UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Artificial intelligence solutions for quantum communications

Seyed Morteza Ahmadian

Universitat Politècnica de Catalunya

Optical Communications Group

Artificial Intelligence Solutions for Quantum Communications

Seyed Morteza Ahmadian

Advisor:

Dr. Luis Velasco

Co-advisor:

Dr. Marc Ruiz

A thesis presented in partial fulfilment of the requirements for the degree of

Philosophy Doctor

June 16th, 2023

Optical Communications Group (GCO)

Universitat Politècnica de Catalunya (UPC)

C/ Jordi Girona, 1-3

Campus Nord, D4-2013

08034 Barcelona, Spain

Acknowledgements

First and foremost, I am extremely grateful to my supervisors, Prof. Luis Velasco and Prof. Marc Ruiz for their indispensable advice, continuous support, and patience during my PhD study. Their immense knowledge and plentiful experience have encouraged me in all the time of my academic research and daily life. I would also like to thank Prof. Ben Yoo for accepting and supporting me to work within their group in University of California, Davis, USA. Although in-person collaboration was not possible, our collaboration in the NGIAtlantic project provided me bunch of skills and experiences in my carrier and in my life.

I would like to thank all the colleagues, Fatemeh, Sima, Mariano, Masab, Diogo, Hailey, Shaoxuan and Pol for the cherished time spent together in the GCO lab, and all my colleagues in USA whose contribution in my life is unforgettable.

Finally, I would like to express my gratitude to my parents, my brothers, my sister, and my friends. Without their tremendous understanding and encouragement in the past few years, it would be impossible for me to complete my study.

Abstract

Quantum key Distribution (QKD) has become mature in closed, controlled scenarios. In Polarization encoded QKD optical systems, a Quantum Transmitter (QTx) sends specific polarizations of single photons, i.e., quantum bit (qubit), to a Quantum Receiver (QRx), which decodes them and generates a raw key of a defined length. The raw key is then distilled, using a parallel public channel, established between transmitter and receiver, to correct possible detection errors due to optical transmission and generate a shared secret key. Since optical eavesdropping generates high quantum Bit Error Rate (qBER), key distillation enables its detection.

On a one hand, eavesdropping in between transmitter and receiver can be detectable by both quantum mechanics principles in quantum channel and key distillation procedure in classical channel. First, in the quantum channel, eavesdropper inevitably (based on quantum mechanics) remains signature in the cipher-text transmitted, then key distillation procedure in classical channel can detect this signature by computing the qBER.

On the other hand, Quantum channel can be implemented in whether free space or aerial cable optical channels. Quantum channel based on aerial optical cables can be subject to different environmental events such as wind or thunderstorms. These environmental events have also impact on increasing the qBER in the key distillation procedure.

Researchers are working on distinguishing between high qBER as a result of eavesdropping or environmental events in aerial fibers, to reduce false eavesdropping detection, and increase effective Key Exchange Rate (KER) in QKD protocols. All false eavesdropping detection mitigation as a result of environmental impacts in the literature are reactive.

In this Ph.D. We are going to suggest solutions for compensating these environmental impacts based on proactive solutions hiring Artificial Intelligence

(AI). In fact, we predict the quantum states in next moments of quantum communication and proactively make a good decision to adjust the system in a way that mitigate the negative environmental impacts. This precautionary measure can improve significantly the false eavesdropping detection and KER in the literature.

Firstly, this Ph.D. thesis targets the disturbance compensation in quantum channel as a result of environmental impact to aerial fibers by utilizing AI. Although there are already commercial and research systems that use special hardware or multiplexing technologies, there is considerable space to investigate how AI can foster quantum parties to have higher KER.

Secondly, this Ph.D. thesis aims to use Digital Twin (DT) to fill the gap between virtual QKD systems based on simulations and theories and optical components that should generate real quantum keys in the network. Because quantum (optical) infrastructures lack precision and final implementations are suffering from low KER. Taking advantage of DT, we would be able to rise the key rate and discern eavesdropping from high qBER in the QKD system.

Resumen

La distribución de claves cuánticas (QKD) ha madurado en escenarios cerrados y controlados. En los sistemas ópticos QKD codificados por polarización, un transmisor cuántico (QTx) envía polarizaciones específicas de fotones individuales, es decir, bits cuánticos (qubit), a un receptor cuántico (QRx), que los decodifica y genera una clave sin procesar de una longitud definida. Luego, la clave sin procesar se destila, utilizando un canal público paralelo, establecido entre el transmisor y el receptor, para corregir posibles errores de detección debido a la transmisión óptica y generar una clave secreta compartida. Dado que las escuchas ópticas generan una tasa de error de bit cuántica alta (qBER), la destilación de claves permite su detección.

Por un lado, las escuchas entre el transmisor y el receptor pueden detectarse tanto por los principios de la mecánica cuántica en el canal cuántico como por el procedimiento de destilación clave en el canal clásico. Primero, en el canal cuántico, el intruso inevitablemente (basado en la mecánica cuántica) permanece como firma en el texto cifrado transmitido, luego el procedimiento de destilación de claves en el canal clásico puede detectar esta firma calculando el qBER.

Por otro lado, el canal Quantum se puede implementar en canales ópticos de cable aéreo o de espacio libre. El canal cuántico basado en cables ópticos aéreos puede estar sujeto a diferentes eventos ambientales como viento o tormentas eléctricas. Estos eventos ambientales también tienen un impacto en el aumento del qBER en el procedimiento de destilación clave.

Los investigadores están trabajando para distinguir entre qBER alto como resultado de escuchas o eventos ambientales en las fibras aéreas, para reducir la detección de escuchas falsas y aumentar la tasa de intercambio de claves (KER) efectiva en los protocolos QKD. Todas las mitigaciones de detección de escuchas falsas como resultado de impactos ambientales en la literatura son reactivas.

En este Ph.D. Vamos a sugerir soluciones para compensar estos impactos ambientales basadas en soluciones proactivas contratando Inteligencia Artificial

(IA). De hecho, predecimos los estados cuánticos en los próximos momentos de la comunicación cuántica y tomamos una buena decisión de manera proactiva para ajustar el sistema de manera que mitigue los impactos ambientales negativos. Esta medida de precaución puede mejorar significativamente la detección de escuchas falsas y KER en la literatura.

En primer lugar, este Ph.D. La tesis se enfoca en la compensación de perturbaciones en el canal cuántico como resultado del impacto ambiental en las fibras aéreas mediante el uso de IA. Aunque ya existen sistemas comerciales y de investigación que utilizan hardware especial o tecnologías de multiplexación, existe un espacio considerable para investigar cómo la IA puede fomentar que las fiestas cuánticas tengan un KER más alto.

En segundo lugar, este Ph.D. La tesis tiene como objetivo utilizar Digital Twin (DT) para llenar el vacío entre los sistemas QKD virtuales basados en simulaciones y teorías y los componentes ópticos que deberían generar claves cuánticas reales en la red. Porque las infraestructuras cuánticas (ópticas) carecen de precisión y las implementaciones finales sufren de KER bajo. Aprovechando DT, seríamos capaces de aumentar la tasa de clave y discernir las escuchas desde alto qBER en el sistema QKD.

Table of Contents

List of Figures

Page

List of Tables

Page

Chapter 1

Introduction

1.1 Motivation

Quantum mechanics provides unconditional and unlimited security based on the fundamental properties of quantum particles. The no-cloning theorem states that quantum particles cannot be copied, and measuring quantum particles causes them to collapse onto their measurement basis. By leveraging these properties, unlimited security can be achieved because any action by an eavesdropper leaves a signature on the quantum particle. This security is not a result of the architecture or design of the system, but rather the principles of quantum mechanics.

Out of all the quantum cryptographic systems, QKD [Ma17] is receiving the most attention due to its ability to offer a system design that can be tailored to existing optical equipment in the industry. QKD is capable of generating unlimitedly secure keys that can be used for encryption and decryption of plaintext in telecommunication networks.

Telecommunication networks use various QKD protocols, including discrete variable (DV) and continuous variable (CV) protocols, as well as entanglement-based protocols. Each protocol has its own advantages and disadvantages, and a direct comparison is not always possible as different protocols require different physical layer components. Although DV-QKD is the first and simplest protocol, its unlimited security feature has gained more support from both the industry and academic communities. This is because it uses single photons that cannot be accessed or tampered with by an eavesdropper. In contrast, CV-QKD uses typical optical waves with already defined optical infrastructures, which may result in some security issues [Yu12].

Various DV-QKD protocols have been defined and established, and they can be broadly classified into three main categories: polarization, phase, and time bin encoded systems. Among these, the polarization encoded QKD system is the most commonly used and widely adopted protocol. This is due to the availability of a large body of literature reporting related experiments in controlled scenarios. (see, e.g., [Ag19], [Kh20], [Du18], [Me20]).

Polarization encoded quantum key distribution (DV-QKD) optical systems operate by transmitting specific polarizations of single photons (qubits) from a quantum transmitter (QTx) to a quantum receiver (QRx), which decodes them and generates a raw key of a pre-defined length. To correct possible detection errors that may arise due to optical transmission and generate a shared secret key, the raw key is then distilled using a parallel public channel established between the transmitter and receiver. Key distillation is essential in detecting optical eavesdropping, as it can generate a high quantum bit error rate (qBER).

On the one hand, it is possible to detect eavesdropping between a quantum transmitter and receiver through both quantum mechanics principles in the quantum channel and the key distillation procedure in the classical channel. Firstly, the eavesdropper inevitably leaves a signature in the ciphertext transmitted through the quantum channel, according to the principles of quantum mechanics. Secondly, the classical key distillation procedure can detect this signature by calculating the qBER.

On the other hand, quantum channels can be implemented using either free space or aerial cable optical channels. However, quantum channels based on aerial optical cables are subject to various environmental events, such as wind or thunderstorms, which can have an impact on the key distillation procedure by increasing the qBER.

To reduce false eavesdropping detection and increase the effective key error rate (KER) in quantum key distribution (QKD) protocols, researchers are currently working on developing methods to distinguish between high qBER resulting from eavesdropping and that resulting from environmental events in aerial fibers. This would enable a more accurate detection of eavesdropping and, therefore, increase the security of QKD protocols.

It is worth noting that all existing mitigation methods for false eavesdropping detection resulting from environmental impacts in the literature are reactive in nature. However, we propose a proactive approach using AI to compensate for these environmental impacts. Our approach involves predicting the quantum states in the next moments of quantum communication and making proactive adjustments to the system to mitigate the negative environmental impacts. This precautionary measure has the potential to significantly improve false eavesdropping detection and the KER in the literature.

1.2 Goals of the thesis

In light of the above, this Ph.D. thesis targets the disturbance compensation in quantum channel as a result of environmental impact to aerial fibers by utilizing AI. Although there are already commercial and research systems that use special hardware or multiplexing technologies, there is considerable space to investigate how AI can foster quantum parties to have higher KER.

This Ph.D. thesis focuses on the application of intelligent models to DV-QKD protocol. Tree specific goals are defined to achieve this main goal.

G.1 – AI for Discrete Variable Quantum Key Distribution

This goal targets at providing AI based polarization drift compensation for transmitting discrete photons in quantum channel.

In order to fully achieve this goal, we need to tackle two specific sub-goals:

G1.1 – AI based State of Polarization (SOP) tracking: In this sub-goal, we will design AI based polarization drift compensation in quantum channel. The SOP trajectory will be predicted in the next moments of different environmental events. Here, we should use SOP recognition procedure in QRx and different interpolation methods for planning the compensational rotation should be studied.

G1.2 – Heuristic based rotation manager in BB84 protocol: In this sub-goal, we will design heuristic-based compensation on BB84 standard protocol, which minimum rotations are applied to the receiving photons to prevent the reduction in key rate generation.

G.2 – Experimental assessment of SOP compensation in DV-QKD

This goal targets at addressing the drawback of polarization encoded QKD systems which are: a) the requirements for quantum transmitters and receivers. b) the need of carefully selecting the fibers supporting the quantum channel to minimize the environmental effects that could dramatically change the SOP of photons.

In order to fully achieve this goal, we need to tackle two specific sub-goals:

G2.1 – Set-up the experimental platform and adapt software modules: In this sub-goal, we set up an experimental platform which is being used in the polarization encoded QKD system. Software modules needed for a fast QKD system will be adopted based on uncalibrated platform's components.

G2.2 – Preliminary and final experiments and analysis of results: In this sub-goal, platform validation, fine tuning, and issue solving as well as first fast QKD method will be evaluated. We will ensure the requirements needed for the final experiments and KPI measurements.

G.3 - DT for Discrete Variable Quantum Key Distribution

The aim of this objective is to develop Digital Twin (DT) models that can address the shortcomings of the DV-QKD system, which cannot be achieved through the use of AI-based systems in goal G.1.

In order to fully achieve this goal, we need to tackle two specific sub-goals:

G3.1 – Improvement of AI based SOP compensation: In this sub-goal, DT is helping different AI models to take proper actions against higher velocity environmental events

G3.2 - Eavesdropping detection in BB84 protocol: In this sub-goal, DT targets at detecting eavesdropping actions in quantum channel. Evidences collected from physical component layer can reveal those actions.

A summary of the goals of the thesis is presented in Table 1-1.

Table 1-1: Thesis goals

Goals	
G1 – AI for Discrete Variable Quantum Key Distribution	**G1.1 - AI based State of Polarization tracking**
	G.1.2 - AI based rotation manager in BB84 protocol
G.2 – Experimental verification of SOP compensation in DV-QKD	**G2.1 – Set-up the experimental platform and adapt software modules**
	G2.2 – Preliminary and final experiments and analysis of results
G3 – DT for Discrete Variable Quantum Key Distribution	**G3.1 - Improvement of AI based SOP compensation**
	G.3.2 - Eavesdropping detection in BB84 protocol

1.3 Methodology

This doctoral thesis is premised on the methodology depicted in Figure 1-1. The notion of compensating for changes in SOP that occur when light passes through an unfixed fiber led to the formulation of the central idea of this thesis. In order to accomplish this objective, a number of issues that required attention were carefully considered. Given that DV-QKD was the focus of this study, the primary challenge was how to detect the SOP of photons in the quantum channel. Subsequently, an algorithm for this recognition, as well as a data analysis algorithm, were developed, and the implementation procedure was initiated. The algorithm was implemented and simulated in Python, with numerous iterations and modifications undertaken in order to generate appropriate results. Following the collection of all results, the dissemination process began, culminating in the publication of one journal paper

During the recognition of the SOP, experimental assessments demonstrated its usefulness in examining and validating the algorithm, which was not previously addressed in the quantum communication literature. The algorithms were subsequently adopted and implemented in an experimental testbed established at UCDavis. Multiple adjustment procedures were conducted between the testbed and software modules, as the optical components exhibited non-ideal behavior. The collected results were adequate, and the findings were disseminated.

Following the analysis of the results from the experimental assessment, novel ideas emerged. Subsequently, issues related to the application of the idea to DV-QKD systems were identified in a similar manner. This led to the development of modeling and decision theory solutions, as well as the design of corresponding algorithms. Furthermore, algorithms for partial SOP recognition of photons were also devised. The implementation of these algorithms and the simulation results involved several iterations and modifications to generate precise results. Ultimately, all of the findings and ideas were compiled and submitted to a journal paper.

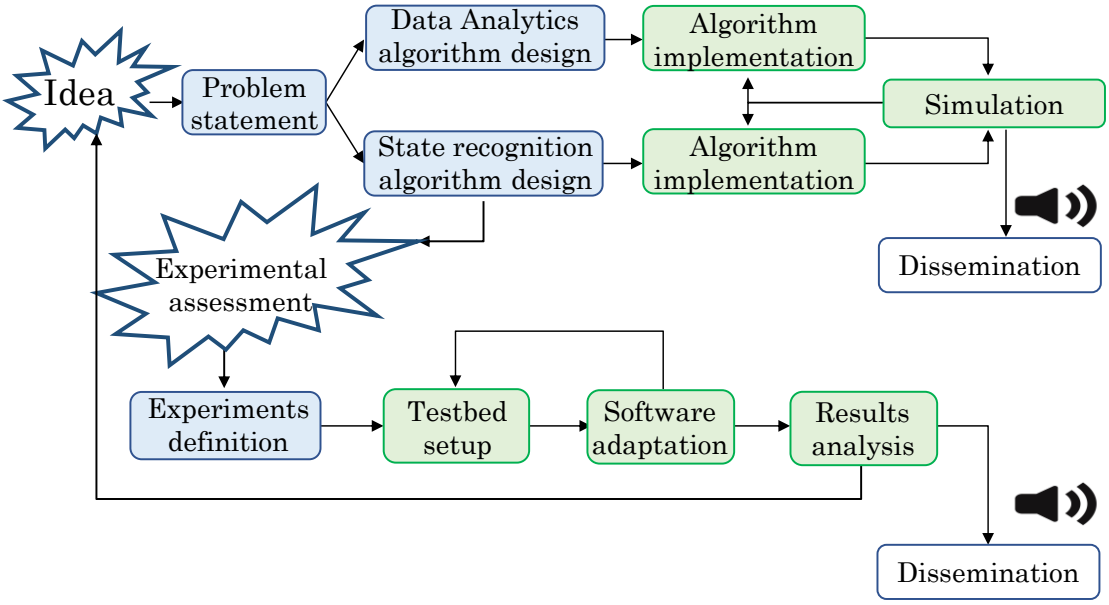


Figure 1-1- Methodology

DV-QKD protocols are being implemented in Python, specifically utilizing qiskit [Qi21]. Additionally, AI is employed in the form of the pytorch [To21] library, which is also implemented in Python. Following the generation of qubits and compensating for any deviations, the key distillation engine utilizing the cascade error correction protocol is implemented in C++. Qubit deviation is applied by an experimental dataset [Bo17] in which the SOP of the transmitting signal measured when a robotic arm move the fiber in different ways. By computing the qBER and KER of the system, the impact of our correction procedure is assessed and compared with other correction methods. Furthermore, DT models are implemented using qiskit and py-pol (Python polarization) library in python, which simulates the behavior of optical devices.

1.4 Thesis outline

The remainder of this Ph.D. thesis is organized as follows.

Chapter 2 briefly reviews the background needed for the objectives of this Ph.D. thesis. Quantum mechanics principles for qubit generation, distortion and measurement (including SOP measurement for distortion detection) based on polarization-encoded systems are explained. Polarization-encoded QKD systems are also presented starting from qubit emission and measurement to privacy amplification in key distillation procedure. DT models are also described in this chapter.

In Chapter 3, a brief review of the current state-of-the-art related to the objectives of this Ph.D. thesis is presented. While the focus of this thesis is on polarization-encoded QKD systems, various compensation methods in continuous-variable QKD systems in the literature are also discussed in order to provide readers with a broader understanding of the field. Additionally, for DT models, other model-based methods for compensation in any type of QKD system are described.

Chapter 4 focuses on goal G.1 and covers AI for DV-QKD. In this chapter, first the method to recognize the SOP of the receiving photons during monitoring intervals are discussed. Then how to plan the compensations' time between monitoring intervals assisted by a greedy exhaustive method is presented. At the end, the methods and algorithms are verified by the results. This chapter is based on one journal publication [JLT22].

Chapter 5 focuses on goal G.2 and covers experimental assessment of SOP compensation in DV-QKD systems. This chapter is based on a collaboration between UPC and UCDavis universities in a project. All results are verified on a testbed deployed at UCDavis. One conference publication [ECOC22] is published based on this chapter.

Chapter 6 relates to goal G.3 and investigates how DT can improve DV-QKD. The chapter focuses on two goals. The first is to distinguish between a high qBER resulting from environmental factors that impact the quantum channel, and a high qBER caused by eavesdropping. The second goal is to develop compensation techniques for environmental events under more challenging conditions. This chapter is based on one Journal publication that is submitted in [JLT23].

Finally, Chapter 7 concludes this Ph.D. thesis.

