lo}\big|\big|\alpha_s\big| \\ \text{Re}\Big\{ \big[\mathbf{Z}_{21} e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi} + \mathbf{Z}_{11}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big] e^{i\frac{V_A(t-nT_s)}{V_\pi}\pi} + \\ \big[\mathbf{Z}_{22}(t-nT_s) e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi} + \mathbf{Z}_{12}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big]\sqrt{\epsilon_{\text{PDL}}}\Big\} h(t-nT_s),\end{aligned} \tag{5.17a}$$

$$\begin{aligned}\big\langle \hat{i}_{p_H}(t) \big\rangle = q_e \big\langle \hat{a}_3^\dagger(t)\hat{a}_4(t) + \hat{a}_4^\dagger(t)\hat{a}_3(t) \big\rangle = -\frac{1}{2\sqrt{2}} q_e \sqrt{\eta_d}\sqrt{\tau_{ch}}\sqrt{\eta_{MZM}(t-nT_s)}\big|\alpha_{Lo}\big|\big|\alpha_s\big| \\ \text{Im}\Big\{ \big[\mathbf{Z}_{21} e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi} + \mathbf{Z}_{11}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big] e^{i\frac{V_A(t-nT_s)}{V_\pi}\pi} + \\ \big[\mathbf{Z}_{22}(t-nT_s) e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi} + \mathbf{Z}_{12}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big]\sqrt{\epsilon_{\text{PDL}}}\Big\} h(t-nT_s),\end{aligned} \tag{5.17b}$$

$$\begin{aligned}\big\langle \hat{i}_{x_V}(t) \big\rangle = q_e \big\langle \hat{a}_5^\dagger(t)\hat{a}_6(t) + \hat{a}_6^\dagger(t)\hat{a}_5(t) \big\rangle = -\frac{1}{2\sqrt{2}} q_e \sqrt{\eta_d}\sqrt{\tau_{ch}}\sqrt{\eta_{MZM}(t-nT_s)}\big|\alpha_{Lo}\big|\big|\alpha_s\big| \\ \text{Re}\Big\{ \big[\mathbf{Z}_{21} e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi} - \mathbf{Z}_{11}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big] e^{i\frac{V_A(t-nT_s)}{V_\pi}\pi} + \\ \big[\mathbf{Z}_{22}(t-nT_s) e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi} - \mathbf{Z}_{12}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big]\sqrt{\epsilon_{\text{PDL}}}\Big\} h(t-nT_s),\end{aligned} \tag{5.17c}$$

$$\begin{aligned}\big\langle \hat{i}_{p_V}(t) \big\rangle = q_e \big\langle \hat{a}_7^\dagger(t)\hat{a}_8(t) + \hat{a}_8^\dagger(t)\hat{a}_6(t) \big\rangle = -\frac{1}{2\sqrt{2}} q_e \sqrt{\eta_d}\sqrt{\tau_{ch}}\sqrt{\eta_{MZM}(t-nT_s)}\big|\alpha_{Lo}\big|\big|\alpha_s\big| \\ \text{Im}\Big\{ \big[\mathbf{Z}_{21} e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi} - \\ \mathbf{Z}_{11}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big] e^{i\frac{V_A(t-nT_s)}{V_\pi}\pi} + \\ \big[\mathbf{Z}_{22}(t-nT_s) e^{i\frac{V_B(t-nT_s)}{V_\pi}\pi} - \mathbf{Z}_{12}(t-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big]\sqrt{\epsilon_{\text{PDL}}}\Big\} h(t-nT_s),\end{aligned} \tag{5.17d}$$

where η_D denotes the detection efficiency, q_e is the charge of the electron, and $\left|\alpha_{Lo}\right|^2$ is the optical flux of the locally generated local oscillator. Note that $\hat{a}_i^\dagger(t)\hat{a}_j(t)$, with $i, j = 1, 2, 3, 4, 5, 6, 7, 8$, is the optical flux in each branch of the BS output in Figure 5.1. Accordingly with the expected value of the currents defined in (5.17), and the voltage-current relation defined in (5.15), the measured quadratures for a given transmitted symbol n are defined by integrating the homodyne voltage over a certain time interval [107, 108, 112, 113],

$$\begin{aligned}\hat{Q}_{H,n} = \frac{1}{T_s}\int_{\frac{T_s}{2}(2n-1)}^{\frac{T_s}{2}(2n+1)} v_{x_H}^{(n)}(t) = \\ = \frac{1}{T_s} g_{\text{TIA}} \int_{\frac{T_s}{2}(2n-1)}^{\frac{T_s}{2}(2n+1)} dt \int_{-\infty}^{+\infty} d\tau' \big\langle \hat{i}_{x_H}(t-\tau')\big\rangle r_{\text{TIA}}(\tau') + \hat{Q}_{e,n} + \hat{Q}_{S_{X,H},n},\end{aligned} \tag{5.18a}$$

$$\begin{aligned}\hat{P}_{H,n} = \frac{1}{T_s}\int_{\frac{T_s}{2}(2n-1)}^{\frac{T_s}{2}(2n+1)} v_{p_H}^{(n)}(t) = \\ = \frac{1}{T_s} g_{\text{TIA}} \int_{\frac{T_s}{2}(2n-1)}^{\frac{T_s}{2}(2n+1)} dt \int_{-\infty}^{+\infty} d\tau' \big\langle \hat{i}_{p_H}(t-\tau')\big\rangle r_{\text{TIA}}(\tau') + \hat{Q}_{e,n} + \hat{Q}_{S_{P,H},n},\end{aligned} \tag{5.18b}$$

$$\begin{aligned}\hat{Q}_{V,n} = \frac{1}{T_s}\int_{\frac{T_s}{2}(2n-1)}^{\frac{T_s}{2}(2n+1)} v_{x_V}^{(n)}(t) = \\ = \frac{1}{T_s} g_{\text{TIA}} \int_{\frac{T_s}{2}(2n-1)}^{\frac{T_s}{2}(2n+1)} dt \int_{-\infty}^{+\infty} d\tau' \big\langle \hat{i}_{x_V}(t-\tau')\big\rangle r_{\text{TIA}}(\tau') + \hat{Q}_{e,n} + \hat{Q}_{S_{X,V},n},\end{aligned} \tag{5.18c}$$

$$\begin{aligned}\hat{P}_{V,n} = \frac{1}{T_s}\int_{\frac{T_s}{2}(2n-1)}^{\frac{T_s}{2}(2n+1)} v_{p_V}^{(n)}(t) = \\ = \frac{1}{T_s} g_{\text{TIA}} \int_{\frac{T_s}{2}(2n-1)}^{\frac{T_s}{2}(2n+1)} dt \int_{-\infty}^{+\infty} d\tau' \big\langle \hat{i}_{p_V}(t-\tau')\big\rangle r_{\text{TIA}}(\tau') + \hat{Q}_{e,n} + \hat{Q}_{S_{P,V},n},\end{aligned} \tag{5.18d}$$

where $\hat{Q}_{e,n}$ is the electronic noise for each transmitted symbol n, and $\hat{Q}_{S_{q,p},n}$ is the shot noise. The variance of the quadratures in (5.18) for a given optical transmitted pulse n is given by [107, 108, 112, 113],

$$\begin{aligned}\sigma_{q_p}^2 = \frac{g_{\text{TIA}}^2}{T_s^2}\int_{\frac{T_s}{2}(2n-1)}^{\frac{T_s}{2}(2n+1)} dt_1 \int_{\frac{T_s}{2}(2n-1)}^{\frac{T_s}{2}(2n+1)} dt_2 \int_{-\infty}^{+\infty} d\tau' \int_{-\infty}^{+\infty} d\tau'' \big[\big\langle \hat{i}_{q_p}(t_1-\tau')\hat{i}_{q_p}(t_2-\tau'')\big\rangle \\ \big\langle \hat{i}_{q_p}(t_1-\tau')\big\rangle\big\langle \hat{i}_{q_p}(t_2-\tau'')\big\rangle\big] r_{\text{TIA}}(\tau')r_{\text{TIA}}(\tau'') + Q_{e,n}^2.\end{aligned} \tag{5.19}$$

For each quadrature $q = \{X, P\}$ we obtain

$$\begin{aligned}\Big(\big\langle \hat{i}_{q_H}(t')\hat{i}_{q_H}(t')\big\rangle - \big\langle \hat{i}_{q_H}(t')\big\rangle\big\langle \hat{i}_{q_H}(t')\big\rangle\Big) = \frac{1}{8}q_e^2\eta_d\big(\big\langle \hat{a}_{B_H}^\dagger(t')\hat{a}_{B_H}(t')\big\rangle \\ + \big\langle \hat{a}_{Lo_H}^\dagger(t')\hat{a}_{Lo_H}(t')\big\rangle\big),\end{aligned} \tag{5.20a}$$

$$\begin{aligned}\Big(\big\langle \hat{i}_{q_V}(t')\hat{i}_{q_V}(t')\big\rangle - \big\langle \hat{i}_{q_V}(t')\big\rangle\big\langle \hat{i}_{q_V}(t')\big\rangle\Big) = \frac{1}{8}q_e^2\eta_d\big(\big\langle \hat{a}^\dagger_{B_V}(t')\hat{a}_{B_V}(t')\big\rangle \\ + \big\langle \hat{a}^\dagger_{Lo_H}(t')\hat{a}_{Lo_H}(t')\big\rangle\big),\end{aligned} \tag{5.20b}$$

where $\big\langle \hat{a}^\dagger_{Lo_H}(t')\hat{a}_{Lo_H}(t')\big\rangle$ is equal to the optical flux of the local oscillator, $\big|\alpha_{Lo}\big|^2$, and

$$\begin{aligned}\big\langle \hat{a}^\dagger_{B_H}(t')\hat{a}_{B_H}(t')\big\rangle = \frac{\tau_{ch}}{2}\big|\mathbf{Z}_{21}(t'-nT_s)e^{i\frac{V_B(t'-nT_s)}{V_\pi}\pi} + \mathbf{Z}_{11}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big|^2 \\ \big\langle \hat{a}^\dagger_{A_H}(t')\hat{a}_{A_H}(t')\big\rangle + \frac{\tau_{ch}}{2}\big|\mathbf{Z}_{22}(t'-nT_s)e^{i\frac{V_B(t'-nT_s)}{V_\pi}\pi} + \mathbf{Z}_{12}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big|^2 \\ \big\langle \hat{a}^\dagger_{A_V}(t')\hat{a}_{A_V}(t')\big\rangle + \frac{\tau_{ch}}{2}\big(\mathbf{Z}^*_{21}(t'-nT_s)e^{-i\frac{V_B(t'-nT_s)}{V_\pi}\pi} + \mathbf{Z}^*_{11}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big) \\ \big(\mathbf{Z}_{22}(t'-nT_s)e^{i\frac{V_B(t'nT_s)}{V_\pi}\pi} + \mathbf{Z}_{12}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big)\big\langle \hat{a}^\dagger_{A_H}(t')\hat{a}_{A_V}(t') + \frac{\tau_{ch}}{2}\big(\mathbf{Z}^*_{22}(t'-nT_s) \\ e^{-i\frac{V_B(t'-nT_s)}{V_\pi}\pi} + \mathbf{Z}_{12}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big)\big(\mathbf{Z}_{21}(t'-nT_s)e^{i\frac{V_B(t'-nT_s)}{V_\pi}\pi} + \\ \mathbf{Z}_{11}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big)\big\langle \hat{a}^\dagger_{A_V}(t')\hat{a}_{A_H}(t')\big\rangle\end{aligned} \tag{5.21a}$$