1.5 Contributions and References from the Literature

For the sake of clarity and readability, references contributing to this Ph.D. thesis are labelled using the following criteria: [<conference/journal> <Year(yy)[.autonum]>], e.g., [ECOC20] or [JSAC21]; in case of more than one contribution with the same label, a sequence number is added.

The rest of the references to papers or books, both auto references not included in this Ph.D. thesis and other references from literature are labelled with the initials of the first author's surname together with its publication year, e.g., [Ve17].

Chapter 2

Background

In this chapter, we introduce the needed background on AI and QKD system. Figure 2-1 shows a schematic view of QKD systems. First QKD scheme developed by Charles Bennett and Gilles Brassard in 1984 (BB84). Alice generates both qubits based on randomly generated bits, as well as bases on her side, and sends them through the quantum channel to Bob. Then, Bob measures the received qubits based on its randomly generated bases on his side, and extracts the bits. Then in the public channel, Alice and Bob exchange their bases, then both obtain the sifted key. Next, Alice sends a split part of the sifted key to Bob, to inform Bob about the qBER. Then, both start error correction procedure to have the remained key corrected. Apart from the corrected key, Alice will obtain the leaked information from the error correction procedure, and based on that, in privacy amplification, she discards part of the key to ensure more security. Finally, Alice and Bob have the final key.

The quantum channel can be either free space or fiber. If the fiber is aerial, it can be subject to different environmental events such as wind, thunderstorm, or high temperature of the sun, and it can degrade the quantum channel in terms of qBER and KER at the end.

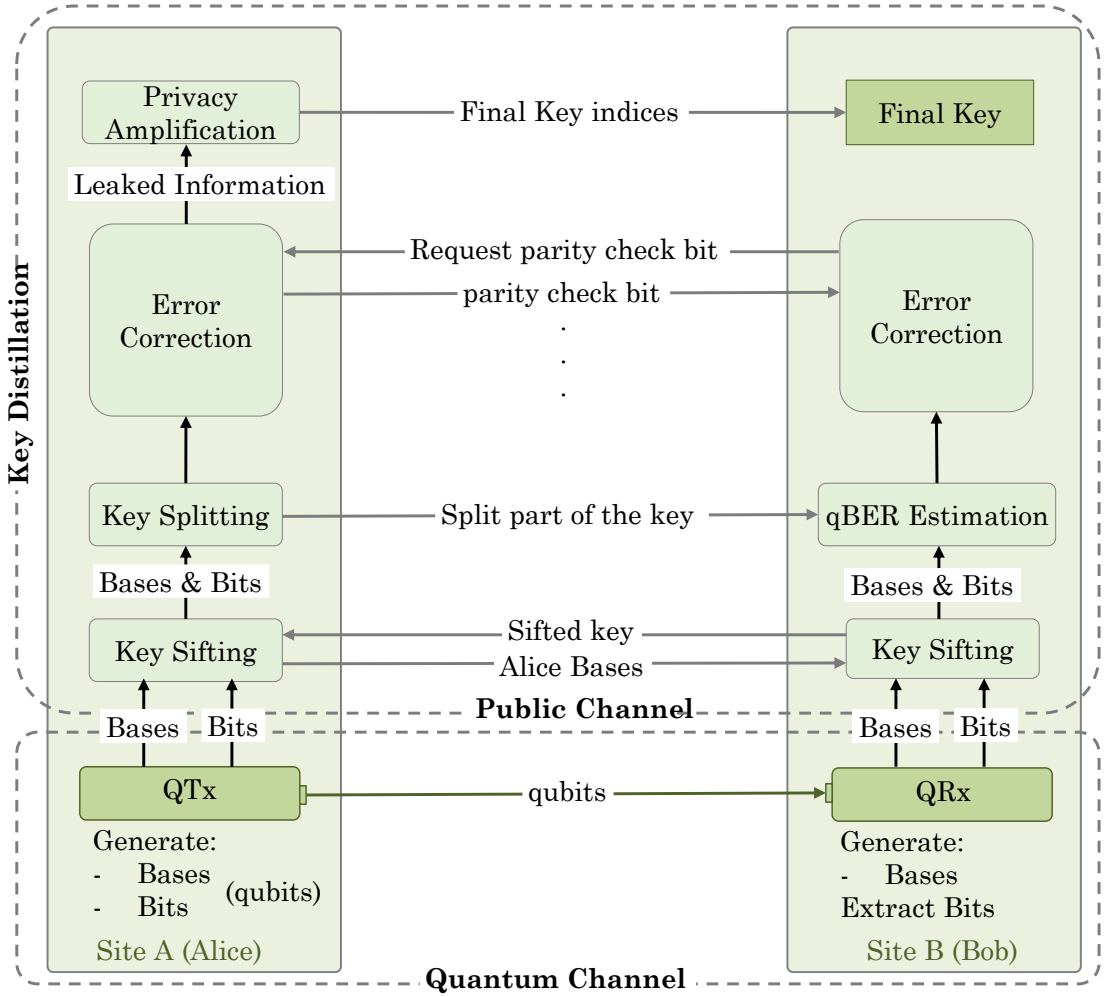
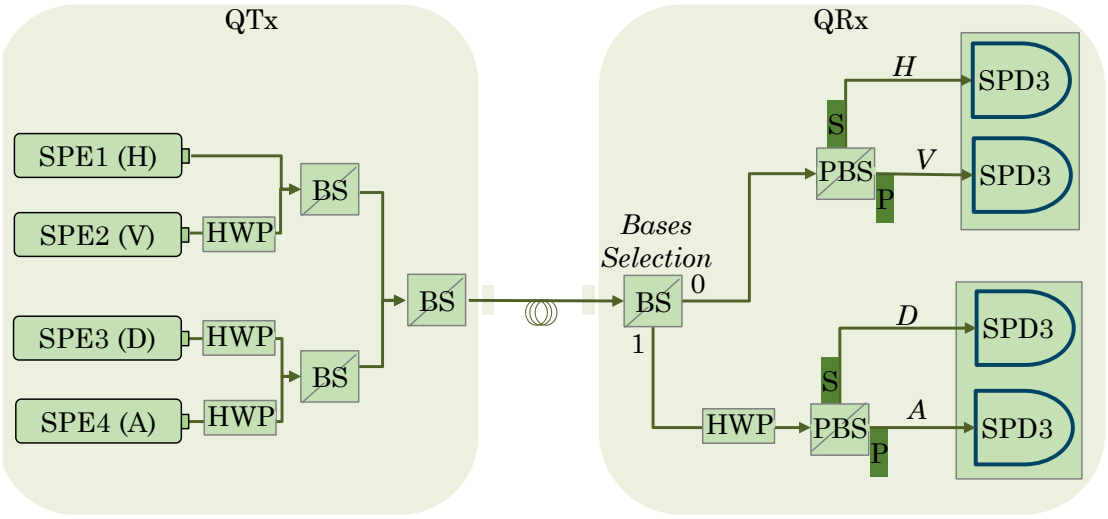


Figure 2-1- QKD System

2.1 Discrete Variable QKD system architecture

In DV-QKD system QTx encodes qubits on the SOP of single photons. The tiniest particle of light can carry quantum information to be used in DV-QKD systems. Different dimension of the single photon can be used to encode bits on qubits such as SOP, phase or time, but we focus on the simplest one which is the polarization encoded QKD system.

Figure 2-2 illustrates how the physical layer of DV-QKD works. QTx chooses one of four Single Photon Emitters (SPE) based on the generated random bit and basis. The emitted photon reaches and passes the fiber (channel). In QRx, the photon randomly chooses either transmission (1) or reflection (0) of the Beam Splitter (BS) to represent Bob basis selection. If the photon is transmitted, it is counted in (Single Photon Detector) SPD1 or SPD2 bases on its polarization to be aligned to Horizontal (H) and Vertical (V) SOPs.



Alice Basis	Alice Bit	SPE Emission
0	0	1
0	1	2
1	0	3
1	1	4

Figure 2-2- DV-QKD System Architecture

Polarizing Beam Splitter (PBS) represents Bob bit selection in QRx. On the other hand, if the photon is reflected, it passes a Half Wave Plate (HWP) to be aligned to Diagonal (D) and Anti-diagonal (A) SOPs and Then, it is counted in SPD3 of SPD4. In this way, Alice and Bob can exchange encoded bits. If the channel is not affected by the eavesdropper or channel noises, half of the photons generated and encoded by QTx can be correctly decoded in QRx i.e the SOP of the photons are correctly revealed by QRx as QTx has sent.

From quantum information theory point of view, HWP in QRx change the measurement axis for receiving photons, and BS choose the measurement axis between z and x axis for the photons. The measurement result in z and x axes would be H or V and D or A, respectively. For instance, if QTx encodes the photon in D SOP and sends it to QRx, it will be correctly measured if it is reflected and passed through HWP, so it will be counted in SPD3 which means D SOP.

At the end, key distillation engines realize which photons are correctly measured and the final key is extracted from those photons with match basis chosen in QTx and QRx. Next, we present the technology that helps DV-QKD system to take actions against polarization changes in the quantum channel.

2.1.1 SOP estimation in DV-QKD systems

DV-QKD as a quantum system also, can take advantage of the quantum features estimation in quantum systems and estimate the differential phase (distortion) induced by optical infrastructures. As DV-QKD system is using SOP of single photons (qubits) to generate secure keys, the corresponding Hilbert space of the quantum information system has only one dimension which is zero or one along S_1 axis represented on the Bloch (Poincaré) sphere in Figure 2-3.

The point is that under different environmental circumstances or state initialization in the QKD system, this quantum state can be in superposition of the zero and one states. So, assuming the Bloch (Poincaré) sphere representing all possible quantum states of the qubit, infinite number of states might be assigned to the qubits. In conclusion, quantum state (SOP) estimation of the qubits (photons) is of upmost importance for the DV-QKD system.

As we have three axes (S_1(Z), S_2(X), S_3(Y)) to specify the SOP (quantum state) of a photon (qubit), three different measurement are needed to estimate the state in the sphere. In this procedure, QTx sends photons with predefined SOP (H) to the QRx through the quantum channel. Due to environmental events, the SOP will be changed, and the quantum state will be in a superposition of the H and V SOPs.

In the first step, S_1 value of the SOP in the superposition is measured. As depicted in Figure 2-3, a bucket of H polarized photons is sent by QTx to QRx. Then, QRx measures these photons along S_1(Z) axis of the Poincaré (Bloch) sphere. From QKD system architecture prospective, QRx counts the photons that hit SPD2 transmitted by BS (basis 0). If the photons are not distorted by the channel, all photons will hit SPD1. The portion of sent photons that hit SPD2 reveals S_1 value of the SOP that needs to be estimated.

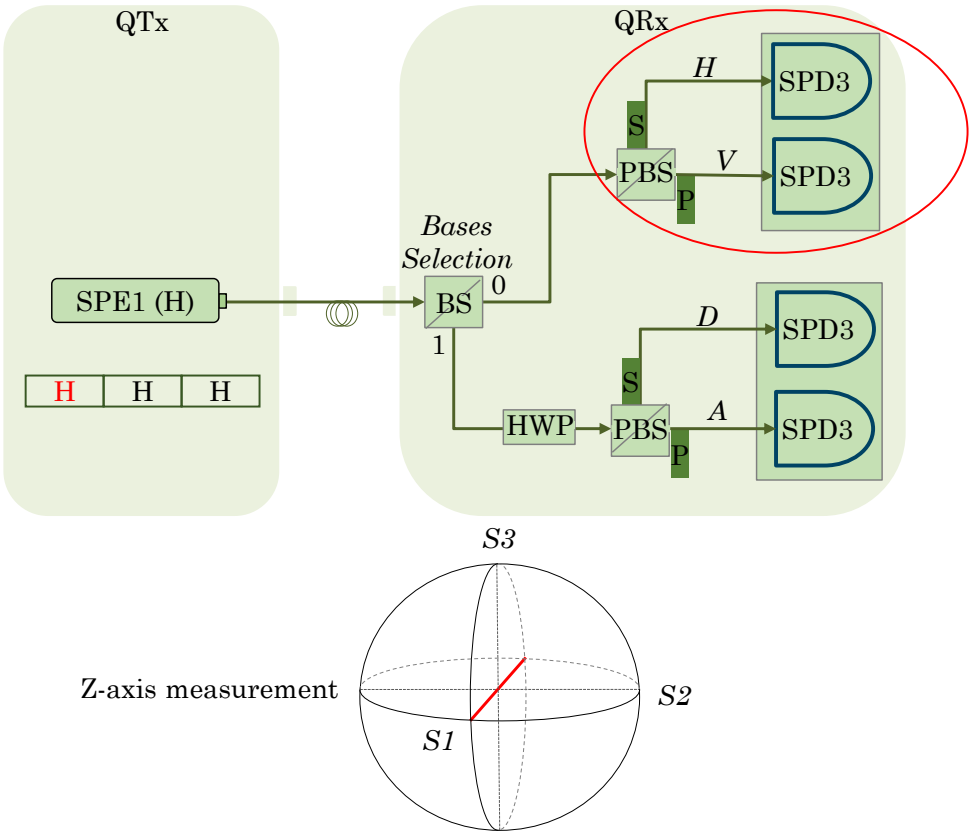


Figure 2-3- S_1 axis measurement in DV-QKD System

In the second step, S_2 value of the SOP in the superposition is measured. As depicted in Figure 2-4, another bucket of H polarized photons is sent by QTx to QRx. Then, QRx measures these photons along S_2(X) axis of the Poincaré (Bloch) sphere. From QKD system architecture prospective, QRx counts the photons that hit SPD4 reflected by BS (basis 1). A HWP is used to rotate the SOP and make the photons ready for S_2(X) axis measurement. If the photons are not distorted by the channel, half of the photons will hit SPD3 and the other half hit SPD4. This proportion reveals S_2 value of the SOP that needs to be estimated.

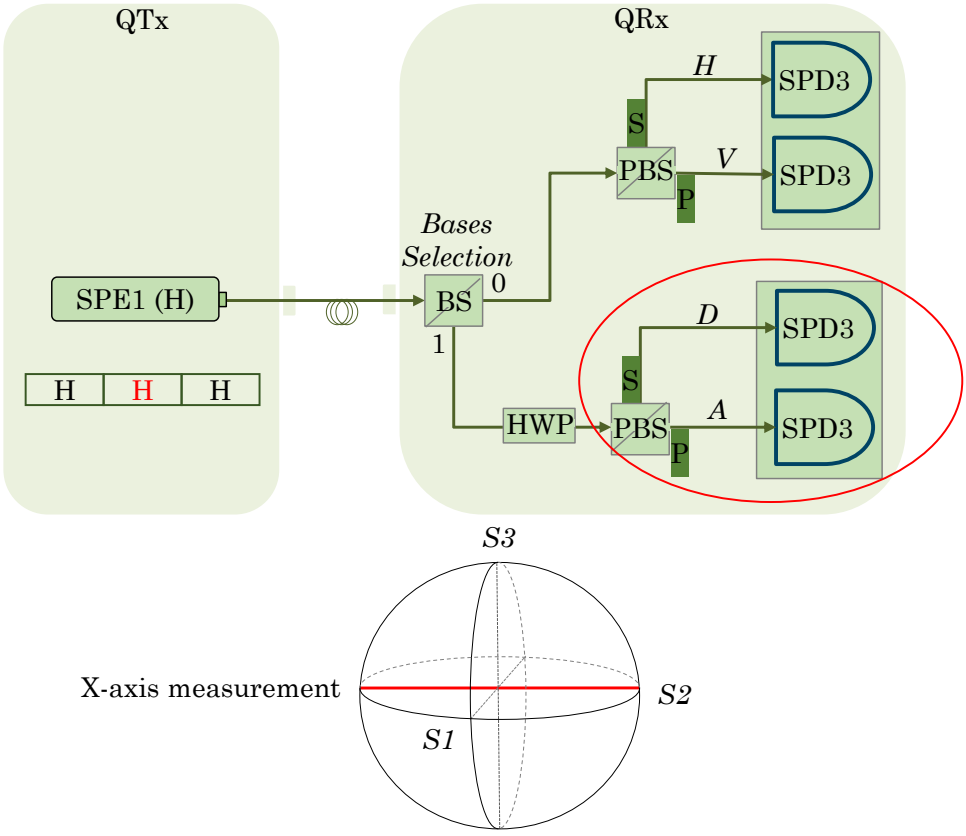


Figure 2-4- S_2 axis measurement in DV-QKD System

Finally, S_3 value of the SOP in the superposition is measured. As depicted in Figure 2-5, third bucket of H polarized photons is sent by QTx to QRx. Then, QRx measures these photons along S_3(Y) axis of the Poincaré (Bloch) sphere. From QKD system architecture prospective, QRx counts the photons that hit SPD2 and SPD4 both transmitted and reflected by BS (basis 0 and 1). In this step, two Quarter Wave Plates (QWP) are also installed before final measurements in both 0 and 1 bases to make S_3(Y) axis measurement possible with additional SOP rotations. For this measurement, H photons should be equally distributed among all SPDs to show no distortion in the estimated SOP.

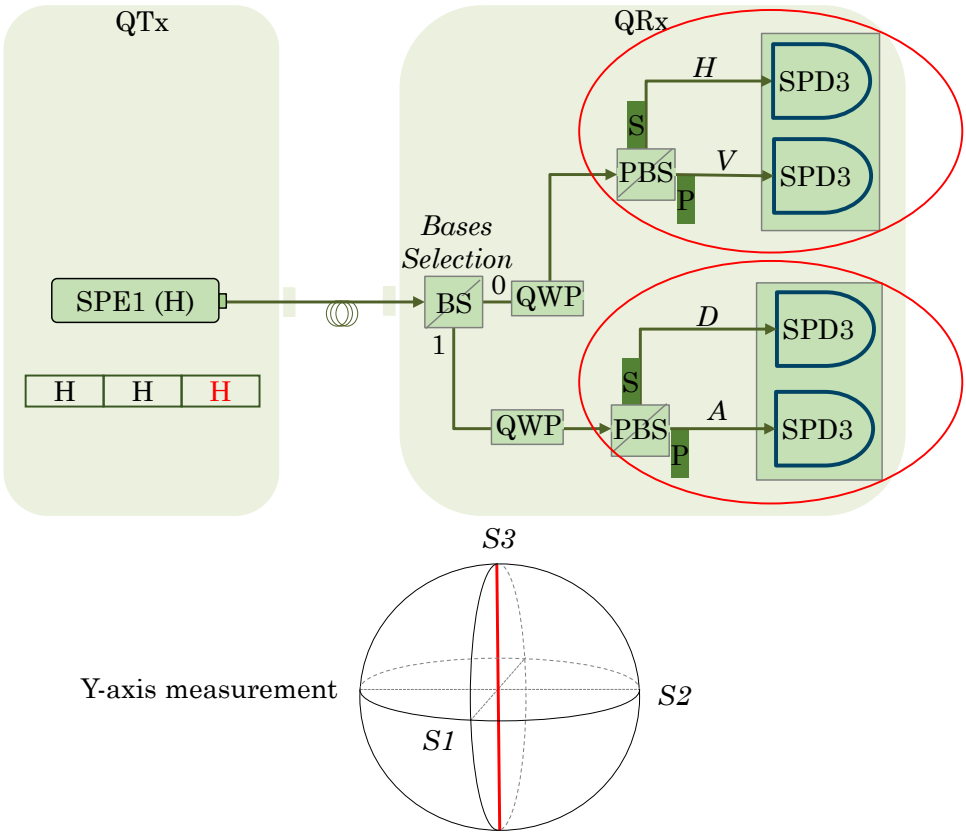


Figure 2-5- S_3 axis measurement in DV-QKD System

Having these three different measurements, three stokes of the SOP are estimated and the distortion in the quantum channel (fiber) between QTx and QRx are recognized. This recognition helps DV-QKD with SOP distortion compensation through a method called feedback-based polarization drift compensation.

In the next section, we present needed information about Machine Learning (ML) and optimization algorithms.