$$\begin{aligned}\big\langle \hat{a}^\dagger_{B_V}(t')\hat{a}_{B_V}(t')\big\rangle = \frac{\tau_{ch}}{2}\big|\mathbf{Z}_{21}(t'-nT_s)e^{i\frac{V_B(t'-nT_s)}{V_\pi}\pi} - \mathbf{Z}_{11}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big|^2 \\ \big\langle \hat{a}^\dagger_{A_H}(t')\hat{a}_{A_H}(t')\big\rangle + \frac{\tau_{ch}}{2}\big|\mathbf{Z}_{22}(t'-nT_s)e^{i\frac{V_B(t'-nT_s)}{V_\pi}\pi} - \mathbf{Z}_{12}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big|^2 \\ \big\langle \hat{a}^\dagger_{A_V}(t')\hat{a}_{A_V}(t')\big\rangle + \frac{\tau_{ch}}{2}\big(\mathbf{Z}^*_{21}(t'-nT_s)e^{-i\frac{V_B(t'-nT_s)}{V_\pi}\pi} - \mathbf{Z}^*_{11}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big) \\ \big(\mathbf{Z}_{22}(t'-nT_s)e^{i\frac{V_B(t'nT_s)}{V_\pi}\pi} - \mathbf{Z}_{12}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big)\big\langle \hat{a}^\dagger_{A_H}(t')\hat{a}_{A_V}(t') + \frac{\tau_{ch}}{2}\big(\mathbf{Z}^*_{22}(t'-nT_s) \\ e^{-i\frac{V_B(t'-nT_s)}{V_\pi}\pi} - \mathbf{Z}_{12}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big)\big(\mathbf{Z}_{21}(t'-nT_s)e^{i\frac{V_B(t'-nT_s)}{V_\pi}\pi} - \\ \mathbf{Z}_{11}(t'-nT_s)\sqrt{\epsilon_{\text{PDL}}}\big)\big\langle \hat{a}^\dagger_{A_V}(t')\hat{a}_{A_H}(t')\big\rangle\end{aligned} \tag{5.21b}$$

with

$$\big\langle \hat{a}^\dagger_{A_H}(t')\hat{a}_{A_H}(t')\big\rangle = \frac{1}{2}\eta_{\text{MZM}}(t'-nT_s)\big|h(t'-nT_s)\big|^2|\alpha_s|^2 \tag{5.22a}$$

$$\big\langle \hat{a}^\dagger_{A_V}(t')\hat{a}_{A_V}(t')\big\rangle = \frac{1}{2}\epsilon_{\text{PDL}}\eta_{\text{MZM}}(t'-nT_s)\big|h(t'-nT_s)\big|^2|\alpha_s|^2 \tag{5.22b}$$

$$\big\langle \hat{a}^\dagger_{A_H}(t')\hat{a}_{A_V}(t')\big\rangle = \frac{1}{2}\sqrt{\epsilon\text{PDL}}\sqrt{\eta_{\text{MZM}}(t'-nT_s)}e^{-i\frac{V_A(t'-nT_s)}{V_\pi}\pi}|\alpha_s|^2\big|h(t'-nT_s)\big|^2 \tag{5.22c}$$

$$\big\langle \hat{a}^\dagger_{A_V}(t')\hat{a}_{A_H}(t')\big\rangle = \frac{1}{2}\sqrt{\epsilon_{\text{PDL}}}\sqrt{\eta_{\text{MZM}}(t'-nT_s)}e^{+i\frac{V_A(t'-nT_s)}{V_\pi}\pi}|\alpha_s|^2\big|h(t'-nT_s)\big|^2. \tag{5.22d}$$

In addition to the quadratures voltages defined in (5.18), we can also obtain the Stokes parameters for each transmitted symbol n. The Stokes parameters allow us to characterize the polarization state after homodyne detection at Bob detection system in Figure 5.1. This is essential to see the impact of the PMD on the pilot tone during its evolution on the transmission channel. Mapping the polarization state obtained for the pilot tone, allows to implement adequate polarization compensation techniques. The total intensity of the

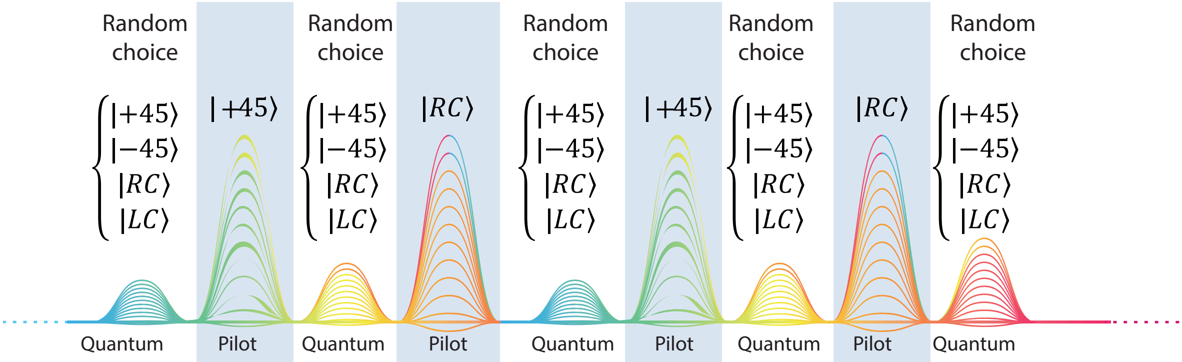


Figure 5.4: Transmitted frame where the pilot tone that follows a deterministic sequence alternating between $|45\rangle$ and $|RC\rangle$ is time-multiplexed with the quantum data signal, which the sequence is randomly chosen between four possible SOPs.

transmitted pilot-pulse n is defined by the Stokes parameter $\hat{S}_{0,n}$ which can be expressed as following [114]

$$\hat{S}_{0,n} = \big(\hat{Q}_{H,n} + i\hat{P}_{H,n}\big)^{\dagger}\big(\hat{Q}_{H,n} + i\hat{P}_{H,n}\big) + \big(\hat{Q}_{V,n} + i\hat{P}_{V,n}\big)^{\dagger}\big(\hat{Q}_{V,n} + i\hat{P}_{V,n}\big). \tag{5.23}$$

The three-dimensional vector $(\hat{S_{1,n}}, \hat{S_{2,n}}, \hat{S_{3,n}})$ divided by the total intensity of each transmitted pulse n (see equation 5.23) denotes the location of the state of polarization on Poincaré sphere with coordinates

$$\hat{S}_{1,n} = \big(\hat{Q}_{H,n} + i\hat{P}_{H,n}\big)^{\dagger}\big(\hat{Q}_{H,n} + i\hat{P}_{H,n}\big) - \big(\hat{Q}_{V,n} + i\hat{P}_{V,n}\big)^{\dagger}\big(\hat{Q}_{V,n} + i\hat{P}_{V,n}\big), \tag{5.24a}$$

$$\hat{S}_{2,n} = \big(\hat{Q}_{V,n} + i\hat{P}_{V,n}\big)^{\dagger}\big(\hat{Q}_{H,n} + i\hat{P}_{H,n}\big) + \big(\hat{Q}_{H,n} + i\hat{P}_{H,n}\big)^{\dagger}\big(\hat{Q}_{V,n} + i\hat{P}_{V,n}\big), \tag{5.24b}$$

$$\hat{S}_{3,n} = -i\Big(\big(\hat{Q}_{V,n} + i\hat{P}_{V,n}\big)^{\dagger}\big(\hat{Q}_{H,n} + i\hat{P}_{H,n}\big) - \big(\hat{Q}_{H,n} + i\hat{P}_{H,n}\big)^{\dagger}\big(\hat{Q}_{V,n} + i\hat{P}_{V,n}\big)\Big). \tag{5.24c}$$

From the quantum state of polarization Stokes coordinates in Poincaré sphere we can have information about the current location of the state without the need of additional signals, which allows us to have knowledge about the suffered drift though the quantum transmission channel. In this way, we can track the pilot signal and easily find the reversal polarization random drift operator and compensate it performing a deterministic rotation on the EPC at the Bob's input in Figure 5.1.

5.3 DV-QKD BB84 Protocol Implementation

In this sub-section, we detail the DV-QKD BB84 protocol implementation in the proposed quantum communication system. The DV-QKD BB84 is a prepared-measured protocol that requires the preparation of four states of polarization obtained from two non-orthogonal mutually unbiased bases. In this work, we consider the diagonal and circular bases. When Alice and Bob choose the same polarization basis the homodyne detection output is deterministic. For instance, in the diagonal basis the $|45°\rangle$ and the $|-45°\rangle$ polarization states will be measured in Figure 5.1 by the homodyne detectors $v_{x_H}^{(n)}(t)$ and $v_{x_V}^{(n)}(t)$, respectively. On the other hand, when Alice and Bob use the circular basis the $|RC\rangle$ and $|LC\rangle$ polarization states will be measured in Figure 5.1 by the homodyne detectors $v_{p_H}^{(n)}(t)$ and $v_{p_V}^{(n)}(t)$, respectively. When

Alice and Bob basis aren't coincident the measurement is random. Figure 5.5 summarizes the possible outcomes of the measurement results. Moreover, in terms of binary, the bit 0 is obtained whenever the $|+45\rangle$ or $|\mathrm{RC}\rangle$ are prepared in Alice's side and the diagonal or circular measurement basis is chosen in Bob's phase modulator, respectively. The bit 1 is obtained whenever the $|-45\rangle$ or $|\mathrm{LC}\rangle$ are prepared in Alice's side and the diagonal or circular measurement basis is chosen in Bob's phase modulator, respectively. Besides that, when the state of polarization in Alice's side is prepared in a different basis than the selected measurement basis in Bob's side, a random outcome is obtained. Since the preparation and measurement bases are orthogonal, the single-photon has a 1/2 probability of emerging in $\hat{c}_H$ and a 1/2 probability of emerging in $\hat{c}_V$ in Figure 5.1.

The implemented protocol comprises two time-multiplexed signals, see Figure 5.4. The pilot tone (classical optical signal) is implemented assuming $\eta_{\mathrm{MZM}}(t - nT_s) = 1$ in the MZM. The pilot signal is used for compensate the phase and frequency mismatches between Alice and Bob lasers, and also for characterize the polarization drift imposed by the optical fiber. That polarization drift compensation can be achieved assuming that for the pilot tone Alice and Bob agrees in a previously established sequence of polarization states, see for instance Figure 5.4. In order to prepare this pilot tone, Alice alternately applies $V_A = 0$ V and $V_A = -V_\pi/2$ in its phase modulator to send $|+45°\rangle$ and $|\mathrm{RC}\rangle$ polarization states, respectively. Bob measures the pilot tone alternatively (not randomly) applying $V_B = 0$ V and $V_B = V_\pi/2$ to choose the diagonal and circular basis, respectively. From the difference between what Bob measures and the ideal scenario without fiber PMD, Bob can use that information to reverse the fiber polarization drift using the EPC in Figure 5.1. The pilot tone is time-multiplexed with the quantum signal in consecutive transmitted symbols. The quantum signal is prepared choosing a very low efficiency in the Alice's MZM amplitude modulator, which is calculated according with equation 5.2, such that at Alice output we have $\langle n_Q \rangle = 0.1$ photons per pulse. For the quantum signal implementation, Alice randomly chooses one of the four voltages for preparing one of the four considered states of polarization: $V_A = 0$ V or $V_A = V_\pi$ V to prepare

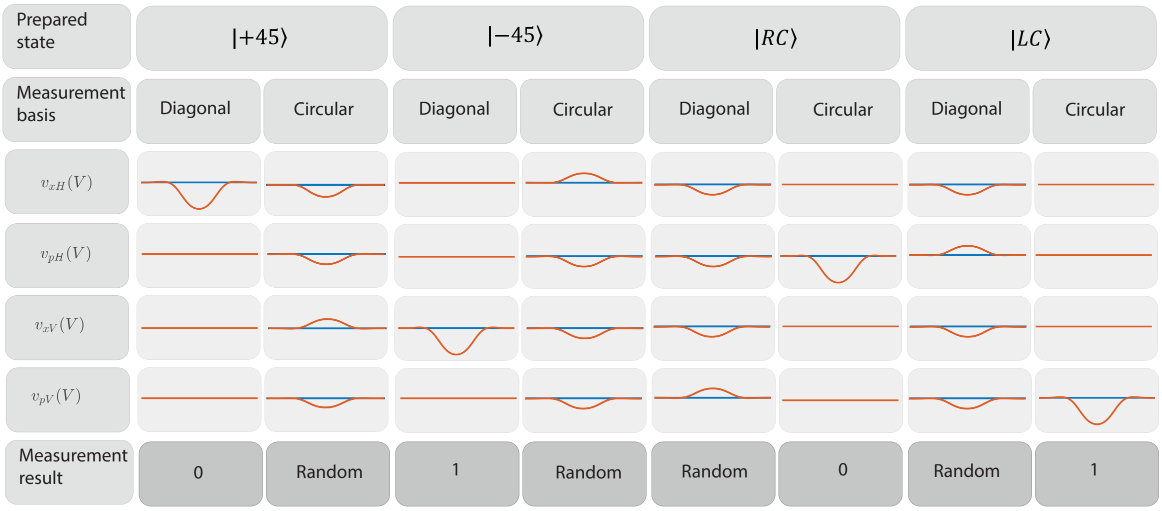


Figure 5.5: Voltages at TIA's output in Figure 5.1 for each of the four prepared states considering one of the two measurement basis, and the corresponding bit measurement result.

$| + 45°\rangle$ or $| - 45°\rangle$, respectively, and $V_A = V_\pi/2$ V or $V_A = -V_\phi/2$ V to prepare $|\mathrm{RC}\rangle$ or $|\mathrm{LC}\rangle$, respectively. For quantum pulses measurement, the measurement basis is also chosen in a random fashion. Bob randomly chooses between the diagonal basis, applying $V_B = 0$ V, or the circular basis applying $V_B = V_\pi/2$ V.

5.4 Polarization Drift Compensation

Polarization mode dispersion is a serious obstacle on practical polarization encoded based communication system over optical fiber networks. In this work, we take advantage of continuous Stokes parameters information, measured from the obtained quadrature, and calculated

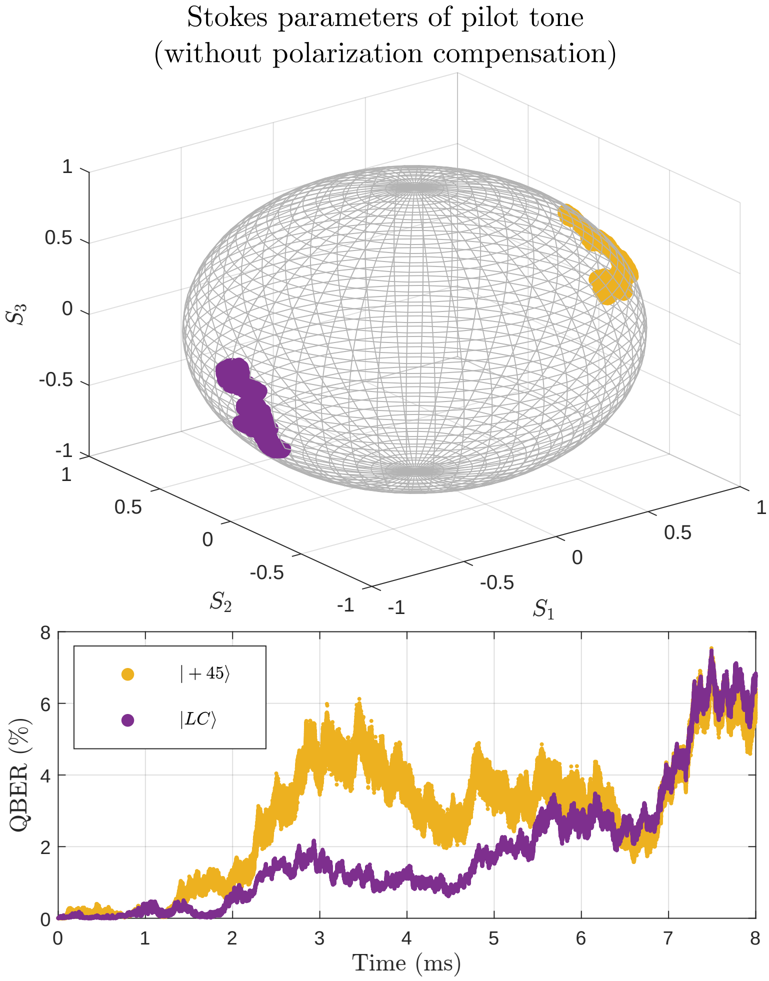


Figure 5.6: Poincaré sphere representation of the evolution of the SOPs $|45\rangle$ and $|\mathrm{RL}\rangle$ sent in the pilot tone, and the respective QBER of each SOP over time for a simulation without an active compensation of the EPC at Bob's input in Figure 5.1. We consider that 8 million of symbols were transmitted, where the pilot tone is time multiplexed with the quantum signal. The polarization random drift was modelled using a $\sigma^2 = 2 \times 10^{-9}$ to obtain the matrix M_F in equation 5.4 for each transmitted symbol. In this simulation we consider a 40 km standard optical fiber channel.

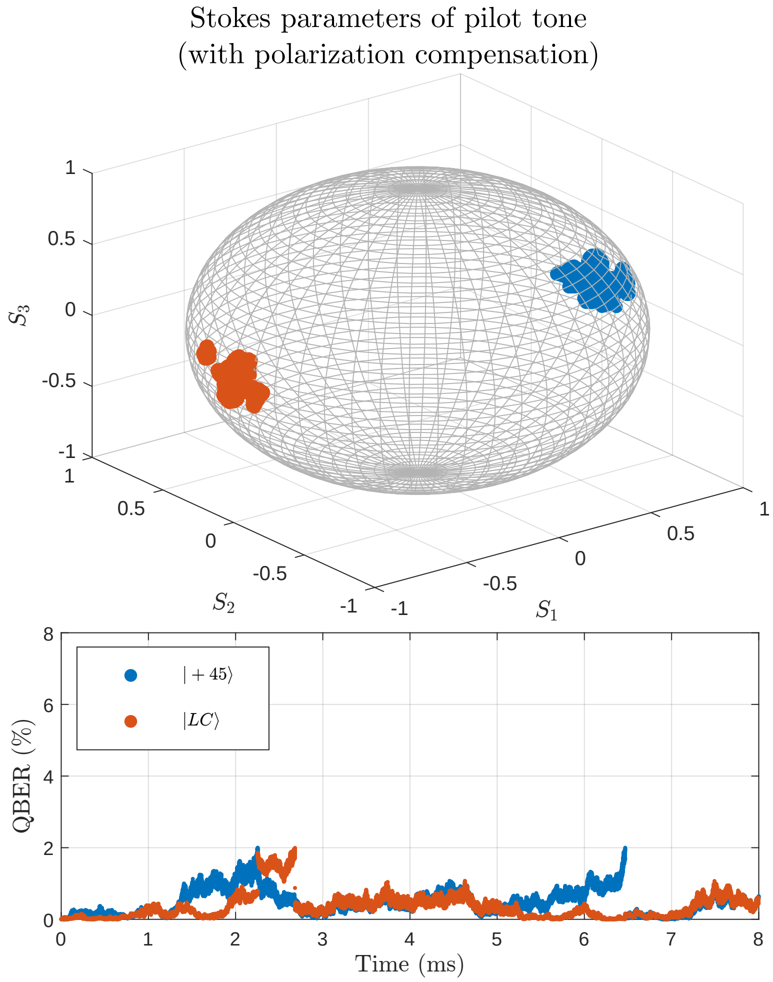


Figure 5.7: Poincaré sphere representation of the evolution of the SOPs $|45\rangle$ and $|\text{RL}\rangle$ sent in the pilot tone, and the respective QBER of each SOP over time for a simulation with an active polarization compensation on the EPC in Figure 5.1 using the Stokes parameters calculated with equations 5.24 for each transmitted pilot signal n. We consider that 8 million of symbols were transmitted, where the pilot tone is time multiplexed with the quantum signal. The polarization random drift was modelled using a $\sigma^2 = 2 \times 10^{-9}$ to obtain the matrix M_F in equation 5.4 for each transmitted symbol. In this simulation we consider a 40 km standard optical fiber channel.

---

according with equations 5.24, to reconstruct the received state of polarization and compensate the polarization random drift due to PMD. In order to find the polarization random drift reversal operator, we monitor the deterministic sequence sent in the pilot tone that contains two states of polarization from two non-orthogonal mutually unbiased bases and apply the needed compensation rotations to maintain the QBER bellow the defined error boundary due to polarization random drift. In this work, we consider a boundary of 2% error above which a compensation rotation must be applied using for instance an EPC. The polarization random drift velocity is modelled considering a $\sigma^2 = 2 \times 10^{-9}$ to obtain the the matrix M_F for each transmitted symbol n, which induces a continuous drift on the prepared states of polarization when travel over a 40 km standard single-mode optical fiber with an attenuation coefficient of 0.2 dB/km. That value for σ^2 maintains the QBER bellow the defined boundary for a little more that 2 ms, which is a typically value for a buried fiber subjected to external perturbations. We at Alice side an optical power at of $P_s = 3$ mW at laser output, a symbol duration of $T_s = 1$ ns, and for the pilot tone we use $\eta_{\text{MZM}}(t - nT_s) = 1$. Moreover, at Bob detection system we consider a detection efficient per homodyne detection of 76%, a TIA gain of $g_{\text{TIA}} = 16^3$ V/A and bandwidth of $B_e = 1.6$ GHz. Moreover, for each transmitted symbol (pilot tone or quantum signal) we generated the electronic noise contribution from a Gaussian distribution with variance $\sigma^2_{\hat{Q}_{e,n}} = 0.4 \times 10^{-3} V^2$ and zero mean [112]. The shot-noise contribution is independently simulated for each homodyne detector from a Gaussian distribution with zero mean and variance calculated according with the variance of the four quadratures as presented in equation 5.19. This also for each transmitted symbol. We consider a PDL value of ϵPDL = 2.3 dB. Figure 5.6 shows the stokes parameters obtained for the pilot tone states of polarization without active polarization compensation on the EPC at Bob's input, and Figure 5.7 shows the stokes parameters obtained for the pilot tone states of polarization with active polarization compensation. Moreover, the QBER for each transmitted symbol n can be calculated from the stokes parameters obtained in relation to a reference state of polarization according with the following [27],