2.2 ML and optimization Techniques

Development of models receiving input data besides utilizing statistical analysis to forecast an output value within a suitable range is the key objective of ML. The ML is one of the rapidly growing areas with comprehensive applications in the domain of computer science, telecommunication and many other areas. The supervised, unsupervised and Reinforcement Learning are among the classifications of ML algorithms. The well-known procedures used in the ML algorithms are none other than the supervised algorithms.

Furthermore, regression and classification are the further sub-divisions of supervised algorithms. A number of ML algorithms are used in literature. The Logistic Regression, Decision Tree, Naive Bayes, support vector machines (SVM), K-Means, k-nearest neighbors (KNN) and Random Forest are among the commonly used ML algorithms. [Sa20]

2.2.1 Deep Learning Techniques

A new branch of ML, i.e., the deep learning has currently gained widespread recognition and the same has been used for intrusion detection. Moreover, traditional methods are outperformed by the deep learning as per the findings of the studies. The technique is found to be more efficient in terms of its performance. Nonetheless, the feature reduction ability of the deep learning is emphasized by this category of references. It implements classification through the traditional supervision model and deep learning methods are primarily used for pre-training. [Sa20]

Learning process is achieved by training neurons in multiple neural network layers and with more neurons than classical ML techniques more non-linearity can be investigated and learned. In this way DNN models are able to predict these complex nonlinearities for different applications. We have used these models to be able to predict future distortion of coming photons through the fiber. Having used DNN models, less compensational actions are need to be applied by optical devises and consequently we can benefit from DNN models to improve our QKD systems.

2.2.2 Exhaustive Greedy Algorithm

The Exhaustive Greedy (EG) algorithm is proposed to reduce the search space of the (Enumerate Subgraphs) ESU algorithm but still maintain the good join orders by combining the Exhaustive Search with Greedy algorithm [Tr09]. Introducing a threshold to the algorithm, we do not need to apply all values in the search space to the correction algorithm. We can use optimized values to minimize the applied corrections.

2.3 Digital Twin for different applications

Figure 2-6 illustrates how DT can bridge the gap between the virtual and physical realms by leveraging its fundamental tenets and practical applications. In the physical space, where errors and losses are commonplace, data acquisition is facilitated through monitoring procedures defined between physical systems and DT, enabling the collection of relevant information that is then stored in a database. By data analysis techniques, the information is transformed into useful insights and in-

depth knowledge. Using this information and data, virtual models can be created dynamically in the DT, tailored to meet specific application requirements. These virtual models generate the tuned parameters and provide appropriate feedback to the physical domain, enabling the implementation of optimization strategies [Wa21].

The interaction between the physical and virtual worlds is facilitated through forward measurements to DT models and backward tuning to physical systems, resulting in an excellent experience. Thanks to the principles of DT, a plethora of successful applications have been showcased in diverse fields including smart cities, telecommunication, ship marine, and civil engineering [Wa21].

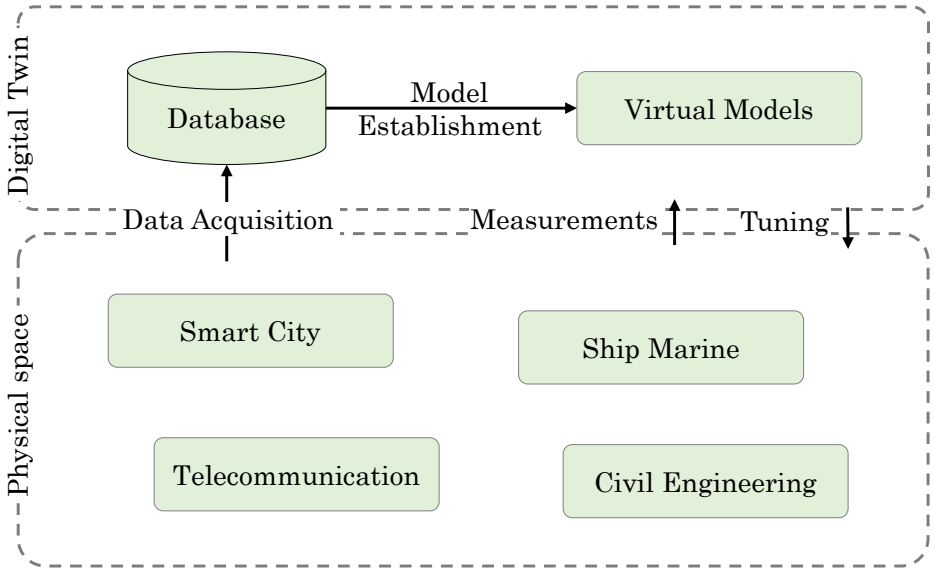


Figure 2-6- Basic principle of DT

2.4 Conclusion

This Ph.D. thesis focuses on the improvement of the DV-QKD protocol among all quantum communication protocols. The rationale behind this choice is the protocol's suitability for enhancing the security of SOP-based quantum communication. The first chapter covers the essential background information required to comprehend the work presented in this thesis. In subsequent chapters, the three goals introduced in chapter 1 will be examined in detail.

Chapter 3

State-of-the-Art

In this chapter, we present a review of the state-of-the-art of the DV-QKD subject to polarization drift in aerial optical cables. In addition, the objective of ensuring that AI-aided quantum measurement adjustment in DV-QKD have not yet been covered in the literature.

3.1 Distortion Compensation in Quantum Key Distribution w/o AI

Several works in the literature have focused on polarization drift mitigation or monitoring in discrete-variable QKD.

Authors in [Ra20] are using qBER estimation procedure to have approximate SOP of received photons in Polarization-based QKD. They have considered a threshold for violating SOP change limit as a result of birefringence, and if this violation is happened, they will perform reversal operation to compensate the polarization random drift. The qBER estimation and reversal operation is performed in monitoring mode not using the qubit for key generations and generating the keys in transmission mode.

Authors in [Ag20] have used 1 million qubits for qBER estimation every second. After finding the qBER, they have used a hardware called actuator for stabilizing the Poincaré Sphere. They are performing this stabilization in four steps. At each step they are rotating the sphere proportional to the estimated qBER in a round, and if after one rotation, the qBER decreases they continue the rotation in the same direction, and if not, they reverse the rotation and start new round for performing rotations in a new direction in the next step. They continue doing this till the qBER is under a required threshold.

Authors in [Di17] have obtained polarization information in quantum channel of polarization-basis QKD from key distillation procedure. They have obtained this information by sending just horizontally polarized photons from transmitter side and using qBER of that portion of photons in the key distillation process. By doing this they have claimed that they are not interrupting the key generation process which is tricky. Because at the end they will discard that portion of photons which have been used for qBER estimation. With the qBER information they are able to find disturbances in SOP of polarized photons and quantum channel in general.

Authors in [Ma21] and [Y19] have used intensity modulator (additional hardware) for quantum signals to compensate the polarization drift in quantum channel. In this self-alignment method, QTx have sent phase modulated or polarization modulated (in another term) photons to QRx, and the receiver is able to detect the polarization misalignment resulted from channel disturbances without any feedback signal control. But, as we can imagine they are using additional photons for modulating just one quantum state, and this is clearly an additional overhead introduced by this method.

Authors in [Li18] are using Wavelength Division Multiplexer (WDM) to send qubits and polarization feedbacks in a single optical fiber simultaneously. The polarization feedback obtains the polarization mode dispersion (PMD) in the fiber and prepare reversal polarization drift to calibrate imperfections in polarized photon. All the procedure is performed in the transmitter side.

Authors in [Ko02] have used Time Division Multiplexer (TDM) instead of WDM to stabilize the polarization drift in quantum channel. They are decreasing the key rate by a factor of three, as they consider three time slots for signal transmission. The first two signals are for controlling the polarization perturbation, and the third one is the quantum signal which is attenuated.

Authors in [Wa19] have used Kalman filter which is a method to track the speed of a vehicle when we have starting and ending speed in a period of time, to estimate the polarization misalignment between QTx and QRx in quantum channel. Then they are using two-step phase compensation to recover the quantum signal.

Authors in [Ne21] took advantage of entangled photons to detect polarization dispersion of transmitting photons passing through the fiber. The temporal correlation of entangled photons is improved by making use of nonlocal dispersion compensation. This method needs two entangled photons to be emitted for a single photon preparation in BB84 protocol. One of the entangled photons stays with the transmitter for the dispersion compensation. Additional cost of auxiliary photon emission is considered for BB84 installation.

Authors in [Re21] are using supervised ML classifiers to classify different QKD protocols based on their performance in different conditions. The feature space contains those different conditions, such as efficiency of SPDs, number of pulses, transmission distance, and dark count rate. Supervised ML methods like random

forest have been hired to choose the best QKD protocol tailored with each specific condition.

Authors in [Co22] are using ML techniques to help the polarization controller in the receiver to compensate for the polarization random drift induced by the fiber. In this method additional waveplates is added to the polarization controller to have more controller over the phase retardation of the quantum signal. A cost function based upon qBER due to SOP distortion is defined to maximize KER in the polarization encoded QKD system.

Authors in [Qi20] have derived from ML to stabilize the QKD system which is phase encoded. They have considered two periods of time: 1- learning 2- prediction. In learning period, no keys are being generated. In this phase they are using quantum channel and an auxiliary classical channel to label the output of quantum measurement in QRx by sent chosen quantum state in QTx through auxiliary channel. Next, they train their supervised ML model with created dataset. In the prediction phase, QRx measures quantum states as input for the trained model, then predicted reference quantum state have been considered as the main measured quantum state. In this way, authors are calibrating imperfect quantum state measurements and generate keys in prediction time period.

Authors in [Di19] are using Long Short-Term Memory (LSTM) models to first extract useful features from existing data i.e., the operating temperature, the humidity, the intensity of a laser, and the voltages, then designate the voltage of the next moment as labels. With this LSTM model, they are able to predict the next voltage to bypass the traditional 'scanning and transmitting' problem for phase-coding QKD systems.

Authors in [Ch21] are compensating phase noise in quantum communication of the QKD protocol by hiring ML methods. This phase tracking ML algorithm compares previously learned phase retardation and received signals and predict probable phase shift in the quantum channel. After calculating the error, they will update the parameters in the quantum channel to compensate the phase noises.

To the best of our knowledge, precise SOP estimation and utilizing ML techniques to compensate for SOP distortion in the polarization encoded QKD systems has not been investigated in the literature. In this thesis, we propose this technique to proactively address the low KER due to fiber stressing events.

3.2 Experimental Demonstration of Quantum Key Distribution

Authors in [Ch17] have performed an experimental analysis to evaluate the influence of polarization variations on polarization-sensitive QKD systems in both buried and aerial optical fibers. They have estimated two parameter - polarization drift time and required tracking speed - to characterize polarization disturbances.

Authors in [Li19] have conducted a research about the impact of different environmental events on aerial quantum communications. They have considered Polarization-based QKD as a reference, and have experienced real environmental impacts (wind, sun, etc.) on this QKD protocol. They realized that different environmental events have different impact on qBER when we have PBS with H/V photon detectors.

Authors in [Du22] have installed a silicon-based chip before photons' measurement to compensate for the random polarization drift. The method contains feedback-based control of the quantum signal to first estimate the distortion of the polarized photons and then apply compensations in a reactive approach. Additional hardware is needed for such polarization compensation method which results in additional costs in the BB84 protocol implementation.

Authors in [Xa09] have used WDM to have two classical side channels along with the quantum channel in the same optical fiber. In this way, they can send quantum signals without interruptions to the receiver and derive from polarization disturbances information obtained from classical channels to compensate polarization drifts in the quantum channel.

3.3 Digital Twin for Quantum communication

Authors in [Ma20] offers a review of some technologies, solutions and applications scenarios where quantum optical communications are expected to disrupt telecommunications. Among the key technologies enabling quantum optical networks, the paper briefly addresses: quantum optical switching and computing, THz-to-optical conversions and advanced metamaterials for smart radio-optical programmable environments and AI. The paper concludes with an example of a future application scenario, called quantum optical twin, where the above quantum optical communications technologies are exploited to provide services such as: ultra-massive scale communications for connected spaces and ambient intelligence, holographic telepresence, tactile Internet, new paradigms of brain computer interactions, innovative forms of communications, etc.)

Authors in [Am22] presents the status quo of research and practice on quantum DT. It also discusses their potential to create competitive advantage through real-time simulation of highly complex, interconnected entities that helps companies better address changes in their environment and differentiate their products and services.

On the other hand, authors in [Lv22] proposed an idea to use quantum communication to make DT more secure and efficient. They are using QKD to efficiently generate keys which can encrypt transmitting data between different models of DT in different locations as well as between DT models and physical

equipment. This approach is the opposite of our approach which is using DT to improve QKD systems.

3.4 Conclusions

In this chapter, we have reviewed the state-of-the-art of relevant works related to the goals of this thesis. Table 3-1 summarizes the study.

Table 3-1: State-of-the-art summary

Goals	References
G1 –Distortion Compensation in Quantum Key Distribution w/o AI	[Ra20], [Ag20], [Ch17], [Ma21], [Y19], [Li18], [Ko02], [Wa19], [Ne21], [Qi20], [Di19], [Ch21], [Re21], [Co22]
G2 –Experimental Demonstration of Quantum Key Distribution	[Di17], [Li19], [Du22], [Xa09]
G3 – DT for Quantum Communication	[Ma20], [Am22], [Lv22]

We can conclude that, although some previous works have worked on compensating polarization drift in QKD, proactive and intelligent approaches for the mitigation process are really needed.

Chapter 4

AI for Discrete Variable Quantum Key Distribution

In the previous chapters, we have reviewed the state-of-the-art and the background concepts needed to fully understand this work. In this chapter, we focus on how AI can improve polarization encoded quantum key distribution.

Secure communications have become a requirement for virtually all kind of applications. Currently, two distant parties can generate shared random secret keys by using public key cryptography. However, quantum computing represents one of the greatest threats for the finite complexity of the mathematics behind public key cryptography. In contrast, QKD relies on properties of quantum mechanics, which enables eavesdropping detection and guarantees the security of the key. Among QKD systems, polarization encoded QKD has been successfully tested in laboratory experiments and recently demonstrated in closed environments. The main drawback of QKD is its high cost, which comes, among others, from: i) the requirements for the QTx and QRx; and ii) the need of carefully selecting the fibers supporting the quantum channel to minimize the environmental effects that could dramatically change the SOP of photons. In this chapter, we propose a ML (ML) -based polarization tracking and compensation that is able to keep shared secret key exchange to high rates even under large fiber stressing events. Exhaustive results using both synthetic and experimental data show remarkable performance, which can simplify the design of both QTx and QRx, as well as enable the use of aerial optical cables, thus reducing total QKD system cost.

4.1 Introduction

As mentioned before, in polarization encoded QKD systems, QTx sends polarized photons to QRx, which decodes them and generates a raw key of a defined length. The raw key is then distilled, using a parallel public channel established between transmitter and receiver, to correct possible detection errors due to optical transmission and generate a shared secret key. E.g., the authors in [Kh20] showed a polarization-based QKD system using the BB84 protocol [Be20], [Sh00] that reaches shared secret KER > 1 Mb/s for distances >100 km.

Currently, research efforts are also focused on demonstrating such performance in real (more challenging) scenarios [Me20], including aerial cables, where QKD transmission might be severely affected by weather conditions (e.g., high wind) that stresses optical fibers [Li19]. Such mechanical stress changes fiber birefringence, which introduces fluctuations on the SOP of the transmitted qubits and, as a result, qBER increases. Note that qBER is causally related to the effective KER, which reduces when qBER increases, e.g., from Mb/s to Kb/s or even b/s as shown in [Fr17]. Since optical eavesdropping generates high qBER, a post processing phase named key distillation enables its detection. However, excessive qBER coming from SOP fluctuations might derive into false eavesdropping detection (threshold is typically set within the range 5%-10%); in such case, safety mechanisms against attacks are activated, thus interrupting (i.e., KER becomes temporarily 0), or even blocking that quantum channel for key exchange.

Consequently, QKD devices must include mechanisms to soften such negative effects while guaranteeing robustness and efficiency to be deployed in real scenarios. In particular, SOP compensation mechanisms need to be implemented at the QRx to correct perturbations induced by environmental causes, thus increasing KER without reducing the security level. Precisely for that, authors in [Ra20] proposed a procedure to estimate the SOP of received photons in polarization based QKD systems. They performed a reactive reversal operation to compensate measured polarization random drift, which resulted in qBER reduction. Authors in [Ag20] used 106 qubits/s for qBER estimation. After finding the qBER, they proposed a polarization compensator implemented in hardware for stabilizing the SOP. They performed such stabilization in four steps, where they rotate the sphere proportionally to the estimated qBER; if qBER decreases the rotation continues in the same direction, and otherwise they reverse the rotation and start a new round. Authors in [Di17] obtained information about polarization by sending horizontally polarized photons and using qBER of that portion of photons in the key distillation process aiming at not interrupting the key generation process, although that portion of photons need to be discarded.

Authors in [Ch17] performed an experimental analysis to evaluate the influence of polarization variations on polarization sensitive QKD systems in both buried and aerial optical fibers. They estimated two parameters, i.e., polarization drift time and

required tracking speed, to characterize polarization disturbances. Specifically for aerial quantum communications, authors in [Li19] studied the impact of different environmental events. They considered real environmental impacts (like wind, sun, etc.) and realized that different environmental events have different impact on qBER. In fact, as shown in [Ru20], SOP fluctuations caused by environmental events can be accurately predicted by means of ML [Ra18].

In this work, we propose a lightweight ML-based SOP tracking and polarization compensation that uses DNN models for polarization encoded QKD systems. Such models accurately anticipate SOP fluctuations, so adaptive actions can be taken at the QRx to reverse them before they produce negative impact. The proposed system is specifically designed to maximize performance, i.e., to reduce false eavesdropping detection and increase effective KER, in scenarios exposed to environmental events. The proposed approach will enable cost reduction of QKD systems as: i) QTx specifications can be relaxed since SOP imperfections can be corrected by the QRx; and ii) the hardware design of the QRx can be simplified and rely on software.

The rest of the chapter is organized as follows. Section 4.2 presents the main concepts related to QKD. In addition, it describes in depth the operation cycle for SOP tracking and the proposed ML-based fast QKD. The proposed solution is based on SOP monitoring, SOP prediction, and proactive rotation plan. These key components are detailed in Section 4.3, which also includes the notation used along this chapter. The discussion is supported by the results in Section 4.4. Finally, Section 4.5 draws the main conclusion of the work.

4.2 ML-Based Fast Quantum Key Distribution

In this section, we first briefly present the main concepts and used notation. Rather than an exhaustive description of QKD systems, we first present the essential concepts regarding transmission, propagation, and photons measurement for raw keys exchange under the BB84 protocol [Sh00]. Next, we identify opportunities and propose solutions to accelerate the distribution of keys over a quantum channel in the presence of SOP fluctuations.

4.2.1 Preliminary concepts

In BB84, the QTx continuously generates raw keys containing sequences of pairs of Boolean values, each pair containing a basis (B) and bit (b). The pair $<B(t), b(t)>$ generated at time t is defined by the quantum state $|q(t)\rangle$, which can be defined as a position on the Bloch sphere [Be06]. Therefore, $|q(t)\rangle$ can be alternative expressed: i) in Euclidean coordinates $<x(t), y(t), z(t)>$, with one component for axis X, Y, and Z, respectively; or ii) in polar coordinates $<\theta(t), \varphi(t)>$, represented by azimuth and ellipticity angles, respectively.

Table 4-1: $|q(t)\rangle$ CONFIGURATION AT QTX

Linear Polarization	**Axis**	**<B, b>**		**<θ_p, φ_p> [rad]**
Horizontal (*H*)	*Z*	0	0	<0, 0>
Vertical (*V*)	*Z*	0	1	<π, 0>
Diagonal (*D*)	*X*	1	0	<π/2, 0>
Anti-Diagonal (*A*)	*X*	1	1	<3 ·π/2, 0>

containing sequences of pairs of Boolean values, each pair containing a basis (*B*) and bit (*b*). The pair <*B(t), b(t)*> generated at time t is defined by the quantum state $|q(t)\rangle$, which can be defined as a position on the Bloch sphere [Be06]. Therefore, $|q(t)\rangle$ can be alternative expressed: i) in Euclidean coordinates <*x(t), y(t), z(t)*>, with one component for axis *X*, *Y*, and *Z*, respectively; or ii) in polar coordinates <$\theta(t)$, $\varphi(t)$>, represented by azimuth and ellipticity angles, respectively.