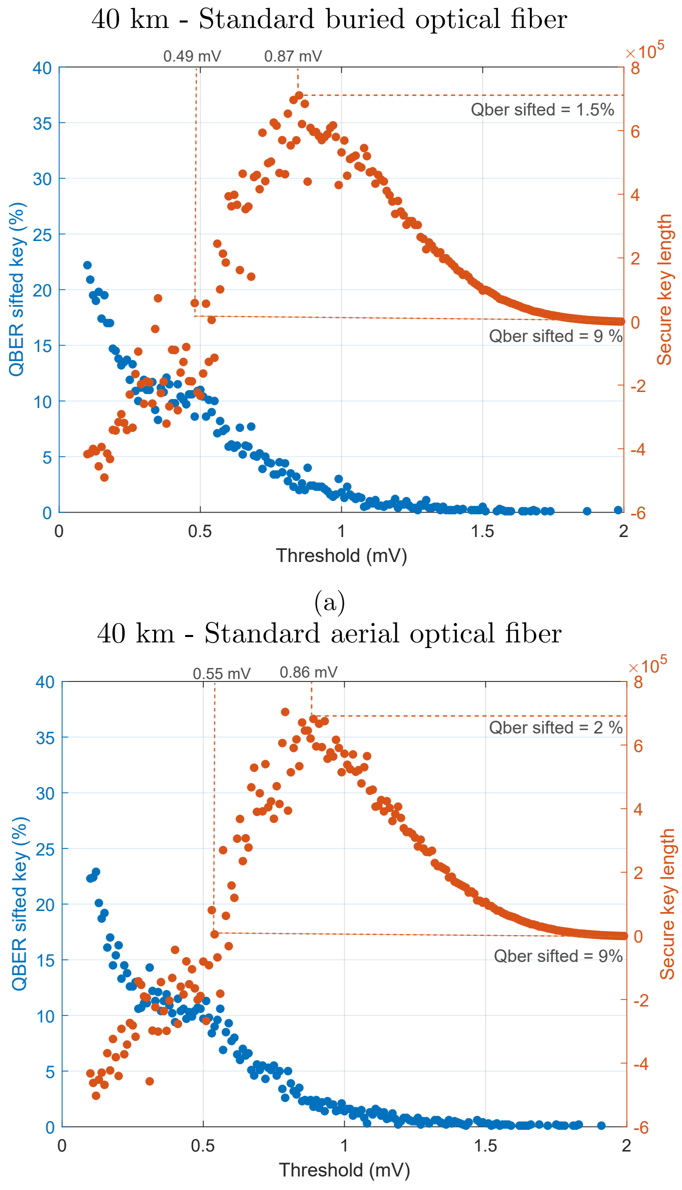
$$\text{QBER}(\theta, \phi) = 1 - \frac{1}{2}\Big(1 + \cos\theta\cos\phi\Big), \tag{5.25}$$

where $\theta = \arctan\frac{\hat{S}_2}{\hat{S}_1}$ and $\phi = \arcsin\hat{S}_3$. In the top of Figure 5.6, the pilot tone Stokes parameters without polarization drift compensation, which correspond to a temporal evolution of QBER represented in the bottom of Figure 5.6. On the other hand, in the top of Figure 5.7, the pilot tone Stokes parameters considering an active compensation using the EPC at Bob side. In the bottom of Figure 5.7 the corresponding QBER is presented. The implemented polarization random drift compensation method guarantees a QBER bellow the defined error boundary due PMD for the total acquisition time. The method for polarization drift compensation presented in this work is free of additional hardware or extra bandwidth signals, since it uses the pilot tone states of polarization, which is already needed for phase and amplitude differences compensation between the transmitter laser and the locally generated local oscillator.

5.5 Conjugate Homodyne Detection in Counting Mode

The DV-QKD protocols demand to discriminate the vacuum state from non-vacuum states. In order to operate the conjugate homodyne detection scheme in photon counting mode, the continuous detection measurements must be mapped to one of the two possible events, click or no-click. In this work, we adopt a strategy based on pre-defined detection threshold, $\tau \in \{0, \infty\}$, above which we consider a click and below which we consider no-click. That mapping process is software implemented in the post-processing stage. By choosing the appropriate τ we aim the longer secure key with a lower sifted key QBER in the DV-QKD BB84 protocol.

The basic idea of BB84 protocol is the exchange of two set of states orthogonal within each set with a 1/2 probability of overlap between sets. Since the receiver randomly chooses the measurement basis, Bob and Alice obtain a raw key that after being distilled results in a sifted

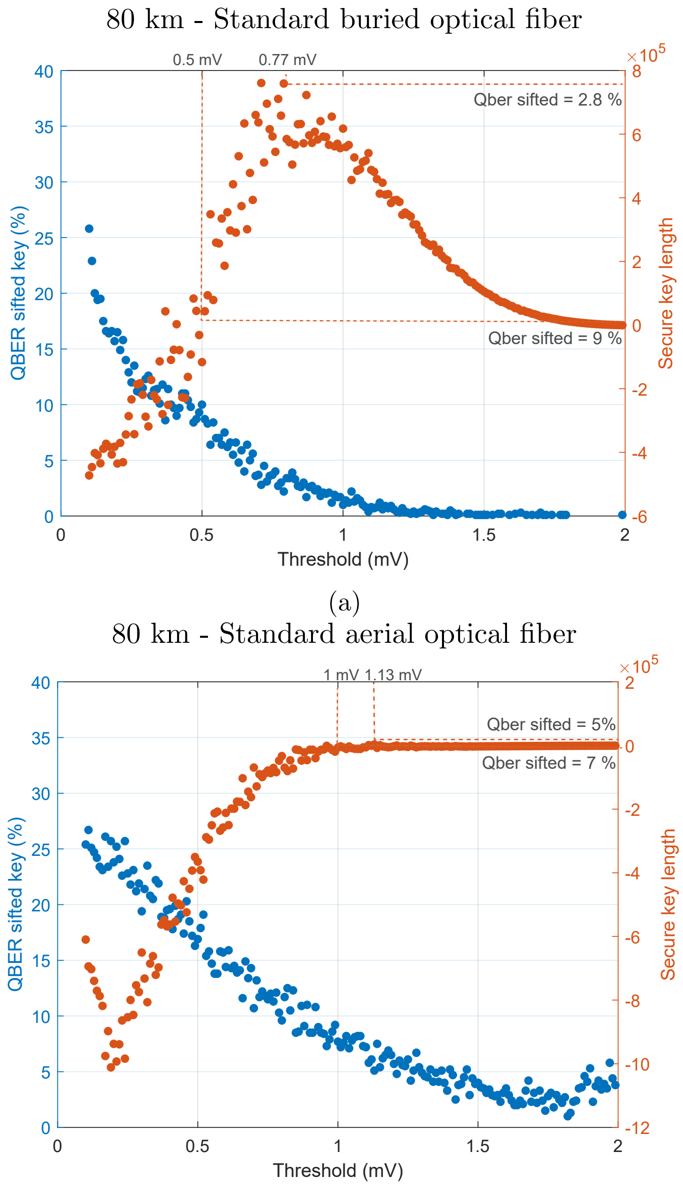


(a)

(b)

Figure 5.8: QBER of the sifted key and secure key length as a function of the voltage threshold applied in the quadratures calculated using equations 5.18. We consider that 8 million of symbols were transmitted, where the pilot tone is time multiplexed with the quantum signal. For the pilot tone we assume $P_s = 3$ mW with $\eta_{\text{MZM}} = 1$, whereas for the quantum signal we use $P_s = 3$ mW and $\eta_{\text{MZM}} = 9.83 \times 10^{-5}$. We consider a 40 km standard optical fiber channel length under two different external conditions scenarios. In (a), it was consider a $\sigma^2 = 2 \times 10^{-9}$ to obtain the matrix M_F in equation 5.4 for each transmitted symbol, which corresponds to a standard buried optical fiber. In (b), it was consider a $\sigma^2 = 6 \times 10^{-9}$ to obtain the matrix M_F in equation 5.4 for each transmitted symbol, which corresponds typically to an aerial optical fiber implementation.

key after publicly perform basis reconciliation. Figure 5.8 and Figure 5.9 show the QBER



(a)

(b)

Figure 5.9: QBER of the sifted key and secure key length as a function of the voltage threshold applied in the quadratures calculated using equations 5.18. We consider that 8 million of symbols were transmitted, where the pilot tone is time multiplexed with the quantum signal. For the pilot tone we assume $P_s = 3$ mW with $\eta_{\text{MZM}} = 1$, whereas for the quantum signal we use $P_s = 3$ mW and $\eta_{\text{MZM}} = 9.83 \times 10^{-5}$. We consider a 80 km standard optical fiber channel length. In (a), it was consider a $\sigma^2 = 2 \times 10^{-9}$ to obtain the matrix M_F in equation 5.4 for each transmitted symbol, which corresponds to a standard buried optical fiber. In (b), it was consider a $\sigma^2 = 6 \times 10^{-9}$ to obtain the matrix M_F in equation 5.4 for each transmitted symbol, which corresponds typically to an aerial optical fiber implementation.

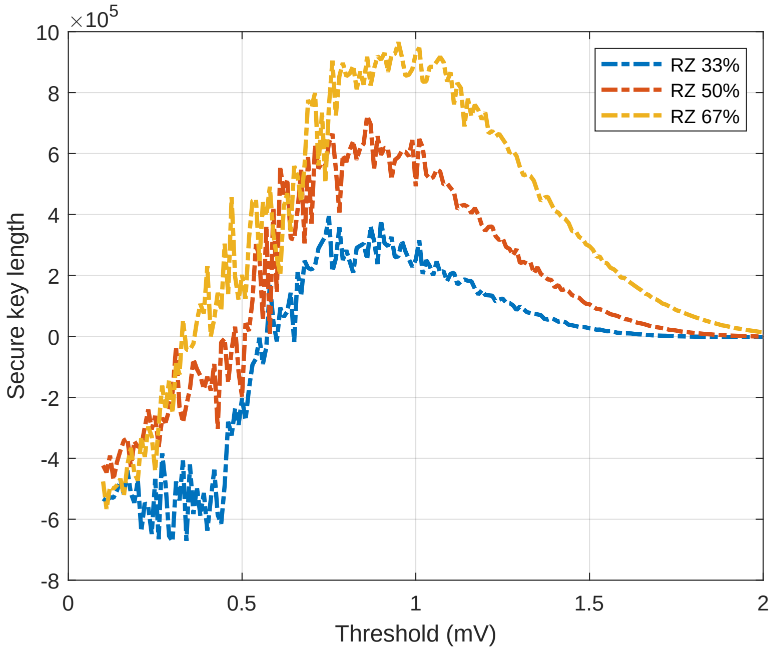


Figure 5.10: Secure key length as a function of the voltage threshold applied in the quadratures calculated using equations 5.18 for different signal return-to-zero ratios. For this simulation, 8 million symbols were transmitted, assuming $P_s = 3$ mW and $\eta_{\mathrm{MZM}} 9.83 \times 10^{-5}$. It was consider a $\sigma = 2 \times 10^{-9}$ to obtain the matrix M_F in equation 5.4 for each transmitted symbol, which corresponds to a standard buried optical fiber. Three different signal return-to-zero ratios were considered.

calculated using 1000 bits from the sifted key, which are later discarded before obtain the final secure key, as a function of the chosen threshold τ. The system was simulated considering two different distances for the quantum channels, 40 km (see Figure 5.8) and 80 km (see Figure 5.9), assessing a buried optical fiber and a standard aerial optical fiber for each distance. In this way, the curves of the QBER of the sifted key and the secure key length as a function of the defined voltage threshold was obtained in Figure 5.8-(a) and in Figure 5.9-(a) considering a standard buried optical fiber channel ($\sigma^2 = 2 \times 10^{-9}$). In Figure 5.8-(b) and in Figure 5.9-(b)considering an aerial optical fiber subject to heavy external conditions ($\sigma^2 = 6 \times 10^{-9}$). In this work, we consider the power of eavesdropper is limited to an individual attack for realistic signal sources [97], where Eve uses the single-photon detectors operating in gated mode commonly used in standard DV-QKD implementations. In this way, we consider that the error correction code has a practical efficiency of $f_{EC} = 1.2$, and the estimated portion of the sifted key disclosed is leak$_{EC} = f_{EC} h(E)$, where $h(E)$ is the binary Shannon entropy of the observed error rate E. Moreover, we also consider that the estimated error rate from a sifted key of size N may be deviated from the actual value with probability ϵ_{PE} and can be given as $\tilde{E} = E + \frac{1}{2}\sqrt{\{2\ln(1/\epsilon_{PE}) + 2\ln(N+1)\}(1/N)}$. The secure key length in Figures 5.8 and 5.9 is calculated as following [100]

$$l = N\Big(1 - h\big(\tilde{E}\big)\Big) - N\mathrm{leak}_{EC} - 7N\sqrt{\frac{1}{N}\log_2\frac{2}{\tilde{\epsilon}}} - 2\log_2\frac{1}{\epsilon_{PA}} - \log_2\frac{2}{\epsilon_{EC}}, \tag{5.26}$$

where $\epsilon = \epsilon_{PE} + \tilde{\epsilon} + \epsilon_{PA} + \epsilon_{EC}$ is a security parameter, $\tilde{\epsilon}$ is the probability that information of