In practice, $|q(t)\rangle$ is encoded as a single photon, which translates into a single point on the unitary Poincaré sphere; Both Bloch and Poincaré spheres are exchangeable if axes *X*, *Y*, and *Z* of the former match Stokes S_2, S_3, and S_1, respectively, in the latter. Table 4-1 specifies the four possible linear polarizations for each $|q(t)\rangle$ in terms of: i) axis; ii) coded basis and bit; and iii) position on the Poincaré sphere.

Effects related to fiber propagation and eavesdropping alter $|q(t)\rangle$. Let us denote $|p(t)\rangle = <\theta_p(t), \varphi_p(t)>$ as the real polarization of the received photon. We adopt the QRx hardware architecture proposed in [Ra20], where the QRx is equipped with an Electronic Polarization Controller (EPC) followed by a PBS. The photon first reaches the EPC, which is in charge of polarization alignment. Specifically, given a reference SOP *r(t)* (hereafter denoted as rotation) defined by the tuple <$\theta_r(t)$, $\varphi_r(t)$>, the EPC performs a reversal operation to align the photon detector with the configured SOP. Hence, it is worth noting that the rotation with configuration $\theta_r(t)=\theta_p(t)$ and $\varphi_r(t)=\varphi_p(t)$ is the one perfectly aligned with the state $|p(t)\rangle$ of received photon. Before the photon passes through the PBS, a basis is selected, which entails selecting a specific axis in the sphere to detect the photon and extract its bit [Sh00]. Two main conditions lead to erroneous bit extraction: *i*) if the sphere is perfectly aligned with $|p(t)\rangle$, the bit is wrongly decoded if QRx selects the wrong basis; and *ii*) even if QRx selected the correct basis, bit error can be produced if there is misalignment between $r(t)$ and $|p(t)\rangle$.

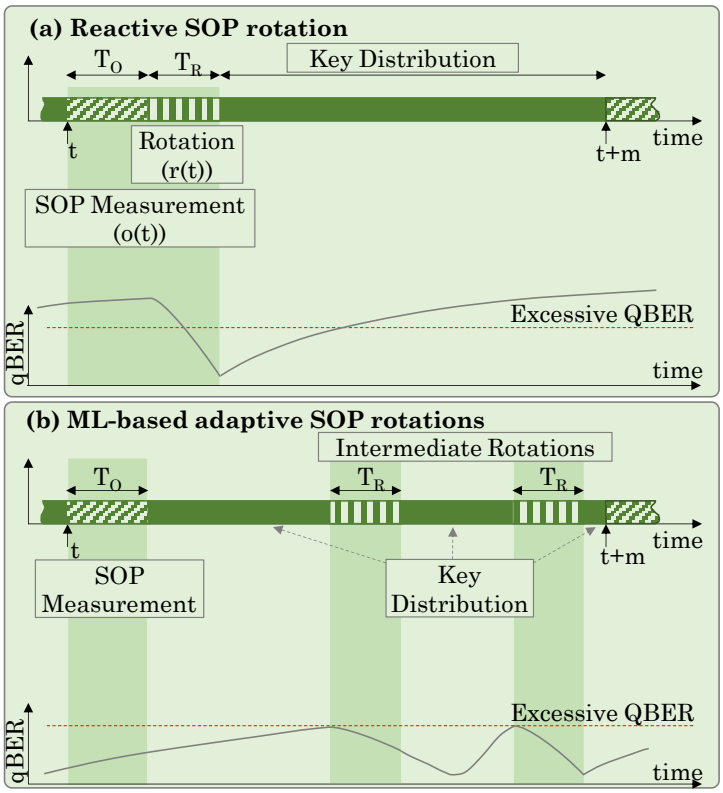


Figure 4-1- Reactive (a) and ML-based adaptive (b) SOP rotation.

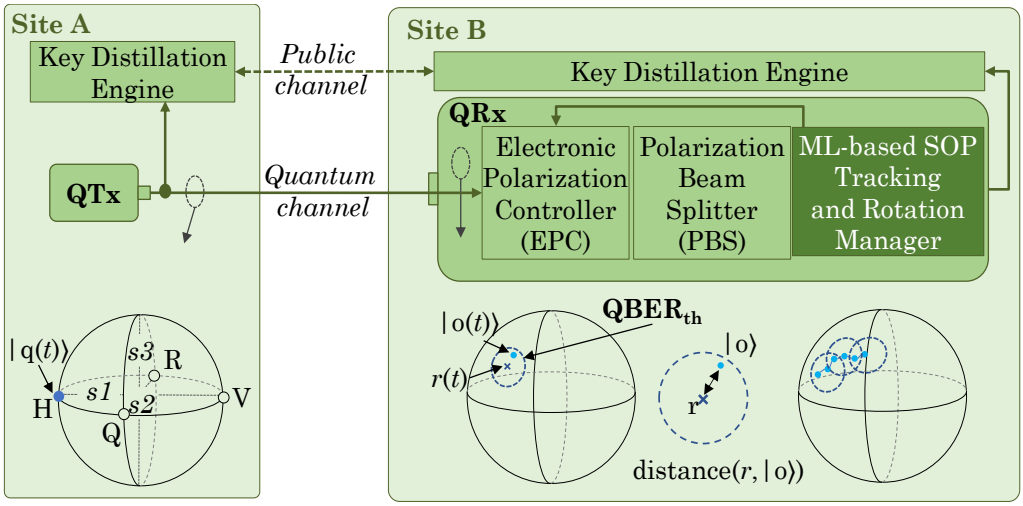


Figure 4-2- System architecture.

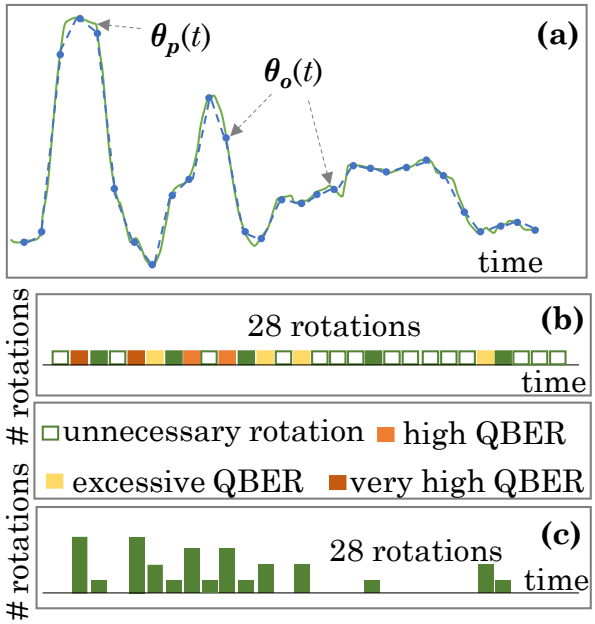


Figure 4-3- Example of operation (a) and performance of the reactive (b) and ML-based adaptive (c) SOP rotation.

Besides the quantum channel, a parallel secure public channel is used for key distillation purposes [Ma17]. QRx starts sending a subset of decoded bits and basis to QTx in order to quantify bit errors, i.e., qBER. In case that qBER exceeds a given threshold, e.g., 10%, eavesdropping in the quantum channel is assumed, which triggers a safety mechanism, such as QKD interruption. Otherwise, QKD is assumed to be secure enough. Next, bases need to be verified, since they were randomly selected at the QRx side. To that end, key sifting is performed, where QTx sends to QRx the sequence of used bases through the public channel, so that QRx can check them and discard the wrong ones. After the bases are synchronized, error cascading is conducted to correct the erroneous bits, which results into a corrected sifted key. In the end, a portion of the sifted key is selected as the final shared secret key to amplify privacy. This process results into a maximum achievable KER when qBER is low, and it will be noticeably reduced when qBER increases.

4.2.2 Opportunities and proposed solutions

For illustrative purposes, Figure 4-1a shows the operation of the quantum channel with time based on the approach proposed in [Ra20]. At regular time intervals of size m, the QTx sends a number of qubits with a predefined polarization that are used to monitor the current SOP, denoted $|o(t)\rangle$, at the QRx. Based on the measured SOP, the QRx computes the needed rotation (denoted $r(t)$) to compensate the polarization drift. Once the rotation is performed, the quantum communication system exchanges polarization-encoded keys. If the value of m is large enough compared to the time for monitoring (T_O) and rotation (T_R), this scheme introduces a small overhead, while

allows to react quickly to changes in the SOP. Figure 4-1a also includes a possible evolution of the qBER from one rotation to the next. In the presence of SOP fluctuations, it might happen that the rotation performed at the starting of a period does not allow to keep the qBER under a desired threshold (denoted $qBER_{th}$), e.g., 1%, until the next SOP is measured, and a new rotation is performed.

A possible solution to deal with scenarios with large SOP fluctuations would be to reduce m, which would result in a higher system overhead, especially during the time when fluctuations are small or negligible. For that, m can be defined dynamically, which would entail a way to synchronize QTx and QRx real-time. In view of this, we propose an approach to track SOP fluctuations and apply ML to predict the next SOPs based on such tracking. Then, rotations can be planned to be performed at any intermediate time from one SOP measurement to the next; the number of rotations would vary from none to several, so the obtained qBER is always under $qBER_{th}$ (Figure 4-1b). Because rotations can be planned to be performed at intermediate times, accurate estimation of future states is of paramount importance for the proposed system. Armed with such predictive tool, an optimization problem can be solved to decide not only when to perform the rotations, but also the value of each rotation to minimize the number of total rotations that are performed; this would result into a reduced overhead, while assuring a contained qBER. In the example of qBER evolution in Figure 4-1b, no initial rotation is needed, as qBER was initially low, whereas two rotations are performed at intermediate times. In particular, the first rotation is performed to compensate SOP at a future state, as revealed by the evolution of the qBER that progressively reduces until a minimum and increases again reaching a value close to $qBER_{th}$ before the second rotation is performed.

Figure 4-2 shows a schematic view of a quantum communication channel established between remote sites A and B. Without assuming any specific polarization based QTx implementation, let us consider that a qubit is generated by randomly selecting one linear polarization (points H, V, R, and Q on the sphere at site A in Figure 4-2). Then, the perfectly polarized photon is sent to the QRx. When the photons are received and measured at the QRx side, the SOP position might have drifted. Figure 4-2 reproduces the EPC and PBS modules in the QRx based on the architecture proposed in [Ra20]. The obtained qBER will be below $qBER_{th}$ if the state of the received photons is within an area centered in the current reference SOP with radius d_{th}. When the reference SOP of the QRx is rotated, the area of tolerable $qBER_{th}$ also moves covering a different region. In the proposed system, a ML-based module is in charge of tracking SOP and deciding the rotations to be performed, as illustrated in Figure 4-2.

An illustrative example of the operation is presented in Figure 4-3. Figure 4-3a shows the evolution polarization angle θ of the real photons state $|p(t)\rangle$ and measured state $|o(t)\rangle$, both at the QRx. In addition, linear (polynomial of degree 1) interpolation connecting two measured SOPs is represented. Note that although

linear interpolation is used for the sake of simplicity in the drawing, higher degrees can be used. In Figure 4-3b-c, the rotations that are performed under the reactive and adaptive approaches are shown. We assume here the same period m for both approaches. In the reactive approach (Figure 4-3b), one single rotation is performed once the current state $|o\rangle$ is measured after T_O, which results into 28 rotations for the sample in Figure 4-3a. However, as many as 15 of the rotations are unnecessary, because at the time they are performed, the measured SOP is within the area of low qBER. On the contrary, there are 4 periods with high and very high qBER, due to large SOP fluctuations in those periods. In contrast, the proposed ML-based SOP tracking and rotation planning approach, is able to achieve low qBER even during large SOP fluctuations (Figure 4-3c), due to its ability to predict future SOPs and plan the needed rotations. Note that the total number of rotations under the ML-based approach is equivalent (it can be even lower) to the reactive approach, which ensures high efficiency. That fact, combined to the reduced qBER, results in faster KER.

Table 4-2: Notation

$b(t)$	Bit at time t.
$B(t)$	Basis at time t.
$\|q(t)\rangle$	Quantum state at QTx at time t.
$\theta(t)$	Azimuth angle of the quantum state at time t.
$\varphi(t)$	Ellipticity angle of the quantum state at time t.
S_i	Stoke parameters (i in [1, 3]).
$\|p(t)\rangle$	Real photon state at the QRx at time t.
$\|o(t)\rangle$	Measured (estimated) state at QRx at time t.
$r(t)$	Reference SOP (rotation) at QRx at time t.
m	QKD Operational time period.
w	Previous time window for DNN prediction.
O	Sequence of k SOPs.
$qBER(t)$	quantum Bit Error Rate at time t.

Algorithm 4-I. SOP Monitoring Procedure

INPUT: $QBER(t)$
OUTPUT: $|o(t)\rangle$

1: $\theta(t) \leftarrow \cos^{-1}(1\text{-}2 \cdot qBER(t).Z)$
2: $\sin(\varphi(t)) \leftarrow (1\text{-}2 \cdot qBER(t).Y)/\sin(\theta(t))$
3: $\cos(\varphi(t)) \leftarrow (1\text{-}2 \cdot qBER(t).X)/\sin(\theta(t))$
4: $\varphi(t) \leftarrow \tan^{-1}(\sin(\varphi(t))/\cos(\varphi(t)))$
5: **return** $|o(t)\rangle = <\theta(t), \varphi(t)>$

4.3 ML-based SOP Tracking and Rotation Manager

In this section, we first present the procedure used to measure and predict the evolution of photons' SOP based on the combination of the quantum state tomography theory [To19] and DNN models. Next, the procedure to plan the sequence of Poincaré sphere rotations that needs to be carried out to achieve accurate polarization alignment based on the SOP prediction is described. Table 4-2 summarizes the notation that will be consistently used along the chapter.

4.3.1 SOP monitoring and prediction

As introduced in the previous section, SOP can be affected by perturbations on the fiber, during the monitoring period starting at time t, the QTx sends a number of photons with a known polarization and the QRx measures them in different axes to accurately estimate the current state $|o(t)\rangle$, defined by the tuple $<\theta_o(t), \varphi_o(t)>$. Specifically, the QTx generates n photons with H polarization (i.e., $<B,b> = <0,0>$), which are propagated through the quantum channel. At the QRx side, the received photons are separated in three different chunks of $n/3$ photons, one for each of the three axes X, Y, and Z measurements. The decoded bits can contain some 1's due to the combination of the selected axes for measurement, the fluctuations of the SOP during propagation, and the current rotation configuration in the EPC. Then, we define the qBER of a chunk as the sum of the extracted bits (number of erroneous bits) over the length of the chunk ($n/3$). After transmitting and decoding all n photons, measurement results are available for each axis, i.e., $qBER(t) = \{X, Y, Z\}$. Algorithm 4-I specifies the steps to estimate $|o(t)\rangle$ as a function of the computed qBERs, based on the well-known theory and equations presented in [Wo13]. The measurement along the Z axis is enough to compute $\theta(t)$ (line 1 in Algorithm 4-I), whereas $\varphi(t)$ requires from measurements along X and Y axes to estimate sine and cosine of $\varphi(t)$, respectively (lines 2-4).

ALGORITHM 4-II. SOP PREDICTION PROCEDURE

INPUT: $o(t)$, DB, f, $params=\{w, m, l, k\}$
OUTPUT: O

1: $DB \leftarrow DB \cup o(t)$
2: $X \leftarrow DB$.query("time">=t-w)
3: $|o(t+m)\rangle \leftarrow f$.predict($X$)
4: $X \leftarrow X$.append($o(t+m)$)
5: $g \leftarrow$ polynomialFitting(X, l)
6: $O \leftarrow g$.predict($t+i \cdot m/k$, $\forall\ i \in [0,k]$)
7: **return** O

Once the current SOP $|o(t)\rangle$ is estimated, it is used to predict the SOP evolution until the next monitoring period. Algorithm 4-II presents the pseudocode; it receives as inputs: i) the currently estimated state $|o(t)\rangle$; ii) the set of past SOP estimations *DB*; iii) the DNN model f used for SOP prediction; and iv) a set of configuration parameters. The objective is to generate sequence O containing the current estimated state $|o(t)\rangle$ and the prediction of the next k consecutive and evenly distributed SOPs connecting $|o(t)\rangle$ and the expected one for the next monitoring period, i.e., $|o(t+m)\rangle$. O can be formally defined as:

$$O(t,m,k) = \left[|o\left(t + i \cdot \frac{m}{k}\right)\rangle, \forall i \in [0..k]\right] \quad (1)$$

Sequence O is determined by using DNN-based forecasting and polynomial fitting sequentially. The DNN is used to accurately forecast a discrete time-dependent event ahead in time, whereas polynomial is used to interpolate unknown SOPs between known states. The procedure is as follows; the last estimated SOP is stored in the SOP database and the last estimated SOPs within the previous time window w is retrieved (lines 1-2 in Algorithm 4-III) that are used to feed a DNN model that predicts $|o(t+m)\rangle$ (line 3). The DNN has $2 \cdot \lfloor w/m \rfloor$ inputs (for angles θ and φ of those last SOP values), several hidden layers using the tanh activation function, and two outputs for angles θ and φ of predicted state $|o(t+m)\rangle$. Next, the last w estimated SOPs together with the predicted $|o(t+m)\rangle$ are used to interpolate a polynomial-based model g (lines 4-5). To increase the accuracy of the interpolation procedure, g is a compound model with four l-degree polynomials used to estimate $\sin(\theta)$, $\cos(\theta)$, $\sin(\varphi)$, and $\cos(\varphi)$ as a function of time in the range $[t, t+m]$. Finally, g is used to obtain k predictions between $|o(t)\rangle$ and $|o(t+m)\rangle$ (line 6).

4.3.2 Rotation plan computation based on SOP prediction

After the SOP prediction phase, the problem of finding which rotations need to be applied within the time interval $[t, t+m]$ is solved. This problem can be modeled as an optimization problem and stated as follows:

Given:

- The sequence O of predicted states, each for a relative time $i \in [0, m]$ and defined as $O(i) = <\theta_o(i), \varphi_o(i)>$.
- The set of candidate rotations R, where every rotation r is defined by $<\theta_r, \varphi_r>$. R includes the rotation r_0 currently configured in the EPC.
- A circular area of radius d_{max} [rad] defined for a target qBER and thus, determining the need of rotations. A candidate rotation $r \in R$ that becomes active at relative time j is valid for state predictions $|o\rangle \in O \ / \ i \geq j$ if and only if distance$(r, |o\rangle) \leq d_{max}$.

Output: The rotations plan $P = [<r, i>]$, where every element defines the relative time $i \in [0, m]$ when candidate rotation $r \in R$ needs to be configured in the EPC.

Objective: minimize the number of rotations to be performed.

To reduce the complexity of the rotation plan problem, we consider that set R includes the current rotation r_0 and all predicted SOPs in O. Therefore, a trivial feasible solution would consist in performing k rotations, one for each predicted state. To efficiently solve the rotation plan optimization problem, we designed the fast deterministic greedy algorithm specified in Algorithm 4-III. After the needed initializations (line 1 in Algorithm 4-III), a pre-computation phase is run to find the subset of predicted SOP that can be served from each candidate rotation (lines 2-5). Then, an iterative procedure is executed to build the plan (sequence) of rotations until all SOPs are assigned to, at least, one of the selected rotations (lines 6-16). At every iteration, the greedy cost of every rotation is computed (lines 7-11). Such cost is defined as a weighted sum of three components, with weights $\beta_1 >> \beta_2 >> 1$. The three components account: i) whether the rotation covers reference SOP $|o_{ref}\rangle$, which is initialized with the measured SOP and updated with the last state covered by the rotation when a new rotation is performed. This component tries to foster selecting new rotations that overlap with the previous one, which forces building the plan as a sequence that tracks the evolution of O; ii) whether the rotation is the currently active one or not, so as to reduce the number of rotations; and iii) the number of SOPs covered by the candidate rotation. The candidate rotation with the highest greedy cost is selected and added to the incumbent solution (lines 12-13). Then, the relative time to perform the next rotation is computed and the set of covered SOPs O_{in} and reference state $|o_{ref}\rangle$ are updated (lines 14-16). Finally, the rotation plan is returned (line 17).

4.4 Results

In this section, we first present the simulation environment used to evaluate the proposed ML-based fast QKD system and find the value of d_{th} that results into the considered $qBER_{th}$. Next, we focus on the performance of SOP estimation, prediction, and SOP interpolation. Then, the ML-based adaptive operation is evaluated, and finally, a study of robustness against eavesdropping is presented.

4.4.1 Simulation environment and parameters tuning

The quantum systems presented in the previous sections have been implemented in Python3, using IBM's Qiskit development tools [No20]; this includes the implementation of all the modules and components in QTx and QRx, as well as qubits propagation through the quantum channel. In addition, the full stack of BB84 key distillation steps [Sh00], i.e., key sifting, qBER estimation, error correction cascade, and privacy amplification, have been implemented to emulate the real operation on the public channel.

Algorithm 4-III. Heuristic for the Rotation Plan Problem

INPUT: O, R, d_{max}
OUTPUT: P

$P \leftarrow \{\}$; $i \leftarrow 0$; $O_{in} \leftarrow \{\}$; $|o_{ref}\rangle \leftarrow O[0]$
for $r \in R$ **do**
  for $|o\rangle \in O$ **do**
    if $distance(r, |o\rangle) > d_{max}$ **then continue**
    r.O.append($|o\rangle$)
while $O_{in} <> O$ **do**
  for each $r \in R$ **do**
    if $|o_{ref}\rangle \in r$.O **then** $x_1 \leftarrow 1$ **else** $x_1 \leftarrow 0$
    if $r=r_0$ **then** $x_2 \leftarrow 1$ **else** $x_2 \leftarrow 0$
    $x_3 \leftarrow |r.O|$
    r.cost $\leftarrow \beta_1 \cdot x_1 + \beta_2 \cdot x_2 + x_3$
  $r' \leftarrow$ argmax(r.cost $\forall r \in R$)
  $P \leftarrow P \cup <r', i>$
  $O_{in} \leftarrow O_{in} \cup r'$.O
  $|o_{ref}\rangle \leftarrow r'$.O[-1]
  $i \leftarrow |o_{ref}\rangle$.i
return P

Eavesdropping and SOP perturbations effects impact the propagation of the photons through the quantum channel. To reproduce eavesdropping, a module that emulates eavesdropping, i.e., third-party intercepting (measuring) photons at a fixed predefined rate, was implemented. Regarding SOP, a generator that reproduces fiber stressing events of different types and magnitudes was implemented. In addition to generate purely synthetic random SOP fluctuations, this module uses the experimental dataset containing 10,000 events of 4 seconds in [Ru20] to generate realistic ones. An example of generated SOP fluctuations is represented in Figure 4-4, where three events of incremental magnitude have been reproduced: a) fiber hit, b) fiber bending, and c) fiber shaking; the qBER values in Figure 4-4 represent the average performance when no polarization alignment is considered. We observe that a small hit produces a qBER increment and could be treated as random noise. Fiber bending introduces a slightly larger qBER and requires polarization alignment to keep high performance. Finally, fiber shaking highly increases qBER. Assuming a typical maximum qBER = 5%, the last two events would interrupt QKD operation.

For numerical evaluation purposes, we configured a 50-km QKD channel, which represents a reasonable distance for a metro network scenario. We assume currently commercial QTx and QRx, where photon generation rate is 1 GHz [ID20] and T_R is 2 μs [Ra20]. Moreover, a typical configuration for the key distillation process is considered, with sifted key rate, privacy amplification rate, and eavesdropping detection threshold are 45%, 10%, and 10%, respectively. With this configuration, a nominal KER of 4.5 Mb/s is achieved in the absence of SOP perturbations and eavesdropping.

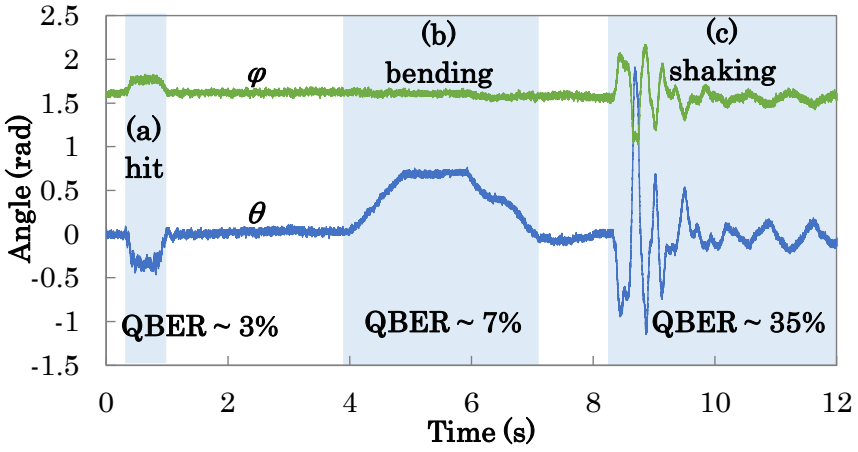


Figure 4-4- Three illustrative fiber stressing events.

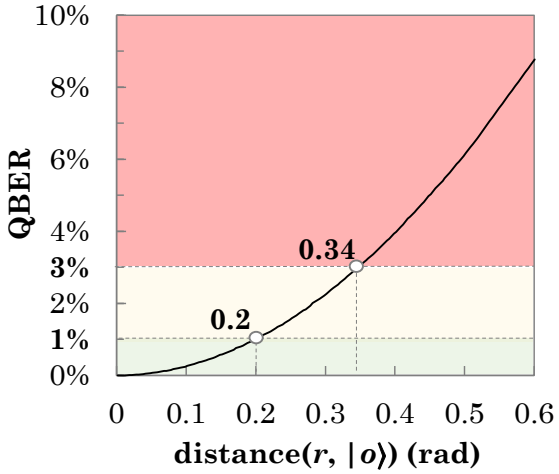


Figure 4-5- QBER vs distance(r, |o⟩).

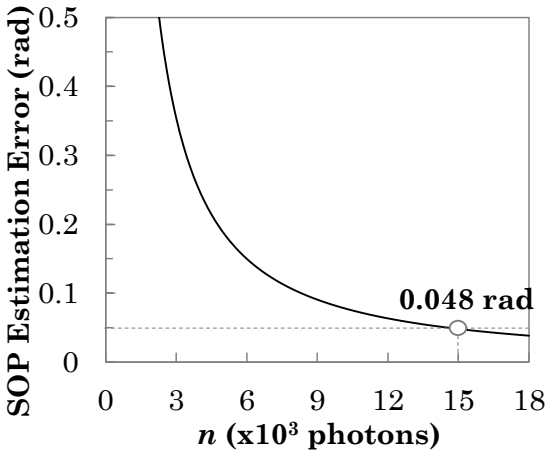


Figure 4-6- |o(t)⟩ estimation error.

With the aforementioned configuration, we conducted an experiment to compute the relation between qBER and distance(r, $|o\rangle$) and find d_{th} so as to achieve a given

desired performance, i.e., $qBER_{th}$. Specifically, we generated photons at a fixed polarization H and introduced random SOP perturbations in the quantum channel for a wide range of magnitudes. The polarization alignment in the EPC, i.e., r, was fixed and perfectly aligned with H. Then, we computed the obtained qBER as a function of the distance between the estimated SOP at the QRx, i.e., $|o\rangle$ and r. The results are presented in Figure 4-5, where we observe that distance($r, |o\rangle$) ≤ 0.34 produces qBER < 3%, whereas distance($r, |o\rangle$) = 0.2 produces qBER ~1%. Hereafter, we consider d_{th} = 0.2 and $qBER_{th}$ = 1% as a target reference value for performance evaluation purposes.

4.4.2 SOP monitoring and prediction

Let us now focus on evaluating the performance of the SOP monitoring process, i.e., $|o(t)\rangle$ measurement. We first need to analyze the error between true received polarization $|p(t)\rangle$ and estimated one $|o(t)\rangle$ as a function of the number of photons to decide the time for monitoring, i.e., To. To this aim, we generated photons with different polarizations and estimated the SOP in the QRx. Figure 4-6 plots the obtained SOP estimation error as a function of the number of photons (n) sent and received during the monitoring interval. In view of the figure, we can conclude that sending and measuring 15,000 photons results in negligible error estimation (lower than 0.05 rad), which leads to additional qBER < 0.1%. Such number of photons require 15 µs. Note that monitoring duration should be longer as time for qBER computation, SOP estimation, SOP prediction, and rotation plan computation needs to be spent. In consequence, we fix the monitoring time To = 1 ms, which should represent just a small portion of the total quantum channel operational period m.

Next, we focus on the performance evaluation of $|o(t+m)\rangle$ SOP prediction. To this aim, we selected 75% of all experiments and train the DNN-based SOP prediction model introduced in section 4.3 with different configurations of input, hidden, and output layers. We start by analyzing the operational time period m, which is of paramount importance for the efficiency of our approach. Figure 4-7a presents the prediction error as a function of m, computed as the difference between the SOP predicted for the next period at time t and the state measured at time $t+m$. For the sake of a fair comparative analysis, we fix w=500 ms. In all the cases, we considered 4 hidden layers, with 400, 200, 50 and 10 neurons using the tanh activation function. We observe that m=50 ms provides maximum deviation error below the target 0.2. Then, fixing m=50 ms, we now study the impact of w. Figure 4-7b shows the obtained error as a function of w. The results confirm the good selection used in the previous results; w lower than 500 ms starts reducing the accuracy whereas no additional value is added with larger window.

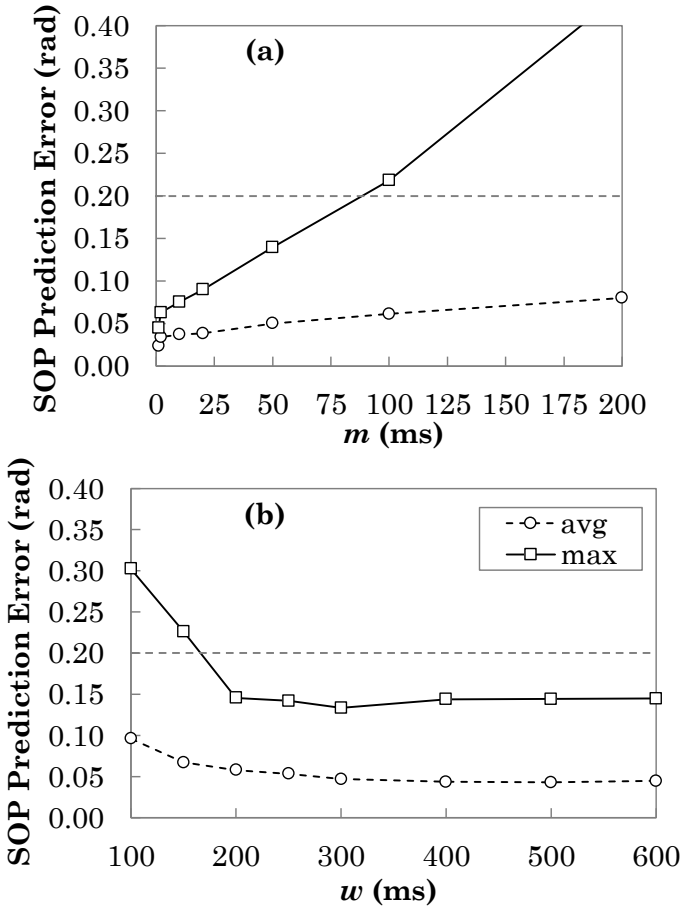


Figure 4-7- o(t+m)⟩ prediction performance.

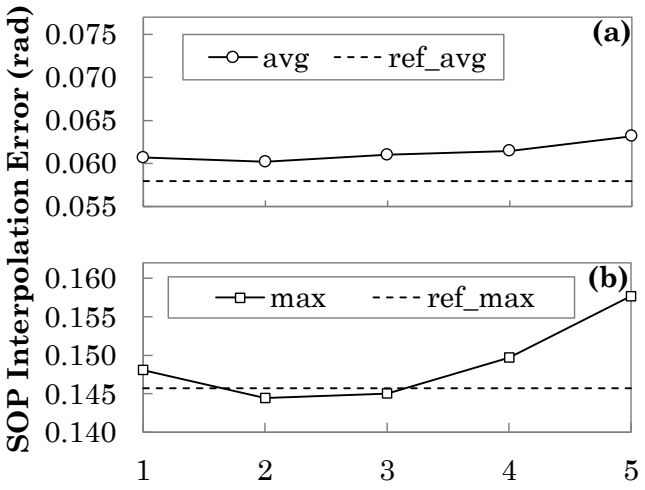


Figure 4-8- O interpolation error.

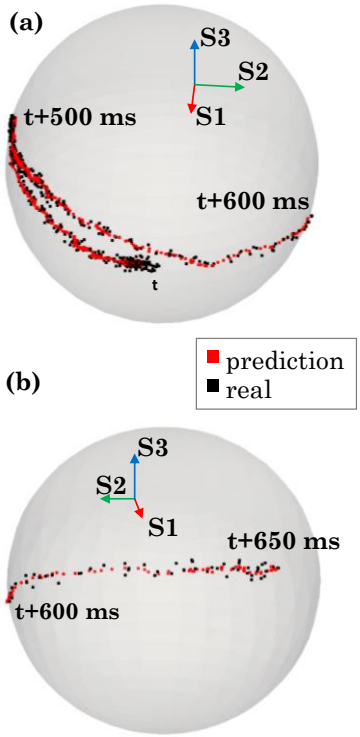


Figure 4-9- SOP tracking example

Finally, we evaluate the accuracy to interpolate SOPs between $|o(t)\rangle$ and $|o(t+m)\rangle$, i.e., sequence O estimation. *To* this end, we fixed k=100 intermediate SOPs (one state every 500 µs) and analyze the average and maximum estimation error as a function of the degree l of the fitting polynomials (Figure 4-8). As a reference, we plot the error obtained by the DNN to predict $|o(t+m)\rangle$. Interestingly, polynomials of degree 2 reach the highest performance, as average error is only 10% over that for $|o(t+m)\rangle$ prediction, while maximum error is even better than that.

In order to better visualize the accuracy of the combined DNN-based and polynomial fitting approach, Figure 4-9 presents the real and predicted SOPs projected in the Poincaré sphere for a 650 ms fiber shaking example. Figure 4-9a shows the first 600 ms, where SOP fluctuation covered around π/2 radians in 500 ms, followed by a sharp and fast change to the opposite direction covering π radians in just 100 ms. The event continues on the other side of the sphere (Figure 4-9b) doubling the speed to cover π radians in 50 ms. We observe that prediction is highly accurate regardless the speed of the event and the position on the sphere, which validates the proposed SOP prediction method.

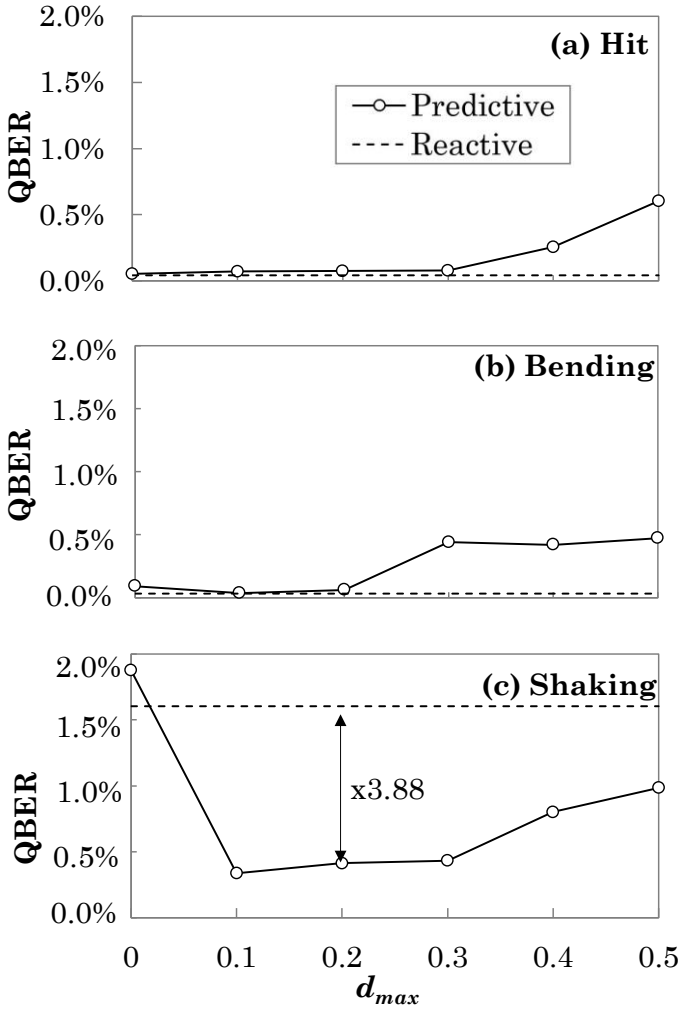


Figure 4-10- QBER vs d_{max} for various SOP fluctuation events.

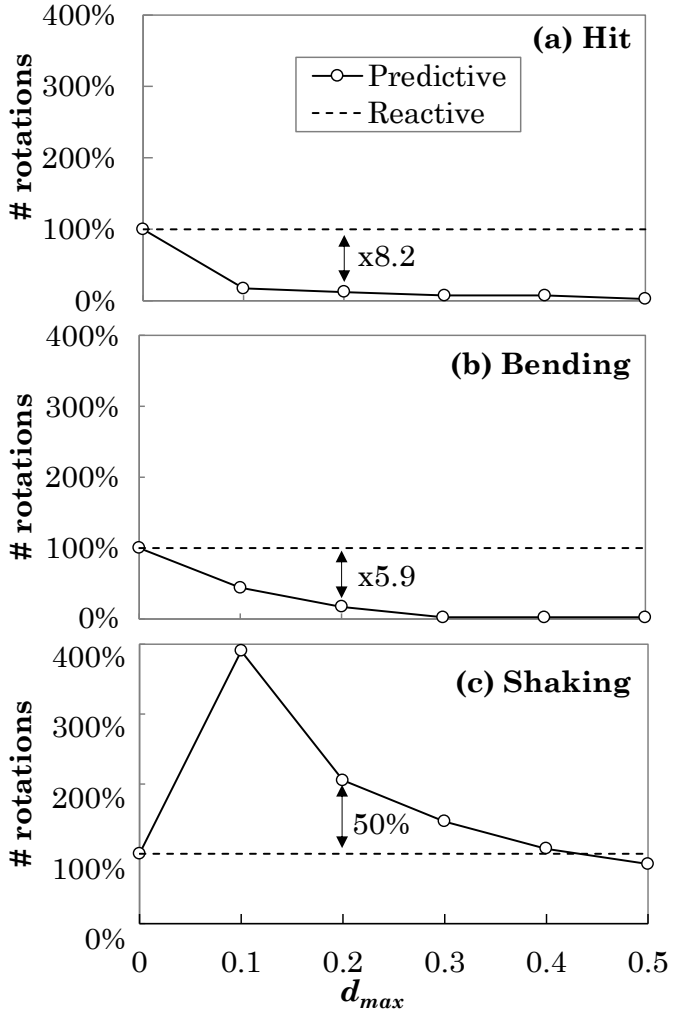


Figure 4-11- #rotations vs d_{max} for various SOP fluctuation events.