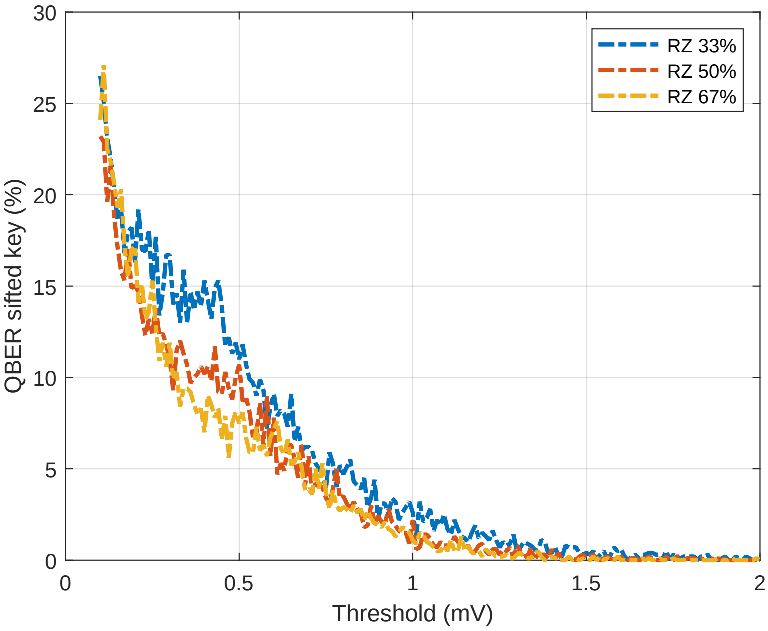


Figure 5.11: QBER of the sifted key as a function of the voltage threshold applied in the quadratures calculated using equations 5.18 for different signal return-to-zero ratios. For this simulation, 8 million symbols were transmitted, assuming $P_s = 3$ mW and $\eta_{\text{MZM}} 9.83 \times 10^{-5}$. It was consider a $\sigma = 2 \times 10^{-9}$ to obtain the matrix M_F in equation 5.4 for each transmitted symbol, which corresponds to a standard buried optical fiber. Three different signal return-to-zero ratios were considered.

Eve is underestimated when using smooth min-entropy, ϵ_{PA} is the collision probability of two different input strings can be projected into the same outcome, and ϵ_{EC} is the probability failure of the error correction code.

As one can see in all Figures 5.8-(a), and (b), and in Figures 5.9-(a), and (b) there is an optimum threshold value τ that leads to the longer secure key obtained with the presented DV-QKD system that does not correspond to the minimum sifted key QBER. It is certain that increasing the threshold leads to less errors on the raw key and consequently on the sifted key. However, a high value for τ leads to a decrease on the secret key length. In Figure 5.8 a positive secure key length is obtained for a QBER lower than 9%. In this way, the minimum threshold applied to obtain a valid secure key length should be higher than 0.49 mV, which sets the zero secure key length. Moreover, a maximum on the secure key length for a 40 km optical fiber channel is achieved for a QBER of approximately of 1.5%. This corresponds to a detection threshold of approximately 0.87 mV. In addition, the robustness of the presented system is clear when one compares Figure 5.8-(a) with Figure 5.8-(b). The proposed polarization drift compensation algorithm allows the large deployment of the presented scheme even considering heavy external perturbation that lead to a fast polarization drift, without consuming more bandwidth neither to use extra hardware. Finally, we can also see from Figure 5.8-(a) that for a system operating at 500 MHz symbol generation clock (considering pilot tone and quantum signal), a secure key length of 750 Kbits was generated over approximately 16 ms, with a sifted 1.5% sifted QBER, and a detection threshold of 0.87 mV. Considering a longer optical fiber channel, for a 80 km buried optical fiber channel, a maximum secure key length of

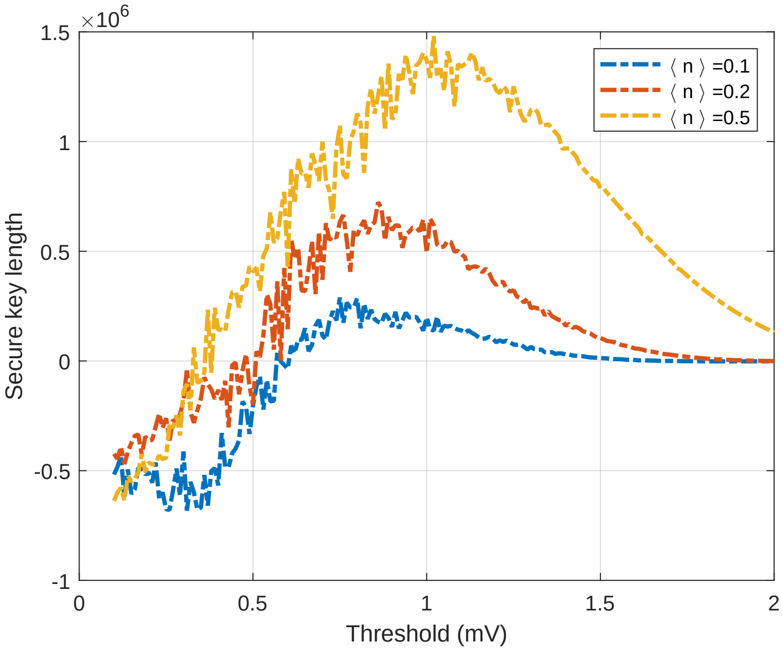


Figure 5.12: Secure key length as a function of the voltage threshold applied in the quadratures calculated using equations 5.18 for different average number of photons per quantum signal pulse. For this simulation, 8 million symbols were transmitted, assuming $P_s = 3$ mW and $\eta_{\text{MZM}} 9.83 \times 10^{-5}$. It was consider a $\sigma = 2 \times 10^{-9}$ to obtain the matrix M_F in equation 5.4 for each transmitted symbol, which corresponds to a standard burried optical fiber. Three different avergare number of photons per quantum signal pulse were considered.

698 Kbits is generated over approximately 16 ms with a QBER of 2.8%, and applying a voltage threshold of 0.77 mV. Moreover, even considering heavy external perturbations the proposed system is able to generate a secure key with a maximum length of 4.3 Kbits over 8 ms with a QBER of 5 % applying a threshold of 1.13 mV. Moreover, when we increase the quantum optical fiber channel length assuming a standard buried optical fiber channel the system shows a decrease of approximately 7 % on the final secret key length. However, for heavy external environments, the system is more sensible to the increase of the length of the quantum optical fiber channel, see Figure 5.9-(a) and (b).

We also assess the performance of the proposed system by varying the both classical and quantum signals return-to-zero ratio. Figure 5.10 shows the secure key length as a function of the threshold voltage applied obtained over a period of 16 ms. Following the same thinking previously presented, besides the optimum threshold that leads to the longest secure key obtained increasing the return-to-zero signal ration also pulls the maximum value upwards. Otherwise, the QBER of the sifted is lower for higher return-to-zero signal ratios on average as shown in Figure 5.11.

Figure 5.12 shows the secure key length as a function of the applied threshold for three different average number of photons per quantum signal pulse. One can see that with the increase of the number of photons per pulse, the final secure key length also increases. However, the increasing of the number of photons per pulse can open security issues when more complex collective attacks are considered. In this work, we consider an individual simple

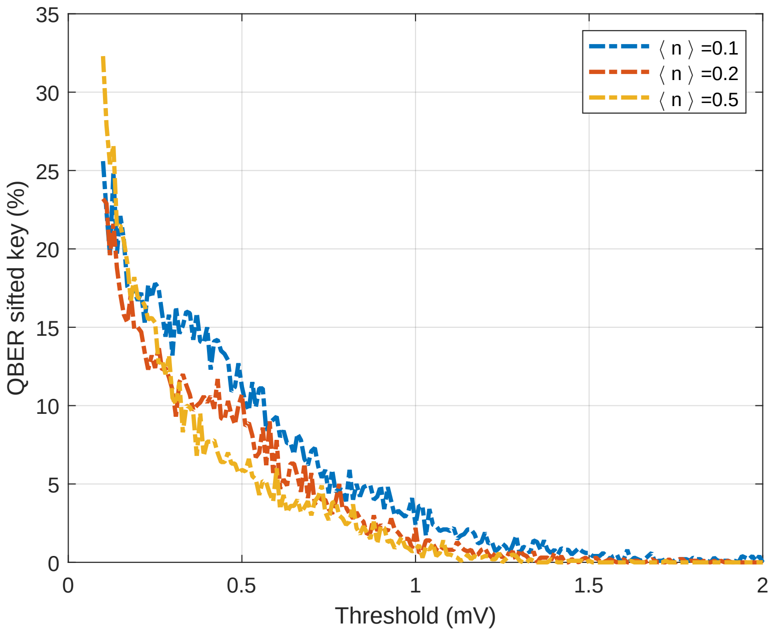


Figure 5.13: QBER of the sifted key as a function of the voltage threshold applied in the quadratures calculated using equations 5.18 for different average number of photons per quantum signal pulse. For this simulation, 8 million symbols were transmitted, assuming $P_s = 3$ mW and $\eta_{\text{MZM}} 9.83 \times 10^{-5}$. It was consider a $\sigma = 2 \times 10^{-9}$ to obtain the matrix M_F in equation 5.4 for each transmitted symbol, which corresponds to a standard burried optical fiber. Three different avergare number of photons per quantum signal pulse were considered.

---

attack but we intend to study more complex attacks in the future, under which the average number of photons per quantum signal pulse can be a critical issue. Furthermore, in Figure 5.13 we show the QBER of the sifted key for different number of photons per pulse, which takes higher values for the lowest average number of photons per pulse as it was expected. In fact, by decreasing the average number of photons per pulse, we are also deacreasing the amount of information that effectively reaches the receiver. Moreover, we are also send information into weakest quantum pulses which leads to more measurement errors since the noise approaches the quantum signal information. In this way, the system noise has more impact when we consider less photons per pulse.

5.6 Final Remarks

In this chapter, we present a novel polarization based DV-QKD system that combines the implementation of quantum states of polarization using phase-modulators with a polarization diversity coherent detection scheme. The deployment of weak quantum signals at high baud-rate are obtained with commercial Mach-Zehnder amplitude modulators followed by a $45\hat{A}$ aligned phase-modulator allowing to switch between states of polarization. On the receiver side the switching of the basis measurement is also performed by a commercial phase-modulator and the states of polarization are measured using standard homodyne detectors. In this way, the proposed system exclusively requires classical hardware, which allows its large deployment in current practical optical fiber networks.