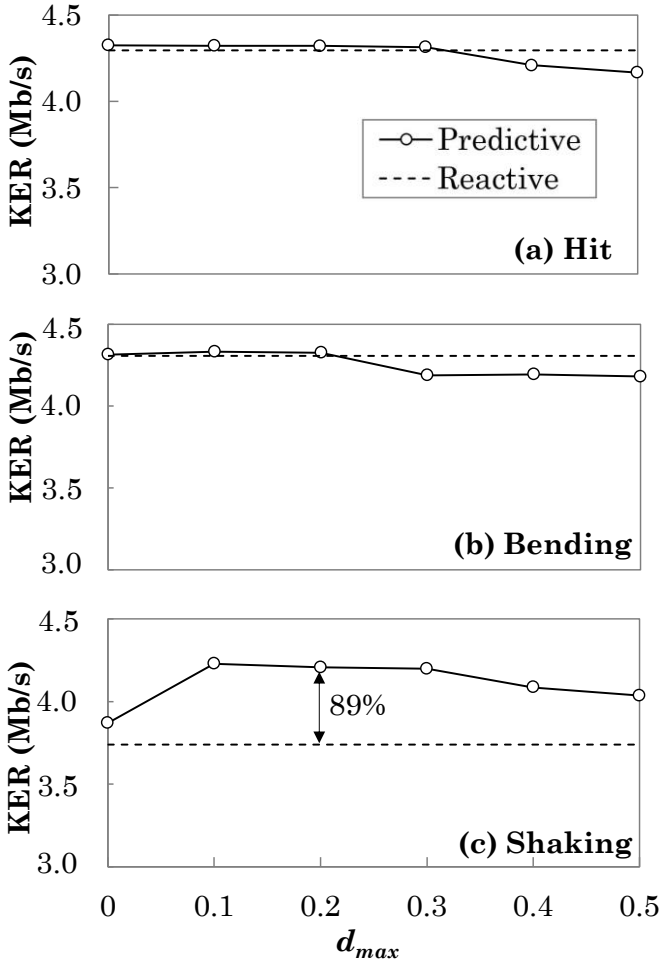


Figure 4-12- KER vs d_{max} for various SOP fluctuation events.

4.4.3 ML-based adaptive operation evaluation

From the previous results, we adopt the configuration T_O = 1 ms and m = 50 ms, which results into a remarkable low overhead of 2%, which is in line with the approach in [Ra20]. Let us now evaluate the ML-based adaptive approaches, where the configuration providing the best performance to estimate sequence O is now used in a set of simulations conducted to emulate QKD operation. The events reproduced in this evaluation belong to the 25% not used during the previous DNN training and polynomial models' evaluation. The reactive approach is also evaluated here with the same configuration, for comparison purposes.

The plots in Figure 4-10, Figure 4-11 and Figure 4-12 show the qBER, number of rotations performed, and KER under the adaptive ML-based method as a function of parameter d_{max}, respectively, and for the different type of events. For benchmarking purposes, the reactive approach is presented; recall that the reactive approach does

not depend on the value of d_{max}. All the values represent the average performance obtained in a sustained presence of events.

We observe that d_{max} = 0.2 is the best configuration, since achieves the overall highest performance in terms of qBER (<0.5%) and KER (close to the nominal value of 4.5 Mb/s). Interestingly, the performance of the predictive approach is as good as the reactive one in the presence of hit and bending events, whereas it remarkably improves the performance of the reactive in the presence of shaking events: 3.88 times lower qBER, which results in 89% increment in KER. The benefits of adaptability can be clearly seen by analyzing the number of rotations. The ML-based approach reduces noticeably the number of rotations as it performs rotations only when they are really needed, e.g., 8.2 and 5.9 times less rotations under hit and blending events to achieve the same performance than the reactive approach. However, in the event of heavy SOP fluctuations, the predictive approach performs more rotations compared to the reactive one. In Fig. 10c, 50% more rotations were needed in the event of fiber shaking. The results confirm the adaptability of the proposed ML-based approach.

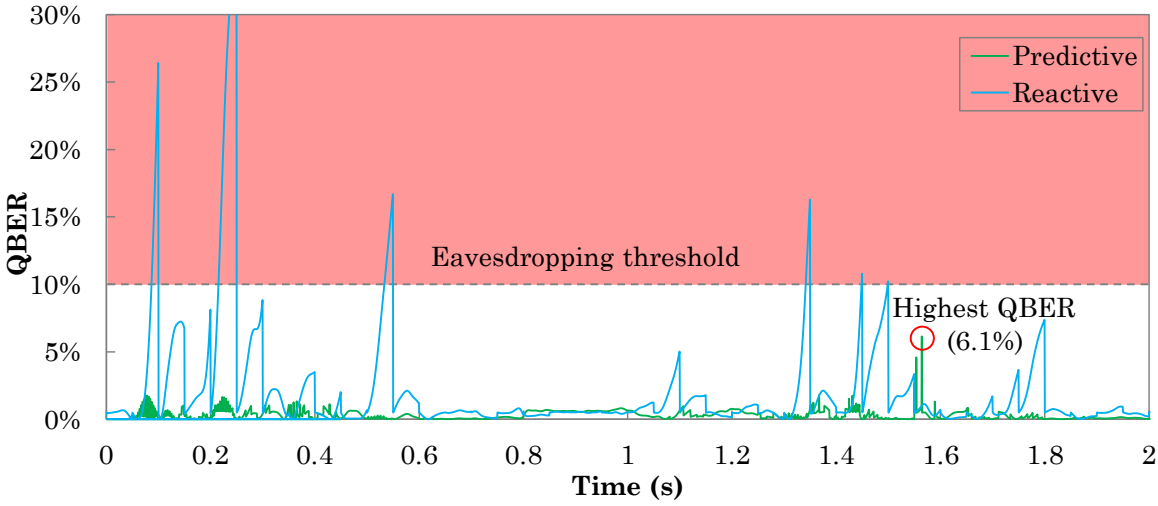


Figure 4-13- Example of QKD performance during a fiber shaking event.

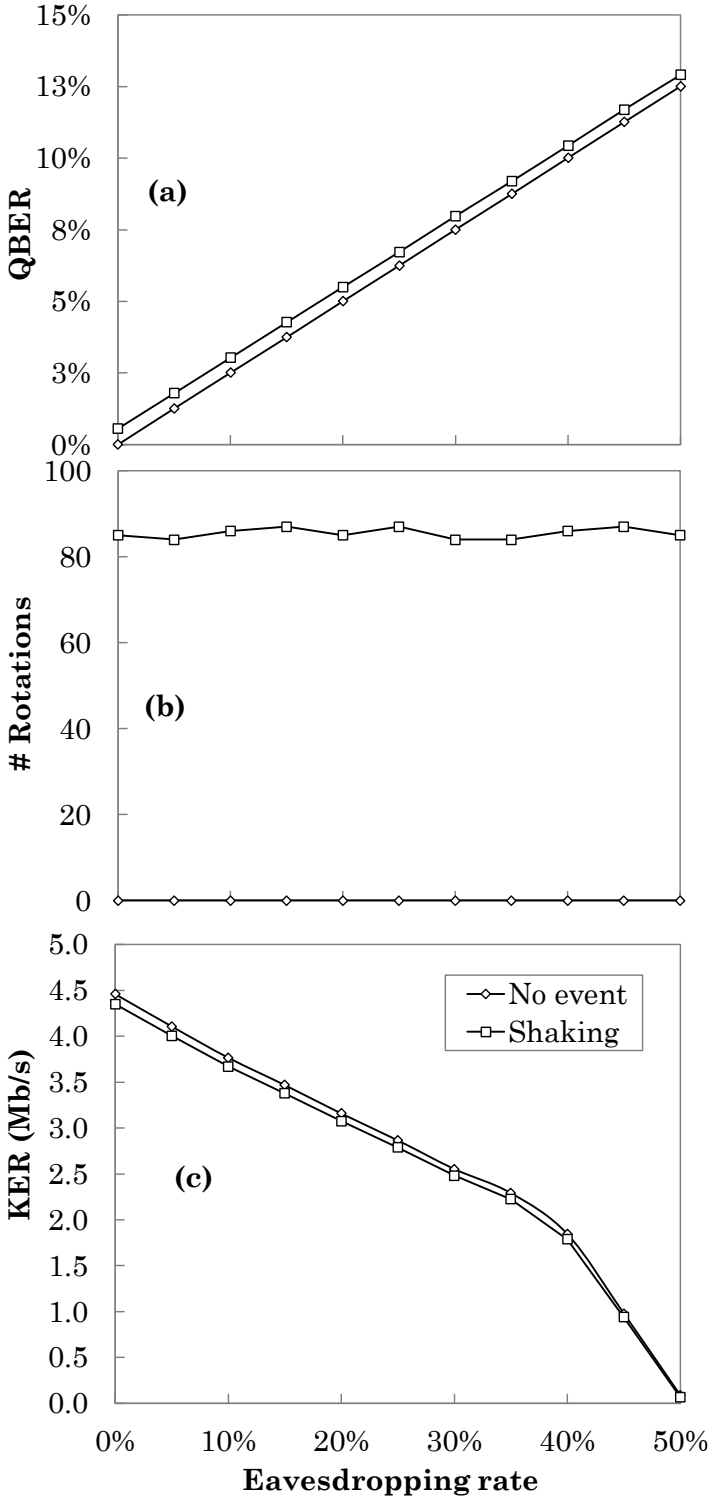


Figure 4-14- Impact of fiber stressing events on eavesdropping detection.

The previous results show clear benefits of the ML-based adaptive approach with respect to the reactive one, from analyzing the average performance. However, if we analyze event by event, the benefits are even larger. An example is presented in

Figure 4-13, where the obtained qBER as a function of time is presented for a fiber shaking event; monitoring periods are not represented for the sake of clarity. We observe that the reactive approach produces high qBER in general and several peaks exceed the eavesdropping threshold (maximum 35%), which lead to intervals where no keys can be exchanged after the key distillation process. In contrast, the proposed ML-based adaptive approach produces low qBER continuously, which is only altered with some isolated peak (maximum 6.1%), which is well below the eavesdropping threshold, and key exchange is never disrupted during the whole event. This fact results in a less variable secret key exchange flow, which might be beneficial from the security of the overall system.

Table 4-3: Performance comparison during shaking events

Approach	QBER	KER (Mb/s)	# Rotations
ML-based (m=50ms, d_{max}=0.2)	0.41%	**4.21**	**205%**
Reactive (m=50ms)	1.60%	3.73	100%
Reactive (m=8ms)	**0.07%**	3.96	624%

The performance of the reactive approach can be improved by reducing the operational period m, so to add more adaptability in the presence of heavy events, at the cost of reducing the efficiency, and thus the KER. Specifically, in the following results we consider m=8 ms, which is in line with [Ra20]. Table 4-3 summarizes the obtained results under shaking events. The new configuration for the reactive approach shows best performance in terms of qBER, even improving that of the predictive one. However, the shorter operational time reduces the throughput of secret key exchanges since the overhead becomes more significant. Moreover, this configuration performs a remarkably larger number of rotations compared to the predictive approach, which is demonstrated to provide the largest KER.

4.4.4 Robustness against eavesdropping

Finally, let us evaluate the robustness of the proposed ML-based adaptive approach in the presence of eavesdropping. Two different cases have been studied while eavesdropping is being active: i) no fiber stressing event is produced; and ii) a large shaking event is produced. Figure 4-14 shows the computed qBER, number of rotations and resulting KER as a function of the eavesdropping rate, defined as the probability that an eavesdropper intercepts a photon. We observe from Figure 4-14a that the proposed ML-based SOP tracking and polarization compensation is able to reduce the qBER in the case of the shaking event to values that are in slightly above to those when no event is produced, and it leaves eavesdropping effects uncorrected.

Figure 4-14b shows the number of rotations, which are totally independent of the eavesdropping rate. Finally, Figure 4-14c shows that the resulting KER are remarkably close in both cases. In conclusion, the performance of our proposed ML-based approach is noticeably robust against eavesdropping.

4.5 Conclusion

The polarization based QKD technology is ready for its deployment in real telecom operators' networks and commercial solutions already exist. The main challenge, however, is its very high cost coming from both, hardware requirements of the QTx and QRx, and from the high sensitivity of the quantum channel to polarization variations.

A ML-based SOP tracking and polarization compensator has been presented that might significantly reduce the cost of polarization encoded QKD systems by simplifying the specifications of QTx and QRx and enabling the use of aerial optical fiber cables. The proposed system is based on three main components: i) a SOP monitoring procedure able to precisely estimate the current SOP while minimizing overhead; ii) a lightweight ML-based SOP prediction that is able to accurately forecast future SOP evolution with fine granularity; iii) a Poincaré sphere rotation planner, which decides when rotations need to be performed and the magnitude of such rotations to compensate polarization drift and keep qBER under a given threshold.

The SOP monitoring consists in periodically sending a number of photons with known polarization, so the QRx can accurately estimate the current SOP. In the results, we showed that the estimation error is 0.05 radians when the number of photons sent is 15,000. Such error translates, in the worst case, into an additional qBER of 0.1%, which is almost negligible. Besides, the time to transmit such number of photons is 15 µs, which leaves time to the next components to perform their needed computation. Here, we estimate that a total of 1 ms can be dedicated to SOP monitoring, tracking, and polarization compensation, so the other two components need to be fast and produce accurate decisions, so the total overhead of the proposed system is low.

The ML-based SOP prediction actually consists of two subcomponents: i) a DNN model to predict at time t the SOP for time $t+m$; and ii) a fine grain SOP evolution predictor based on polynomial fitting. The results showed that by fixing m to 50 ms maximum estimation error is below 0.15 radians, which translates, in the worst case, into additional qBER below 0.5%. Such value of m results into a noticeable low system overhead of 2%. Regarding the granularity of polynomial fitting, it was fixed to 500 µs and we showed that a polynomial of degree 2 provides low enough average prediction error.

The rotation planner was modeled as an optimization problem and an efficient greedy heuristic was devised. The results showed that a maximum distance between the current polarization in the QRx and the estimated SOP of 0.2 radians results into low qBER and KER close to the nominal value. With such configuration, the rotation planner showed exceptional performance, as qBER was reduced 3.88 times and KER increased 89% under realistic shaking events, as compared to a reference polarization compensator.

Finally, the proposed system showed total neutrality against eavesdropping, so the system does not interfere its detection.

Chapter 5

Experimental assessment of SOP compensation in Discrete Variable Quantum Key Distribution

In this chapter, the methods defined in chapter 4 to detect the SOP of receiving photons in QRx as well as to compensate for the photons' distortion due to optical components imperfections are experimentally verified.

QKD, a technology that enhances security between trusted users, employs various protocols, including the BB84 protocol that uses single polarized photons as qubits. However, the transmission of polarized photons between a QTx and a QRx via fiber can result in distortion due to fiber movements that affect the SOP, thereby reducing the Key exchange rate. To address this issue, a novel QKD method, which includes an AI-based polarization distortion compensator module in chapter 4 is proposed. This QKD method is set to be tested in a laboratory equipped with the necessary instruments and devices at NGNCS laboratories of UCDavis, California, USA. Additionally, software-based modules that model each component of the testbed to overcome imperfections created by uncalibrated components is developed.

5.1 Introduction

QKD deployments are not limited to telecom networks, but are also expected to be utilized in data centers and other mission-critical infrastructures. Consequently, any enhancement in key rate effectiveness will undoubtedly attract the attention of the industry, particularly in regard to increasing the security level of the internet, particularly with respect to 5G and beyond communication systems, computation and storage infrastructures, and applications. In this regard, the sustainable innovation capacity of proposed DV-QKD encompasses enabling new secure applications and services, impacting the product portfolios of the industry, and bringing significant societal benefits to citizens.

QKD is a security technology that leverages the principles of quantum mechanics to enable the detection of eavesdropping attempts and ensure the security of the key. While polarization encoded QKD has been successfully tested in laboratory experiments and closed environments, its main drawback is its high cost. This is primarily due to the requirements for quantum transmitters and receivers and the need for careful selection of fibers that support the quantum channel to minimize environmental effects that can significantly alter the SOP of photons.

The proposed QKD method is expected to have a significant impact on the deployment of QKD systems to provide long-term data protection in a post-quantum world by reducing its cost. On one hand, the SOP imperfections can be corrected by the QRx, which means that some hardware specifications of the QTx can be relaxed. On the other hand, the hardware design and offsets of the QRx can be simplified and addressed through software.

In addition to the AI-based methods discussed in Chapter 4, it is imperative to ensure that the SOP detection and compensation methods incorporated in the proposed algorithm are effective. To achieve this objective, numerous experiments have been defined and verified in the current chapter. Prior to detailing the experiments, it is necessary to describe the testbed and implementation particulars.

The rest of the chapter is organized as follows. Section 5.2 presents testbed description and implementation details. Section 5.3 describes defined experiments and achieved results. Finally, Section 5.4 draws the main conclusion and impacts of the work.

5.2 Testbed Description and Implementation Details

In this section, on the one hand, photon generation and detection which are needed for BB84 implementation are experimentally ensured, and on the other, the

polarization distortion compensator (called SOP event compensator) module is validated. Polarized photons generated by the transmitter should be received in a way that the photons are counted correctly.

5.2.1 Planned Testbed

The expected testbed consisted of one QTx and one QRx, each with a set of optical components as depicted in Figure 5-1. In the QTx, the testbed included:

a) Weak Coherent Pulses (WCP) as SPE that sourced polarized photons.

b) Polarization Encoder, which polarized the photons emitted by the SPE and launched them into the fiber.

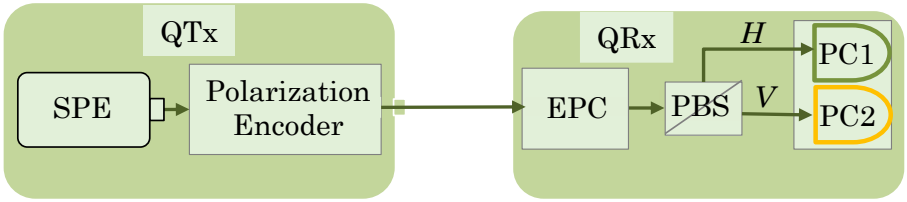


Figure 5-1- Main components of the testbed

In the QRx, the following components were considered:

c) EPC, which was used for polarization dependent loss mitigation. An EPC with maximum rotation rate of 360°/sec was available.

d) PBS that split the signal based on its SOP

e) SPD that counted photons. Its detection was in the infrared range.

5.2.2 Deployed Testbed

The deployed testbed is presented in Figure 5-2, where the main testbed components are shown. There are some differences with respect to the defined testbed.

In the QTx, the deployed testbed included:

a) SPE was unavailable and was replaced with WCP (not shown in the picture). The WCP consisted of a laser source (1551 nm, -13 dBm) plus fixed and variable optical attenuators (VOA).
b) Polarization encoder components were a polarizer and Manual PC (MPC) to generate the desired SOP of the beam.

In the QRx, the following components were used:

c) An EPC that was supposed to compensate and control the SOP. The EPC's model was Agilent/HP 11896A.
d) The PBS received the photons and split them into either H or V SOPs.

e) The Single photon counters (SPD or PC) that counted the received photons.
f) Dual power Sensors were also used to verify the SPDs counts are reasonable or not.