In order to implement the BB84 protocol in the proposed system, two sets of states of polarization orthogonal within each set, and from two non-orthogonal mutually unbiased basis between sets are prepared and measured. Furthermore, the proposed scheme also implements a quantum frame where a time-multiplexed pilot signal is transmitted for phase and amplitude difference compensation between parties, and also for polarization random drift compensation. We showed that the implemented polarization compensation algorithm provides robustness to the implemented system without demanding extra bandwidth consumption, since it is quite insensible to heavy external perturbation. That feature stems from the capability of continuously locate the received SOP though the precise calculation of the Stokes parameters. We implement the DV-QKD BB84 protocol considering 1 GHz clock SOP generation, coherent state source heavily attenuated, electronic and shot noise contributions on the detection scheme, and error correction efficiency different from the Shannon limit. Considering the results in this work, we showed that for a system operating at 500 MHz symbol generation clock (considering pilot tone and quantum signal), a secure key length of 750 Kbits was generated over approximately 16 ms, with a 1.5% sifted QBER, and a detection threshold of 0.87 mV. In this way, the proposed system is able to generate secure keys at a rate of 46.9 MKeys per second with a QBER on the sifted key of 1.5 %. That secret key rate stands as a significant improvement on the current state-of-the-art that reports a final secret key rate of 54.5 kbps [39].

Chapter 6

Conclusions and Future Work

In this chapter, we summarise the main conclusions resulted from the work developed on the scope of this thesis. The work presented in this thesis focused in discrete variables polarization encoded single-photons based quantum communication systems. Although we solved existent issues that were open in the QKD systems implementation, there are other that are still opened. In this way, we also discuss on the future work that may be developed after the conclusion of this thesis.

This chapter contains two sections. In section 6.1, the summary of the main conclusions resulted from the developed work are presented. Section 6.2 is devoted to a discussion on the future work that may follow the presented work.

6.1 Conclusions

The major topics under discussion in this thesis include the experimental implementation of polarized quantum states generation techniques, the imperfections inherent to standard optical fiber based metro networks and how to overcome them when we implement a quantum communication protocol, and on the polarized quantum states detection techniques. In all topics we present a theoretical description which is validated by experimental results or by simulations strongly close to real situations.

We first present the experimental implementation in the laboratory of the discrete variables QKD system, where information is encoded in four different states of single-photons polarization. We start by presenting the current state of the art regarding the main quantum key distribution protocols, for instance the prepare and measure protocols namely the BB84 that relies on the transmission of four states of polarization from two non-orthogonal mutually unbiased bases, the B92 where only two states of polarization from two non-orthogonal bases are prepared, the BBM92 which is the entanglement version of BB84, and the T12 protocol that implements the BB84 with decoy qubits. Furthermore, the state of the art also comprehends various degrees of freedom used to encode information in single-photons, such as the time-phase difference, phase and polarization. Since in this thesis we focus on polarization encoding system, we detail the current polarization based quantum communication systems state of the art, including the preparation techniques of states of polarization, and the measurement techniques advantages and limitations. In this chapter we describe the experimental system implemented in the lab to support the generation and measurement of four states of polarization from two non-orthogonal mutually unbiased bases. We start by presenting the general architecture of the implemented system, which includes three horizontal layers namely the physical-layer, the middleware-layer and the protocol-layer. Each one of those layers performs specific roles with different depth levels, being the protocol-layer the upper-layer, and the physical-layer the lower-layer, where both are connected by the middleware-layer. Moreover, the system may be also divided within three vertical layers namely the transmitter, the communication channel and the receiver. The communication is performed in one direction, more specifically from the transmitter where the quantum states are prepared to the receiver where they are measured. In addition, the communication channel at the upper-layer provides a classical communication channel between parties which allows bi-directional communication. In the implemented experimental system, we chose modulate information into different states of polarization using an EPC, which allowed us to prepare four states of polarization namely $|H\rangle(|V\rangle)$ from rectilinear basis corresponding to bit 0(1), and $|+45\rangle(|-45\rangle)$ from diagonal basis corresponding to bit 0(1). We demonstrated precise quantum states generation at a frequency repetition rate of 500 Hz with an average QBER of 1.8% and a maximum QBER of 2.6% over 21 hours.

Furthermore, we present a method for polarization random drift compensation of a single state of polarization in standard optical-fiber based communication networks. The proposed method is based on the QBER of the reference state induced by the polarization drift. Its representation on the Poincaré sphere provides the location of the rotated state of polarization due the drift suffered over the optical-fiber channel in three iterations at most. The implementation of the method was validated through several simulations. First, we assess the impact of the QBER estimation accuracy for different number of bits used for the estimation, which implies different threshold values for the method to actuate. With the decreasing of the number of bits used to estimate the QBER, the threshold increases, since the possible location area on the Poincaré sphere also increases. Moreover, two different scenarios was considered corresponding to an buried optical-fiber based quantum communication channel, and to an aerial optical-fiber based quantum communication channel. Assuming a QBER threshold of 3% and an ideal receiver, an overhead of 2.54% is required for a 0.8 ms transmission window scenario, and an overhead of 0.31% is required for a 8 ms transmission window scenario. Furthermore, we also consider a real receiver, which led to a maximum overhead of 1% in a 8 ms transmission window, which corresponds to a buried optical-fiber based quantum communication channel. It was demonstrated that this method actively aligns the polarization basis between transmitter and receiver of a particular state of polarization in tens of microseconds with low overhead and without out-of-band signals, which makes it suitable to be applied even in scenarios subject to heavy external perturbations, such as buried optical-fibers in highways, railways, or even aerial optical-fiber installations.

The previous work was extended to propose a novel heuristic method to compensate the polarization random drift of any state of polarization. This method is based on the monitoring of the QBER of two states of polarization from two non-orthogonal mutually unbiased bases. The polarization drift compensation of those two states of polarization provides the compensation of any state of polarization on the Poincaré sphere. The proposed method was validate through numerical simulations considering a quantum key distribution system capable of generate four states of polarization, namely the $|H\rangle$ and $|V\rangle$ from the rectilinear basis, and the $|+45\rangle$ and $|-45\rangle$ from the diagonal basis. An ideal and a real receiver implementation were considered, where the last showed the capability of maintaining the QBER of the data qubits below 2.1% with a 50% bandwidth consumption. Moreover, we were able to conclude that the dead-time parameter of the single-photon detectors has an high impact in the method's performance since it increases the time interval between consecutive symbols, which can lead to uncorrelated consecutive samples used to estimate the QBER. Furthermore, we consider a practical case study where the BB84 protocol was implemented on the system. We demonstrated that the polarization drift compensation method assures long-term key exchanging between parties with a QBER lower than 2% with a 40 km optical-fiber based quantum communication channel using an average number of photons per data and control pulse of 0.2. Furthermore, we also demonstrated that by employing the proposed method in a finite-key implementation of the BB84 protocol, the secrete key generation is improved in 82%, even consuming part of the bandwidth for polarization random drift compensation. Note that, the secret key generation improvement is obtained by dividing the average secret key length in a case where the proposed method is applied, by the secret key length in a case where no compensation method is applied and the compensation is assumed to be instantaneous as soon as the QBER of the sifted key reaches the limit imposed by the BB84 protocol. In addition, we also study the best value to use for the bandwidth consumption and we concluded that 50% of bandwidth consumption leads to the major secret key length. All those calculations were performed using the same transmission window, which implies that in the case of no compensation method is applied, the QBER of the sifted key reaches the limit and no key is generated near that limit.

Moreover, we proposed and validated though numerical simulations a novel polarization-based DV-QKD system that combines the use of phase-modulators for SOP generation and basis switching with a polarization diversity coherent detection scheme. This enables a full implementation of DV-QKD systems using only classical hardware. At transmitter side, high-baud rate low-intensity quantum signals are enabled by using a highly attenuated laser source, and a Mach-Zehnder Modulator followed by 45° aligned Phase Modulator. At receiver side, random basis choice by Bob can be performed using also a 45° aligned Phase Modulator followed by a commercial integrated polarization-diversity coherent receiver. We also propose the implementation of quantum frames with time-multiplexing pilot tone sent by the transmitter to enable the use of a locally generated oscillator at receiver. We propose a theoretical model of the presented system, and we validated it though numerical simulations. We implement the BB84 protocol on the proposed system, where we prepare and measure two sets of states of polarization orthogonal within each set, and from two mutually unbiased bases between sets. We showed that the implemented polarization compensation algorithm provides robustness to the implemented system without demanding extra bandwidth consumption, since it is quite insensible to heavy external perturbation. That feature stems from the capability of continuously locate the received SOP though the precise calculation of the Stokes parameters. Our results open the door to polarization qubits transmission baud-rates of the order of GHz in access and metro networks. We report continuous qubit transmission, even in environments subjected to high polarization drift, without consuming extra-bandwidth with a maximum QBER of 2%. Moreover, we report a secret key generation rate of approximately 46.9 Mbps, with a sifted QBER of 1.5%, and a detection threshold of 0.87 mV, when implementing the BB84 protocol in a system operating at a 1 GHz symbol generation clock over a 40 km standard optical fiber channel.

To conclude, we were able to implement in the laboratory a real-time quantum communication system based on polarization encoded single-photons suitable to support the polarization based QKD and QOKD protocols. Moreover, we also developed methods to allow the implemented system operation outside the laboratory, namely an heuristic method for polarization random drift compensation over optical-fiber metro networks. The final work of this thesis is devoted to the study of the use of coherent detection to improve DV-QKD systems performance, for instance in terms of cost and achievable performance since it allows to achieve transmission rates at the order of Mbps.

6.2 Future Work

The work developed in this thesis obviously did not exhaust all issues in quantum information practical systems that rely on polarization encoded discrete-variables. On the contrary, it also opened new issues to be solved. Within the next steps that can be followed we consider that the following may be interesting to be explored:

- The increasing of the transmission rate in the implemented experimental system described in chapter 2 may be improved by optimizing the encoding and decoding schemes. In order to approach the current state-of-art the EPCs used for polarization modulation may be replaced by phase-modulators, which allow state of polarization generation rates in the order of GHz. Moreover, even achieving that generation rate, the current detection system operates at a maximum of 100 MHz, which is limited by the single-photon detectors rate operating in gated mode. This limitation can be overcame replacing those detectors by superconducting nanowire detectors, or replacing the detection system by the system proposed in chapter 5.

- The polarization drift compensation method proposed in chapter 4 was validated in a practical QKD system through numerical simulations. However, it would be interesting to implement the proposed method on the implemented experimental system described in chapter 2, and compare the obtained results with the results obtained in the numerical simulations. Moreover, move the system to a field environment may be also interesting in order to confirm the method robustness in real-world implementation with the optical-fiber based communication channel subjected to heavy external conditions.

- The security of the system presented in chapter 5 was only assessed considering a simple individual attack from an eavesdropper with limited power. Therefore, the step that should follow this work should be regarding the analyzes of more complex attacks in order to confirm its security.

- An experimental implementation of the DV-QKD system based on homodyne detection may also be interesting to consider.