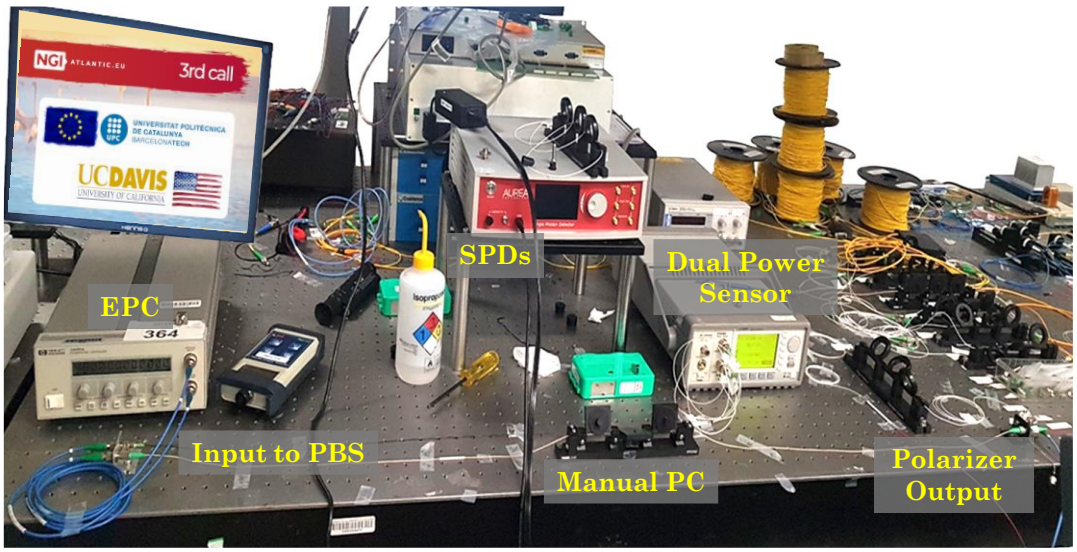


Figure 5-2- Deployed Testbed in UC Davis

5.3 Tests and results

This section collects all the tests performed during the collaboration with UCDavis and it is organized in 3 subsections:

1. Set-up experimental tests, needed to verify the experimental set-up.
2. Preliminary experimental results, performed to extend previous verifications so as to detect inconsistencies.
3. Final experimental tests, to validate the proposed QKD method.

5.3.1 Set-up Experimental tests

In this section, the setup experimental results of the tests are shown. Specifically, two initial experiments had been outlined to validate the testbed.

5.3.1.1 Verifying the SPE

Description:

To build a SPE for QTx, a C-band distributed feedback laser was attenuated. As shown in Figure 5-3 the operating wavelength of the laser was 1551.74nm and the minimum power output of the laser unit was -10 dBm. To reach a range of 1000

photon/second level, one fixed attenuator with 40 dB attenuation was placed. At 1550 nm, 1 mW (0 dBm) power approximately corresponded to 1016 photon/second. To flexibly tune the photon rate, a VOA was used. VOA operation range was 0 to 60 dB attenuation. The insertion loss of the VOA unit was recorded as 4 dB experimentally. The VOA is run above in the 15 dB attenuation range. In this way, even without the added insertion loss of the units, the SPE could not exceed -65dBm optical output which was the maximum optical input power for the SPD.

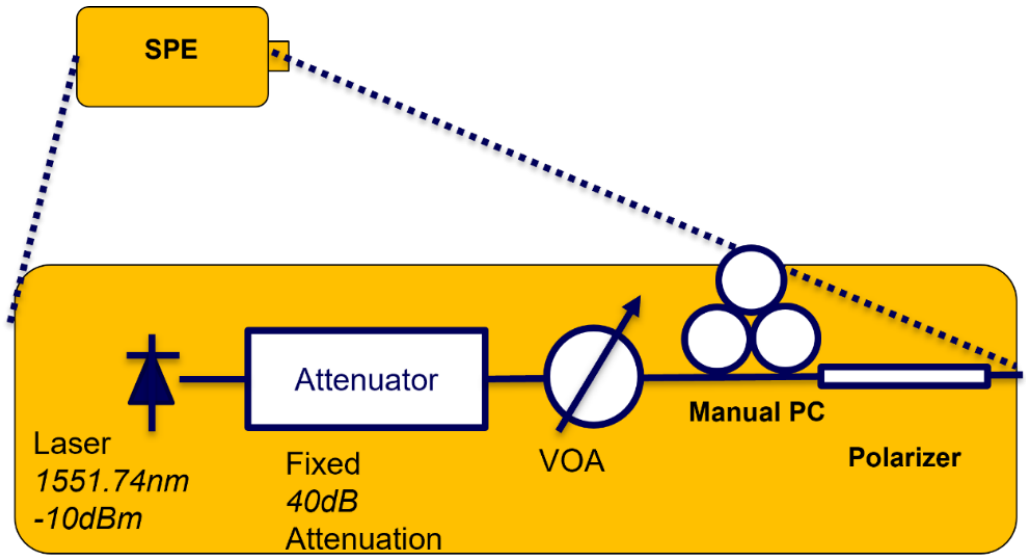


Figure 5-3- Experimental setup for highly attenuated laser sources.

While all the fiber-based components have single mode fibers, a manual fiber-loop based polarization controller and a polarizer were included. In this way, the SOP of the SPE output is well known and aligned to the fast axis of the polarizer.

Execution Plan:

As we mentioned in the plan, the VOA above 15 dB attenuation was run, meaning that the total starting attenuation for the input laser was 65 dB. the VOA attenuation was incrementally increased from 15db to 53db to find an input power level corresponding to 1000 photons in 0.1 sec counted in PC1. As we can see in Figure 5-4, the fiber from the SPE is directly connected to one of the PCs (PC1) without using a PBS to have minimum photon loss.

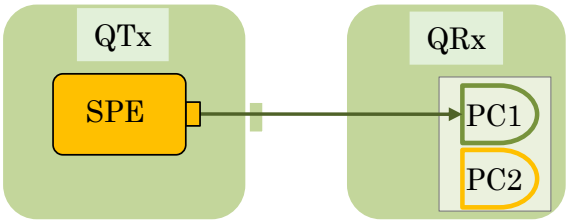


Figure 5-4- Configuration for the SPE Verification

Experimental Results:

As we can see in Figure 5-5, the VOA attenuation level increased from 15 to 52 db. For each attenuation level, the SPE continued sending the photons for 20 seconds. PC1 counted them in 0.1 second integration time. This means the counter waited 0.1 second to measure the received photons.

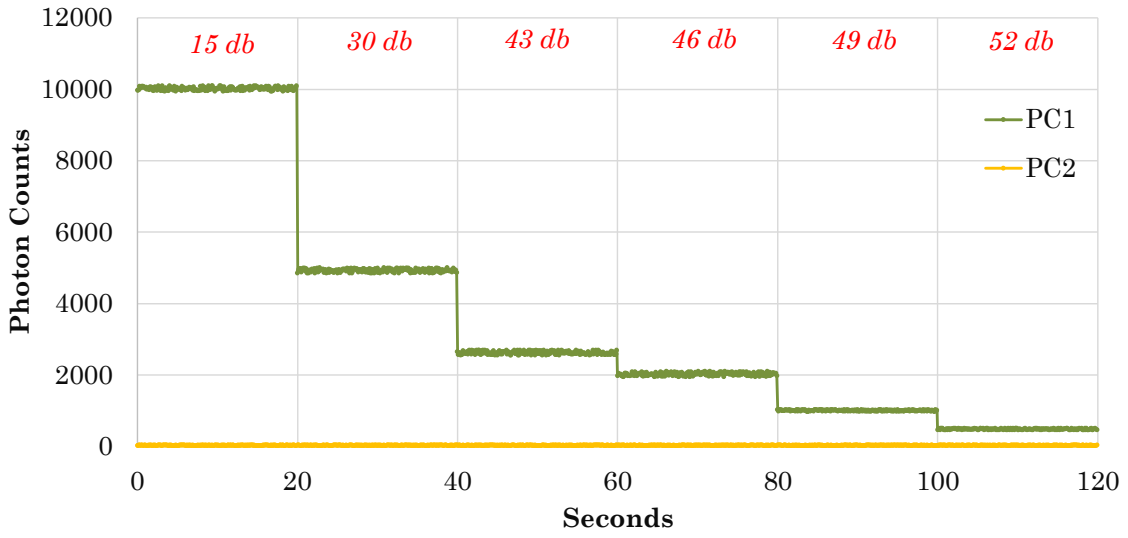


Figure 5-5- Number of counted photons in PC1 and PC2 with different attenuation level in SPE

Conclusion:

The results show that with a VOA attenuation level of 49 dB, we could have 1000 photons counted in the photon counter. So, buckets of 1000 photons can be generated with these configurations settings in the SPE (QTx) and SPDs or PCs (QRx): VOA= 49db attenuation (total attenuation=49 + 40 + 10 = 99 dB), integration time in PCs = 0.1 seconds.

5.3.1.2 Verifying the Polarization Encoder, fiber, PBS and SPDs

Description:

The QTx sends predefined sequences of polarized photons and the PCs should count them correctly. The EPC must be tuned to not introduce any polarization effect. The aim of this verification is to ensure that emitted polarized single photons by the SPE can be encoded and received in any SOP.

Plan:

Figure 5-6 illustrates the setup used for this test. Polarized single photons emitted by SPE should be passed through a polarization encoder to be in specific SOPs. To ensure that all SOPs can be covered, the SOP of the emitted photons are encoded in six states on the Poincare sphere, i.e., H, V, D, A SOPs, Right-handed Circular (RC),

and Left-handed Circular (LC). Then, these polarized photons passing the quantum channel (fiber) entered the PBS. Next, the photons reached the PBS to be split in PC1 or PC2.

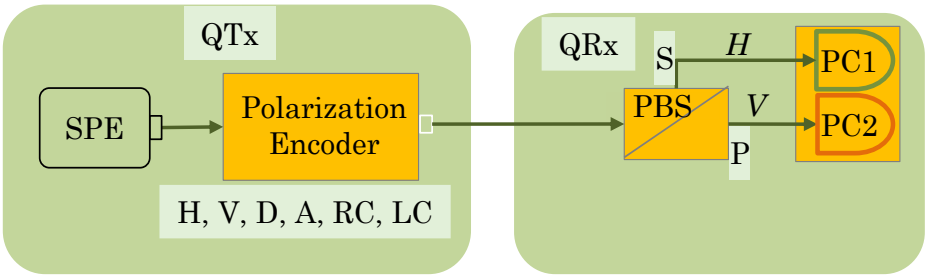


Figure 5-6- Configuration for the MPC, Fiber, PBS and PCs test

Execution plan:

SPE should emit six different SOPs (1000 photons for each) in order (H, V, D, A, RC, and LC).

Expected Results:

For these six sets of different polarized photons, we should receive:

1. H: 1000 photons should be counted in PC1, Nothing in PC2.
2. V: 1000 photons should be counted in PC2, Nothing in PC1.
3. D, A, RC and LC: 500 photons in PC1 and 500 photons in PC2.

Execution details:

As we mentioned before, an attenuated laser source was hired as an SPE and it was difficult to precisely generate 1000 photons in QTx. As a result, it was necessary to perform multiple experiments just to acquire which power of the beam passing through the attenuators would generate the desired number of photons without considering the SOP.

Experimental Results:

The beam with the desired number of photons passed through a polarizer and MPC to generate the specific SOPs. For instance, Figure 5-7 and Figure 5-8 show the configuration of MPC in the QTx needed to generate A and D SOPs, respectively.

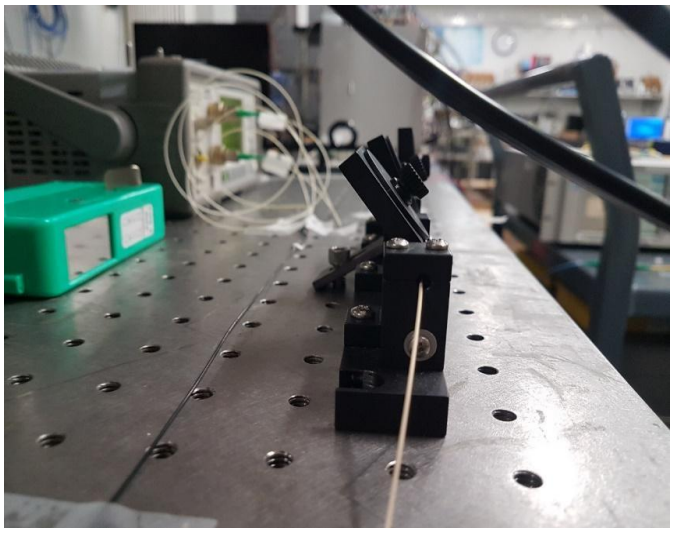


Figure 5-7- MPC configuration for A SOP

Figure 5-8- MPC configuration for D SOP

Then, the PBS split them into either PC1 or PC2. With the aforementioned testbed, we performed the following measurements:

1- H SOP: 1084 photons in PC1, 336 photons in PC2.

2- V SOP: 289 photons in PC1, 1234 photons in PC2.

3- D SOP: 714 photons in PC1 and 807 photons in PC2.

4- A SOP: 753 photons in PC1 and 870 photons in PC2.

5- RC SOP: 692 photons in PC1, 801 photons in PC2.

6- LC SOP: 759 photons in PC1, 886 photons in PC2.

While detailing the expected results, the dark counts in the execution plan were not considered. PCs were affected by the dark count rate that is the average rate of

registered counts without any incident light. So, to validate if these data were reasonable, the magnitude of the dark counts was computed. To this aim, measurements of the photons connecting the WCP directly to the PCs were carried out. With this configuration, sending approximately 1000 photons to each PC1 and PC2, the measurements are the following:

PC1 counted 1220 photons, PC2 counted 1280 photons. So, the dark counts in PC1 and PC2 were 220 and 280, respectively.

Then, the corrected results after the dark count subtraction were computed:

1. H: 1084 – 220: 864 in PC1 & 336 – 280: 56 in PC2
2. V: 289 – 220: 69 in PC1 & 1234 – 280: 954 in PC2
3. D: 714 – 220: 494 in PC1 & 807 – 280: 527 in PC2
4. A: 753 – 220: 533 in PC1 & 870 – 280: 590 in PC2
5. R: 692 – 220: 472 in PC1 & 801 – 280: 521 in PC2
6. L: 759 – 220: 539 in PC1 & 886 – 280: 606 in PC2

Conclusion:

Although the results were not as precise as the expected results, they confirmed the correct generation of photons with desired SOPs in the QTx as well as the correct installation of the fiber between QTx and QRx, PBS and PCs in the QRx. The misalignment was related to the fact that the SOPs were being visually encoded with the MPC. To produce more precise results, an accurate polarimeter were needed.

5.3.2 Preliminary experimental tests

This section shows the preliminary experimental results of the tests. Specifically, two initial experiments are outlined to validate the proposed QKD method. For the ease of understanding, the complete description and plan of each experiment is provided before showing the actual implementation and experimental results.

5.3.2.1 Verifying the SOP estimation function

The SOP estimation function plays a key role in our proposed QKD method to compensate for SOP distortions in the Quantum channel. It estimates the SOP distortion taking advantage of quantum mechanics principles.

Description:

The QTx emulates SOP effects by sending predefined sequences of polarized photons that would correspond to the desired SOP distortion. A function will recognize the distortion using an MPC before the PCs. The aim of this verification is to ensure that the distortion amplitude estimation arising in the quantum channel is possible.

Plan:

As we can see in Figure 5-9, QTx generates three buckets each containing 1000 horizontally polarized photons, and sends them to the QRx through the fiber. Next, SOP changes should be introduced to the MPC at the QRx in a way that: 1) wave plates are oriented at 0'; 2) half wave plate oriented at 22.5'; 3) next quarter wave plate oriented at 45'; 3) the final quarter wave plate oriented at 45'. By having the photon counters outcome after the mentioned procedure, calling the function to estimate the SOP defined in QTx is possible.

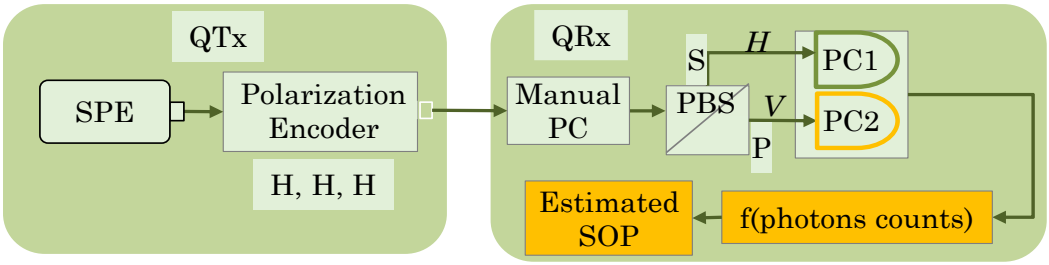


Figure 5-9- Configuration for the SOP estimation verification function test

Execution plan:

The MPC at the QRx should be aligned in a way that it converts H polarization to D. In the first phase, three buckets of 1000 horizontally polarized photons are sent. In the next phase, the experiment with converting H polarization to A is repeated, to ensure that the SOP estimation function was able to distinguish between D and A polarizations.

Expected Results: (numbers specify the counted photons)

Phase 1:

- ✓ First bucket: PC1: 500, PC2: 500.
- ✓ Second bucket: PC 1: 1000, PC2: 0.
- ✓ Third bucket: PC 1: 500, PC2: 500.

Phase 2:

- ✓ First bucket: PC1: 500, PC2: 500.
- ✓ Second bucket: PC1: 0, PC2: 1000.
- ✓ Third bucket: PC1: 500, PC2: 500.

Experimental Results:

In this scenario, half wave plates in the MPC in the QTx were configured to generate horizontally polarized photons. In the QRx, MPC was configured the way shown in Figure 5-8 for phase 1 and Figure 5-7 for phase 2. With the aforementioned testbed, the following measurements were performed:

Phase 1:

- ✓ First bucket: PC1: 870 photons, PC2: 780 photons.
- ✓ Second bucket: PC1: 1200 photons, PC2: 400 photons.
- ✓ Third bucket: PC1: 860 photons, PC2: 780 photons.

Phase 2:

- ✓ First bucket: PC1: 850 photons, PC2: 775 photons.
- ✓ Second bucket: PC1: 400 photons, PC2: 1270 photons.
- ✓ Third bucket: PC1: 870 photons, PC2: 770 photons.

Considering the Dark Photon Counts: PC1 counts 220 photons, PC2 counts 280 Photons, the corrected results for the rotation function after dark count subtraction were computed.

Phase 1:

- $qBER_{first\text{-}bucket} = (PC2 - PC2_{dark\text{-}count}) / (PC1 - PC1_{dark\text{-}count}) + (PC2 - PC2_{dark\text{-}count}) = \mathbf{0.44}$
- $qBER_{second\text{-}bucket} = (PC2 - PC2_{dark\text{-}count})/ (PC1 - PC1_{dark\text{-}count}) + (PC2 - PC2_{dark\text{-}count}) = \mathbf{0.1}$
- $qBER_{third\text{-}bucket} = (PC2 - PC2_{dark\text{-}count}) / (PC1 - PC1_{dark\text{-}count}) + (PC2 - PC2_{dark\text{-}count}) = \mathbf{0.44}$
- $S1 = 1\text{-}2*qBER_{first\text{-}bucket} = \mathbf{0.12}$
- $S2 = 1\text{-}2*qBER_{second\text{-}bucket} = \mathbf{0.8}$
- $S3 = 1\text{-}2*qBER_{third\text{-}bucket} = \mathbf{0.12}$

Which is approximately **diagonal**.

Phase 2:

- $qBER_{first\text{-}bucket} = (PC2 - PC2_{dark\text{-}count}) / (PC1 - PC1_{dark\text{-}count}) + (PC2 - PC2_{dark\text{-}count}) = \mathbf{0.44}$
- $qBER_{second\text{-}bucket} = (PC2 - PC2_{dark\text{-}count})/ (PC1 - PC1_{dark\text{-}count}) + (PC2 - PC2_{dark\text{-}count}) = \mathbf{0.85}$
- $qBER_{third\text{-}bucket} = (PC2 - PC2_{dark\text{-}count}) / (PC1 - PC1_{dark\text{-}count}) + (PC2 - PC2_{dark\text{-}count}) = \mathbf{0.43}$
- $S1 = 1\text{-}2*qBER_{first\text{-}bucket} = \mathbf{0.12}$
- $S2 = 1\text{-}2*qBER_{second\text{-}bucket} = \mathbf{-0.7}$
- $S3 = 1\text{-}2*qBER_{third\text{-}bucket} = \mathbf{0.14}$

Which is approximately **Anti-diagonal**.