Appendix A

General VHDL implemented topologies

A.1 DV-quantum transmitter

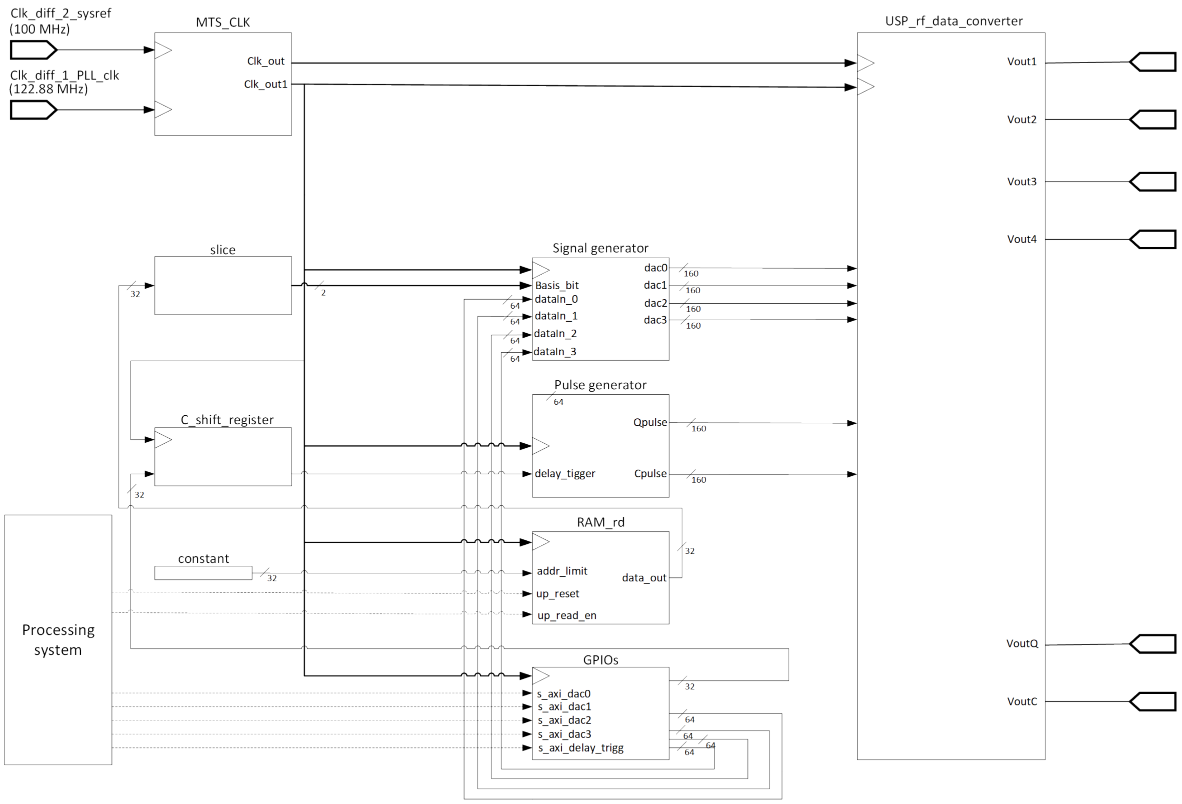


Figure A.1: Topology of the transmitter.

Bibliography

[1] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *arXiv preprint arXiv:1804.00200*, 2018.

[2] F. Maqsood, M. Ahmed, M. M. Ali, and M. A. Shah, "Cryptography: A comparative analysis for modern techniques," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, pp. 442–448, 2017.

[3] M. Roetteler and K. M. Svore, "Quantum computing: Codebreaking and beyond," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 22–36, 2018.

[4] S. P. Jordan and Y.-K. Liu, "Quantum cryptanalysis: Shor, Grover, and beyond," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 14–21, 2018.

[5] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, pp. 188 EP –, Sep 2017.

[6] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Physical Review A*, vol. 54, no. 3, p. 1844, 1996.

[7] W. K. Wootters and W. H. Zurek, "The no-cloning theorem," *Physics Today*, vol. 62, no. 2, pp. 76–77, 2009.

[8] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," in *Advances in Cryptology*, pp. 267–275, Springer, 1983.

[9] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer," in *Annual International Cryptology Conference*, pp. 351–366, Springer, 1991.

[10] C. Crépeau, "Quantum oblivious transfer," *Journal of Modern Optics*, vol. 41, no. 12, pp. 2445–2454, 1994.

[11] A. C.-C. Yao, "Security of quantum protocols against coherent measurements," in *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, pp. 67–75, ACM, 1995.

[12] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the International Conference on Computers, Systems and Signal Processing*, 1984.

[13] N. Gisin, G. , W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[14] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[15] M. Lasota, R. Filip, and V. C. Usenko, "Robustness of quantum key distribution with discrete and continuous variables to channel noise," *Physical Review A*, vol. 95, no. 6, p. 062312, 2017.

[16] Á. J. Almeida, N. J. Muga, N. A. Silva, J. M. Prata, P. S. André, and A. N. Pinto, "Continuous control of random polarization rotations for quantum communications," *Journal of Lightwave Technology*, vol. 34, no. 16, pp. 3914–3922, 2016.

[17] N. J. Muga, M. F. Ferreira, and A. N. Pinto, "QBER estimation in QKD systems with polarization encoding," *Journal of Lightwave Technology*, vol. 29, no. 3, pp. 355–361, 2011.

[18] N. A. Silva and A. N. Pinto, "Effects of losses and nonlinearities on the generation of polarization entangled photons," *Journal of Lightwave Technology*, vol. 31, no. 8, pp. 1309–1317, 2013.

[19] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, no. 1, pp. 1–12, 2016.

[20] M. B. Santos, A. N. Pinto, and P. Mateus, "Quantum and classical oblivious transfer: A comparative analysis," *IET Quantum Communication*, vol. 2, no. 2, pp. 42–53, 2021.

[21] G. Asharov, Y. Lindell, T. Schneider, and M. Zohner, "More efficient oblivious transfer extensions," *Journal of Cryptology*, vol. 30, no. 3, pp. 805–858, 2017.

[22] G. Asharov, Y. Lindell, T. Schneider, and M. Zohner, "More efficient oblivious transfer extensions with security for malicious adversaries," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 673–701, Springer, 2015.

[23] N. J. Muga, M. F. Ramos, S. Mantey, N. A. Silva, and A. N. Pinto, "Deterministic state-of-polarization generation for polarization-encoded optical communications," in *2019 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC)*, pp. 1–3, IEEE, 2019.

[24] N. J. Muga, M. F. Ramos, S. T. Mantey, N. A. Silva, and A. N. Pinto, "Fpga-assisted state-of-polarisation generation for polarisation-encoded optical communications," *IET Optoelectronics*, vol. 14, no. 6, pp. 350–355, 2020.

[25] S. T. Mantey, M. F. Ramos, N. A. Silva, A. N. Pinto, and N. J. Muga, "Algorithm for state-of-polarization generation in polarization-encoding quantum key distribution," in *2021 Telecoms Conference (ConfTELE)*, pp. 1–6, IEEE, 2021.

[26] M. F. Ramos, N. A. Silva, N. J. Muga, and A. N. Pinto, "Reference clock signal distribution for quantum key distribution," in *SBRC Workshop de Comunicação e Computação Quântica WQuantum*, pp. –, August 2021.

[27] M. F. Ramos, N. A. Silva, N. J. Muga, and A. N. Pinto, "Reversal operator to compensate polarization random drifts in quantum communications," *Optics express*, vol. 28, no. 4, pp. 5035–5049, 2020.

[28] M. F. Ramos, N. A. Silva, N. J. Muga, and A. N. Pinto, "Full polarization random drift compensation method for quantum communication," *Optics Express*, vol. 30, pp. 6907–6920, February 2022.

[29] M. F. Ramos, A. N. Pinto, and N. A. Silva, "Polarization based discrete variables quantum key distribution via conjugated homodyne detection," *Scientific Reports*, vol. 12, pp. 1–13, April 2022.

[30] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the internet of things in a quantum world," *IEEE Communications Magazine*, vol. 55, pp. 116–120, 02 2017.

[31] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G.-L. Long, "Implementation and security analysis of practical quantum secure direct communication," *Light: Science & Applications*, vol. 8, no. 1, p. 22, 2019.

[32] S. Chandra, S. Bhattacharyya, S. Paira, and S. S. Alam, "A study and analysis on symmetric cryptography," in *2014 International Conference on Science Engineering and Management Research (ICSEMR)*, pp. 1–8, IEEE, 2014.

[33] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[34] C. Cesare, "Online security braces for quantum revolution," *Nature News*, vol. 525, no. 7568, p. 167, 2015.

[35] L.-J. Wang, K.-Y. Zhang, J.-Y. Wang, J. Cheng, Y.-H. Yang, S.-B. Tang, D. Yan, Y.-L. Tang, Z. Liu, Y. Yu, *et al.*, "Experimental authentication of quantum key distribution with post-quantum cryptography," *npj Quantum Information*, vol. 7, no. 1, pp. 1–7, 2021.

[36] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, no. 2, p. 025002, 2020.

[37] L. Goldenberg and L. Vaidman, "Quantum cryptography based on orthogonal states," *Physical Review Letters*, vol. 75, no. 7, p. 1239, 1995.

[38] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of modern physics*, vol. 81, no. 3, p. 1301, 2009.

[39] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Performance and security of 5 GHz repetition rate polarization-based quantum key distribution," *Applied Physics Letters*, vol. 117, no. 14, p. 144003, 2020.

[40] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, *et al.*, "10-Mb/s quantum key distribution," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, 2018.

[41] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Physical review letters*, vol. 121, no. 19, p. 190502, 2018.

[42] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[43] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, "Unconditional security of the bennett 1992 quantum-key-distribution scheme with a strong reference pulse," *Physical Review A*, vol. 80, no. 3, p. 032302, 2009.

[44] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, no. 14, p. 3018, 1998.

[45] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell theorem," *Physical review letters*, vol. 68, no. 5, p. 557, 1992.

[46] A. K. Ekert, "Quantum cryptography based on Bell theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[47] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Optics express*, vol. 21, no. 21, pp. 24550–24565, 2013.

[48] J. Wang, X. Qin, Y. Jiang, X. Wang, L. Chen, F. Zhao, Z. Wei, and Z. Zhang, "Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units," *Optics express*, vol. 24, no. 8, pp. 8302–8309, 2016.

[49] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, *et al.*, "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[50] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Optics express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[51] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature photonics*, vol. 7, no. 5, pp. 378–381, 2013.

[52] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Scientific reports*, vol. 6, no. 1, pp. 1–9, 2016.

[53] G. Ribordy, N. Gisin, O. Guinnard, D. Stuck, M. Wegmuller, and H. Zbinden, "Photon counting at telecom wavelengths with commercial InGaAs/InP avalanche photodiodes: current performance," *Journal of modern optics*, vol. 51, no. 9-10, pp. 1381–1398, 2004.

[54] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber," *Physical review letters*, vol. 98, no. 1, p. 010503, 2007.

[55] T. Honjo, K. Inoue, and H. Takahashi, “Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit mach–zehnder interferometer,” *Optics letters*, vol. 29, no. 23, pp. 2797–2799, 2004.

[56] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, “Experimental measurement-device-independent quantum key distribution,” *Phys. Rev. Lett.*, vol. 111, p. 130502, Sep 2013.

[57] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, “Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks,” *Phys. Rev. Lett.*, vol. 111, p. 130501, Sep 2013.

[58] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, “Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits,” *Phys. Rev. A*, vol. 88, p. 052303, Nov 2013.

[59] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, “Quantum key distribution without detector vulnerabilities using optically seeded lasers,” *Nature Photonics*, vol. 10, no. 5, pp. 312–315, 2016.

[60] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, “Measurement-device-independent quantum key distribution over a 404 km optical fiber,” *Phys. Rev. Lett.*, vol. 117, p. 190501, Nov 2016.

[61] K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, and Y. Arakawa, “Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors,” *Scientific Reports*, vol. 5, p. 14383, 2015.

[62] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, *et al.*, “Experimental demonstration of free-space decoy-state quantum key distribution over 144 km,” *Physical Review Letters*, vol. 98, no. 1, p. 010504, 2007.

[63] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” *Nature Photonics*, vol. 8, no. 8, p. 595, 2014.

[64] H. Zhou, Y. Zhu, J. Wang, Y. Su, Z. Xu, C. Wu, J. Zhao, Y. Wang, M. He, L. Jianhua, *et al.*, “Quantum key distribution with silent active polarization compensation without a reference optical beam,” in *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, pp. 1–4, IEEE, 2015.

[65] Y. Yu, W. Li, Y. Wei, Y. Yang, S. Dong, T. Qian, S. Wang, Q. Zhu, S. Zheng, X. Zhang, *et al.*, “Experimental demonstration of underwater decoy-state quantum key distribution with all-optical transmission,” *Optics Express*, vol. 29, no. 19, pp. 30506–30519, 2021.

[66] Y.-p. Yuan, C. Du, Q.-q. Shen, J.-d. Wang, Y.-f. Yu, Z.-j. Wei, Z.-x. Chen, and Z.-m. Zhang, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution based on intrinsically stable polarization-modulated units," *Optics express*, vol. 28, no. 8, pp. 10772–10782, 2020.

[67] Y. Li, Y.-H. Li, H.-B. Xie, Z.-P. Li, X. Jiang, W.-Q. Cai, J.-G. Ren, J. Yin, S.-K. Liao, and C.-Z. Peng, "High-speed robust polarization modulation for quantum key distribution," *Optics letters*, vol. 44, no. 21, pp. 5262–5265, 2019.

[68] C. Agnesi, M. Avesani, L. Calderaro, A. Stanco, G. Foletto, M. Zahidy, A. Scriminich, F. Vedovato, G. Vallone, and P. Villoresi, "Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder," *Optica*, vol. 7, no. 4, pp. 284–290, 2020.

[69] A. Duplinskiy, V. Ustimchik, A. Kanapin, V. Kurochkin, and Y. Kurochkin, "Low loss qkd optical scheme for fast polarization encoding," *Optics Express*, vol. 25, no. 23, pp. 28886–28897, 2017.

[70] Á. J. Almeida, N. J. Muga, N. A. Silva, A. D. Stojanovic, P. S. André, A. N. Pinto, J. Mora, and J. Capmany, "Enabling quantum communications through accurate photons polarization control," in *8th Iberoamerican Optics Meeting and 11th Latin American Meeting on Optics, Lasers, and Applications*, vol. 8785, p. 8785CG, International Society for Optics and Photonics, 2013.

[71] G. Agrawal, *Lightwave technology : components and devices / Govind P. Agrawal.* 06 2005.

[72] Y.-Y. Ding, H. Chen, S. Wang, D.-Y. He, Z.-Q. Yin, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Polarization variations in installed fibers and their influence on quantum key distribution systems," *Optics Express*, vol. 25, no. 22, pp. 27923–27936, 2017.

[73] T. Pengyi, L. Guochun, G. Song, Y. Gang, D. Yunqi, X. Yao, L. Dongdong, Z. Yinghua, W. Bing, Z. Ziyan, G. Dequan, L. Jianhong, and W. Jian, "Fast polarization feedback algorithm for quantum key distribution with aerial fiber for power grid," *Acta Optica Sinica*, vol. 38, no. 1, p. 0106005, 2018.

[74] R. Liu, H. Yu, J. Zan, S. Gao, L. Wang, M. Xu, J. Tao, J. Liu, Q. Chen, and Y. Zhao, "Analysis of polarization fluctuation in long-distance aerial fiber for QKD system design," *Optical Fiber Technology*, vol. 48, pp. 28–33, 2019.

[75] C. B. Czegledi, M. Karlsson, E. Agrell, and P. Johannisson, "Polarization drift channel model for coherent fibre-optic systems," *Scientific reports*, vol. 6, p. 21217, 2016.

[76] Y.-Y. Ding, W. Chen, H. Chen, C. Wang, S. Wang, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, "Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits," *Optics Letters*, vol. 42, no. 6, pp. 1023–1026, 2017.

[77] G. Xavier, G. V. de Faria, G. Temporão, and J. Von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding," *Optics Express*, vol. 16, no. 3, pp. 1867–1873, 2008.

[78] D.-D. Li, S. Gao, G.-C. Li, L. Xue, L.-W. Wang, C.-B. Lu, Y. Xiang, Z.-Y. Zhao, L.-C. Yan, Z.-Y. Chen, G. Yu, and J.-H. Liu, “Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback,” *Optics Express*, vol. 26, no. 18, pp. 22793–22800, 2018.

[79] G. Xavier, N. Walenta, G. V. De Faria, G. Temporão, N. Gisin, H. Zbinden, and J. Von der Weid, “Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation,” *New Journal of Physics*, vol. 11, no. 4, p. 045015, 2009.

[80] J. Chen, G. Wu, Y. Li, E. Wu, and H. Zeng, “Active polarization stabilization in optical fibers suitable for quantum key distribution,” *Optics Express*, vol. 15, no. 26, pp. 17928–17936, 2007.

[81] J. Chen, G. Wu, L. Xu, X. Gu, E. Wu, and H. Zeng, “Stable quantum key distribution with active polarization control based on time-division multiplexing,” *New Journal of Physics*, vol. 11, no. 6, p. 065004, 2009.

[82] D. H. Goldstein, *Polarized Light, revised and expanded.* CRC, 2003.

[83] N. J. Muga, A. N. Pinto, M. F. Ferreira, and J. R. F. da Rocha, “Uniform polarization scattering with fiber-coil-based polarization controllers,” *Journal of Lightwave Technology*, vol. 24, no. 11, pp. 3932–3943, 2006.

[84] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, “Advances in InGaAs/InP single-photon detector systems for quantum communication,” *Light: Science & Applications*, vol. 4, no. 5, p. e286, 2015.

[85] L. Bouchoucha, S. Berrah, and M. Sellami, “Influence of experimental parameters inherent to optical fibers on quantum key distribution, the protocol BB84,” *Semiconductor Physics, Quantum Electronics & Optoelectronics*, vol. 21, no. 1, pp. 73–79, 2018.

[86] M. Lopes and N. Sarwade, “On the performance of quantum cryptographic protocols SARG04 and KMB09,” in *2015 International Conference on Communication, Information Computing Technology (ICCICT)*, pp. 1–6, Jan 2015.

[87] G. P. Agrawal, *Lightwave technology: telecommunication systems.* John Wiley & Sons, 2005.

[88] ID Quantique, *id210-SMF or -MMF Advanced System for Single Photon Detection, User Manual*, 2013. Version 1.3.

[89] J. Dynes, A. Wonfor, W.-S. Tam, A. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. Dixon, J. Cho, *et al.*, “Cambridge quantum network,” *npj Quantum Information*, vol. 5, no. 1, pp. 1–8, 2019.

[90] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling, *et al.*, “A trusted node–free eight-user metropolitan quantum communication network,” *Science advances*, vol. 6, no. 36, p. eaba0959, 2020.

[91] M. Karlsson, J. Brentel, and P. A. Andrekson, “Long-term measurement of pmd and polarization drift in installed fibers,” *Journal of Lightwave Technology*, vol. 18, no. 7, pp. 941–951, 2000.

[92] A. V. Sergienko, “Experimental cryptography using continuous polarization states,” in *Quantum Communications and Cryptography*, pp. 111–133, CRC Press, 2018.

[93] I. B. Djordjevic, *Quantum-Key Distribution (QKD) Fundamentals*, pp. 211–265. Cham: Springer International Publishing, 2019.

[94] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, “Proof-of-concept of real-world quantum key distribution with quantum frames,” *New Journal of Physics*, vol. 11, no. 9, p. 095001, 2009.

[95] Y. Shi, H. S. Poh, A. Ling, and C. Kurtsiefer, “Fibre polarization state compensation in entanglement-based quantum key distribution,” *arXiv preprint arXiv:2107.07654*, 2021.

[96] L. Xi, X. Zhang, F. Tian, X. Tang, X. Weng, G. Zhang, X. Li, and Q. Xiong, “Optimizing the operation of $\mathrm{LiNbO_3}$ -based multistage polarization controllers through an adaptive algorithm,” *IEEE Photonics Journal*, vol. 2, no. 2, pp. 195–202, 2010.

[97] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” *Physical Review A*, vol. 61, no. 5, p. 052304, 2000.

[98] R. Y. Cai and V. Scarani, “Finite-key analysis for practical implementations of quantum key distribution,” *New Journal of Physics*, vol. 11, no. 4, p. 045024, 2009.

[99] D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, “Experimental quantum key distribution with finite-key security analysis for noisy channels,” *Nature communications*, vol. 4, no. 1, pp. 1–8, 2013.

[100] P. Chaiwongkhot, S. Sajeed, L. Lydersen, and V. Makarov, “Finite-key-size effect in a commercial plug-and-play QKD system,” *Quantum Science and Technology*, vol. 2, no. 4, p. 044003, 2017.

[101] B. Qi, P. Lougovski, and B. P. Williams, “Characterizing photon number statistics using conjugate optical homodyne detection,” *Optics express*, vol. 28, no. 2, pp. 2276–2290, 2020.

[102] Y. Cheng and Z. Lou, “A brief review of linear regression estimation in quantum tomography,” in *2020 39th Chinese Control Conference (CCC)*, pp. 5813–5817, IEEE, 2020.

[103] E. Lavie, I. W. Primaatmaja, W. Y. Kon, C. Wang, and C. C. W. Lim, “Estimating the photon-number distribution of photonic channels with realistic devices and applications in photonic quantum information processing,” *arXiv preprint arXiv:2102.08419*, 2021.

[104] B. Qi, “Bennett-brassard 1984 quantum key distribution using conjugate homodyne detection,” *Physical Review A*, vol. 103, no. 1, p. 012606, 2021.

[105] I. W. Primaatmaja, C. C. Liang, G. Zhang, J. Y. Haw, C. Wang, and C. C.-W. Lim, “Discrete-variable quantum key distribution with homodyne detection,” *arXiv preprint arXiv:2109.00492*, 2021.

[106] M. Jofre, A. Gardelein, G. Anzolin, G. Molina-Terriza, J. Torres, M. Mitchell, and V. Pruneri, "100 mhz amplitude and polarization modulated optical source for free-space quantum key distribution at 850 nm," *Journal of lightwave technology*, vol. 28, no. 17, pp. 2572–2578, 2010.

[107] D. Pereira, M. Almeida, M. Facão, A. N. Pinto, and N. A. Silva, "Impact of receiver imbalances on the security of continuous variables quantum key distribution," *EPJ Quantum Technology*, vol. 8, no. 22, pp. 1–12, 2021.

[108] R. Loudon, *The Quantum Theory of Light.* Clarendon Press, third ed., 2000.

[109] E. Ip and J. Kahn, "Power spectra of return-to-zero optical signals," *Journal of Lightwave Technology*, vol. 24, no. 3, pp. 1610–1618, 2006.

[110] C. Vinegoni, M. Karlsson, M. Petersson, and H. Sunnerud, "The statistics of polarization-dependent loss in a recirculating loop," *Journal of lightwave technology*, vol. 22, no. 4, p. 968, 2004.

[111] J. Capmany and C. FernÃ¡ndez-Pousa, "Quantum modelling of electro-optic modulators," *Laser & Photonics Reviews*, vol. 5, no. 6, pp. 750–772, 2011.

[112] M. Almeida, D. Pereira, M. Facão, A. N. Pinto, and N. A. Silva, "Impact of imperfect homodyne detection on measurements of vacuum states shot noise," *Optical and Quantum Electronics*, vol. 52, no. 11, pp. 1–13, 2020.

[113] S. Bottacchi, *Noise and Signal Interference in Optical Fiber Transmission Systems: An Optimum Design Approach.* John Wiley & Sons, Ltd, first ed., 2008.

[114] N. Korolkova, G. Leuchs, R. Loudon, T. C. Ralph, and C. Silberhorn, "Polarization squeezing and continuous-variable polarization entanglement," *Phys. Rev. A*, vol. 65, p. 052306, Apr 2002.