Conclusion:

The aforementioned experiment was defined to be performed with the MPC, which could not precisely change the SOP and it was visually adjusted. Considering this imperfection, the polarization movement in the MPC was approximately estimated using the SOP estimation function. In conclusion, these preliminary results support the SOP estimation function verification.

5.3.2.2 Verifying the EPC

Beside the SOP estimation function, proposed QKD method needs an EPC to automatically receive desired SOP rotation from the software and apply it to the photons in transmission. Taking this into account, it is difficult to use a MPC to quickly convert any input SOP to any desired output SOP, as its wave plates should be manually configured. Also, the software should translate the rotation to the input setting of the EPC. So, it should be verified that extracting the EPC's characteristics as well as how to tune it in a way that any SOP conversion is possible.

Description:

The EPC is configured with different rotations that introduce different polarization effects. The QTx sends predefined sequences of polarized photons and the PCs count them correctly with respect to the rotations. The aim of this verification is to ensure the recognition of the original SOP.

Plan:

This verification consists of two phases. First, a specific rotation to the EPC (1 in Figure 5-10) is introduced. Second, the QTx is configured to generate photons with four different SOPs (2) to determine whether QRx can measure the desired results in the photon counters.

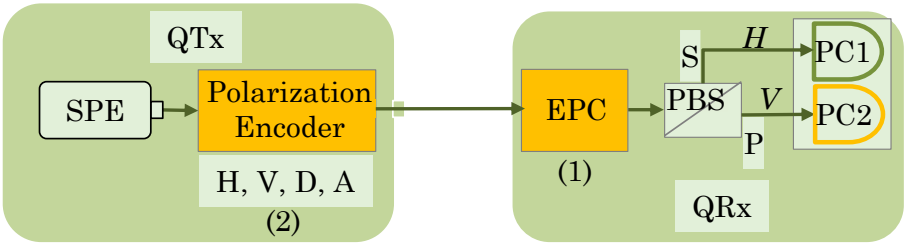


Figure 5-10- Configuration for the EPC verification test

Execution plan:

In the first phase, the EPC is configured with the SOP (s1=1, s2=0, s3=0) to be converted to (s1=0.7071, s2=0.7071, s3=0). Then, the single photons are sent in four cases. The number of photons is 1000 for all the cases.

1- H photons. 2- V photons 3- D photons 4- A photons

Expected Results:

1 & 4 - PC1.counts ≈ 854, PC2.counts ≈ 146

2 & 3 - PC1.counts ≈ 146, PC2.counts ≈ 854

Experimental Results:

During the execution of this test, characterization results were obtained for an Agilent/HP EPC (see in Figure 5-2) that were not in line with those expected. The setup presented in Figure 5-11 were implemented to understand why the attempts to find out the EPC's behavior were not successful and those EPC settings for the experiments were not usable.

The transmitter consisted of a laser source, a fixed attenuator, a variable attenuator, and two MPCs connected before and after a polarizer. A laser source with 10 dBm power was attenuated with a fixed attenuator of 40 dB loss and a variable attenuator (configured with 0 dB loss in this experiment). Then, a MPC was connected before the polarizer to align the signal polarization to the polarizer axis and maximize the power at its output. Another MPC was used to set the polarization of the transmitted photons to the receiver.

The receiver consisted of the EPC under test, a PBS and power sensors. The EPC received the photons and changed their SOP based on its setting (rotation) of four fiber loops inside the EPC. These settings were fixed to 500-500-500-500. The PBS split the photons (optical power) depending on the input SOP of photons to the PBS. A computer was used to record the power reading from power sensors (PD1 and PD2) at every 1 second.

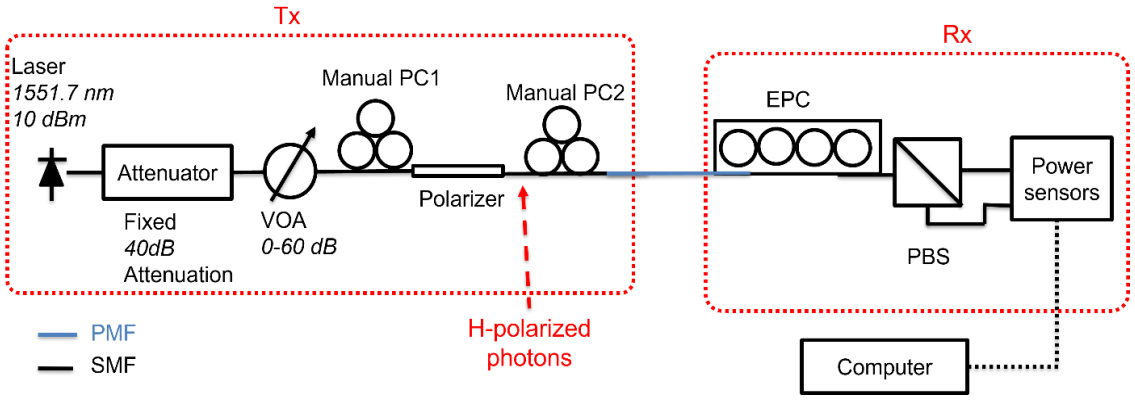


Figure 5-11- Implemented testbed

The setup kept running and the samples were recorded when the EPC was ON and configured to 500-500-500-500 (see Figure 5-12). When EPC was ON, the power ratio drifted over time. The possible reasons for this fluctuation could be the change in temperature of EPC and causing some instability and calibration issues with the fiber loops inside the EPC.

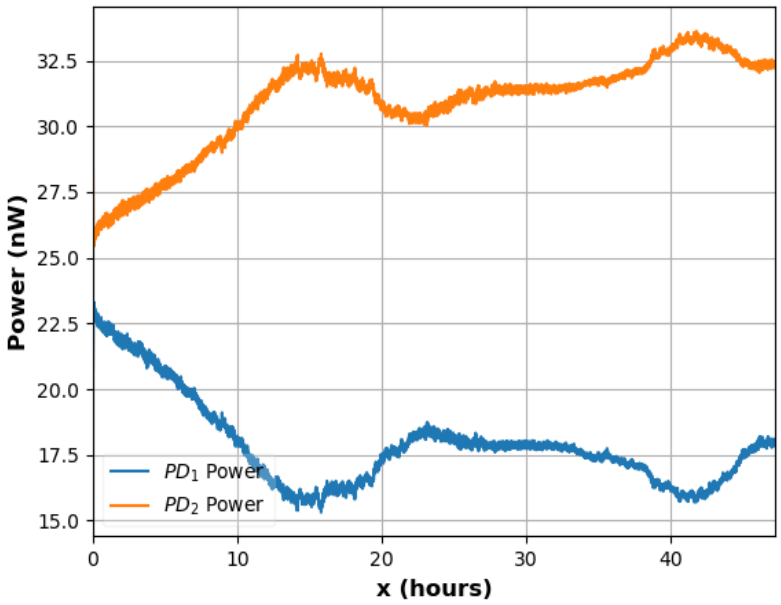


Figure 5-12- Observed Power Drift

Due to this power fluctuation over a time scale comparable to the one required to carry out the calibration procedure (ideally the two orange and blue curves should have been almost flat), the results of the calibration could not be used as they were time dependent.

5.3.2.3 Verifying Phoenix EPC stability

The Agilent/HP EPC was replaced with a second EPC from Phoenix Photonics. First, the stability of the device was needed to be checked to understand whether it can be used or not. As we can see in Figure 5-13, QTx sent buckets of 1500 photons and the polarization encoder polarized the photons with some specific SOP. Then the EPC in the QRx was fixed to some specific setting (three voltages) and photons passing through the fiber and EPC, were split by PBS and finally counted by PCs. This procedure continued for a long time (2000 seconds) to see if polarization drift in the photon counts' proportion can be seen or not.

Experimental Results:

As illustrated in Figure 5-13, photons were split and counted in PC1 and PC2 in a stable manner during a long time period. This means that the SOP of the photons did not drift due to EPC miscalibrations and it can be safely used on the experiments.

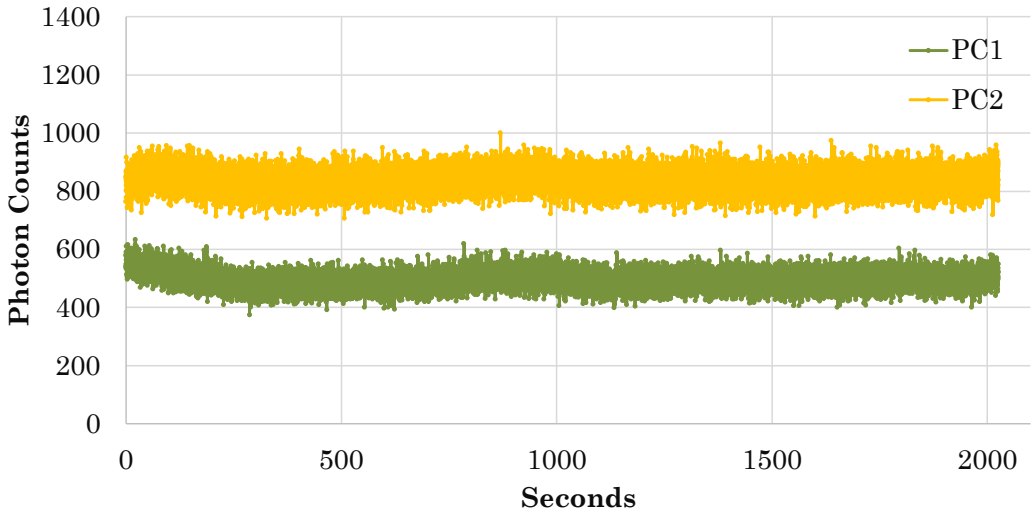


Figure 5-13- Phoenix EPC stability check

In order to use Phoenix EPC, its characteristics were extracted to be able to run the execution plan defined before. Firstly, how the H SOP as an input polarization to the EPC was converted to any other SOP on the Poincare Sphere was investigated. Then any other conversions (any input to any output SOP) can be extracted. An exhaustive scan on the EPC's settings was performed and conversions from H to any other SOP were extracted. Settings consisted of three numbers (Voltages). The EPC applied the desired SOP rotation by three wave plates. Each wave plate got voltages between 0V to 10V. Some examples of SOP conversions from H (in red) to different SOPs are depicted in Figure 5-14. The Poincare sphere is shown with the Stoke axis on the bottom left. Different regions in colors were accessible by EPC settings shown in their label. Areas of the regions are not similar as all voltages were not possible to be applied in the exhaustive scan of the settings. So, the larger the area, the less settings close to that region were scanned.

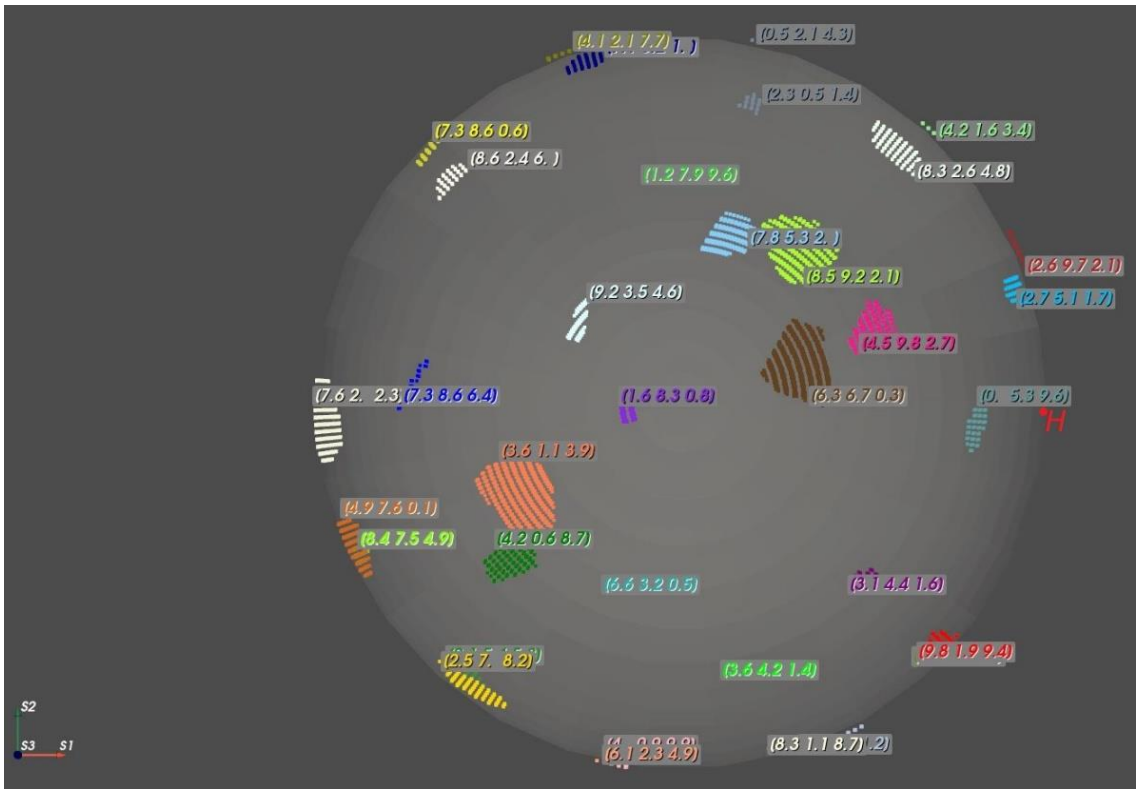


Figure 5-14- Some examples of Phoenix EPC capability to convert H input SOP to SOPs in regions depicted on Poincare Sphere

Having known settings of the EPC for all SOP conversions (stored in a dataset), all EPC's voltage settings needed for next experiments can be presented in Table 5-1.

If a polarimeter was available, the internal characteristics of the EPC such as wave plates' retardation could have been extracted and there was no need to store settings in a dataset.

Experimental Results:

A desired SOP rotation from H to (S1=0.7, S2=0.7, S3=0) was applied by Phoenix EPC. Then, QTx sent four buckets of photons as defined in the execution plan. The results acquired in each case are the following:

- H: 806 photons in PC1, 165 photons in PC2.
- V: 174 photons in PC1, 1025 photons in PC2.
- Diagonal: 271 photons in PC1, 1095 photons in PC2.
- A: 940 photons in PC1, 174 photons in PC2.

Considering the Dark Photon Counts as: PC1 counts 20 photons and PC2 counts 29 photons, the corrected results after dark count subtraction were computed.

- H: 806 – 20: **786** in PC1 & 165 – 29: **136** in PC2
- V: 174 – 20: **154** in PC1 & 1025 – 29: **986** in PC2

- D: 271 – 20: **251** in PC1 & 1095 – 29: **1066** in PC2
- A: 940 – 20: **920** in PC1 & 174 – 29: **145** in PC2

Table 5-1- Essential EPC's voltage settings for next experiments

SOP conversions	Voltage on WP1	Voltage on WP2	Voltage on WP3
H to (S1:0.7, S2:0.7, S3:0)	4.26	4.86	0.09
x-axis measurement	5.26	1.53	0.43
y-axis measurement	9.23	5.6	3.15
z-axis measurement	3.6	5.87	3.39
H to H	7.1	0.52	3.34
V to H	8.04	9.84	6.02
D to H	2.48	9.62	7.75
A to H	0.82	3.38	4.97
RC to H	3.72	5.44	4.44
LC to H	5.32	1.58	4.78

Conclusion:

Although the results are not as precise as expected, they confirm the approximate SOP conversion by the EPC. If a polarimeter could be used, the EPC settings could have been more precisely set. The EPC characteristics (including how it works and offsets before and after it) are extracted by only counted photons in PCs.

5.3.3 Final experimental tests

In this section, the final experimental results are shown. Specifically, the novel SOP distortion compensation method, which is a key part of the proposed QKD method in chapter 4, has been validated. For the ease of understanding, the complete

description and plan of each of them is provided before showing the actual implementation and experimental results.

5.3.3.1 Stabilized photon proportions

As discussed earlier, the SOP estimation function needs three axis measurements to identify the SOP of receiving photons. But the number of photons that are adequate for a precise estimation needs to be studied. To address this question, an experiment was defined to see when the measurements can be counted on.

Description:

As we can see in Figure 5-15, QTx sends buckets of photons with some specific SOP and QRx splits them to PCs to be counted. Number of photons in each bucket increases from ten to 30000 with 10 photon increments.

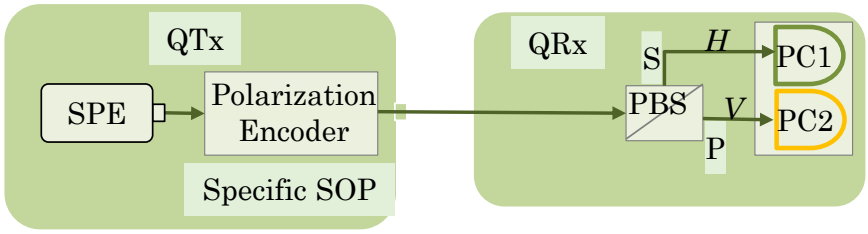


Figure 5-15- Configuration for the final experiment

Expected results:

The photon counts' proportion should be plotted in terms of the number of photons.

Experimental results:

As we can see in Figure 5-16, photon counts' proportion was relatively stable with 10000 counted photons, and as a result 10,000 photons are adequate for each qBER estimation in SOP measurement.

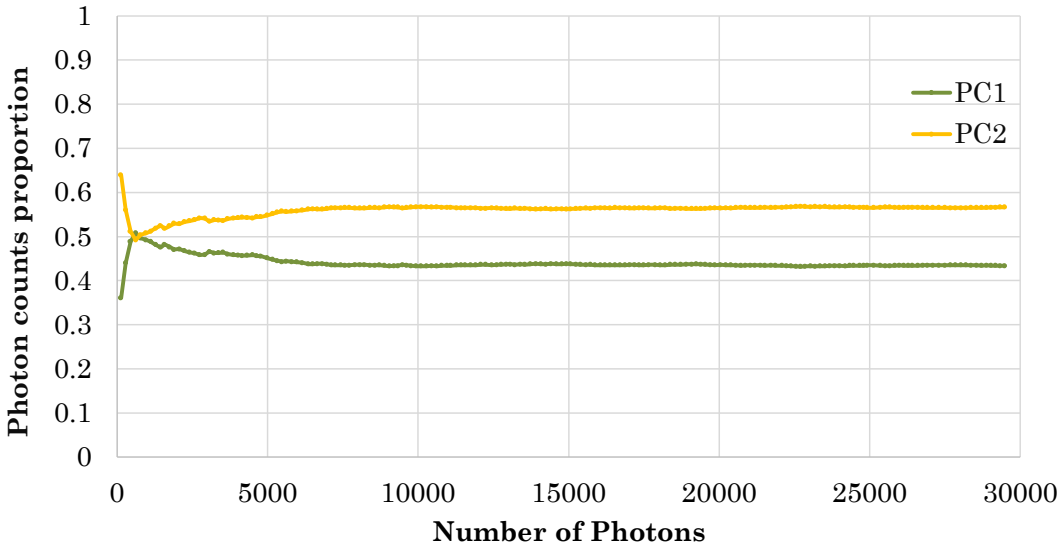


Figure 5-16- Stability check for photon counts proportion

5.3.3.2 Verifying the SOP distortion compensation

This key and final experiment verifies the SOP detection and compensation method in proposed QKD system in chapter 4, and it contains all components that are verified before.

Description:

QTx sends predefined distorted photons in buckets. The QRx firstly estimates the distortion using the SOP estimation function and secondly compensates for the distortion.

Plan:

To ensure that any polarization distortion compensation is possible, QTx encodes the SOP of emitted photons in six SOPs on the sphere (H-V-A-D-RC-LC) (Figure 5-17). Then, these polarized photons passing the quantum channel (fiber) are received by the EPC. The EPC should be tuned in a way that all three axis measurements are taken. After the measurements, the polarization distortion (input SOP in QTx) is recognized by the SOP estimation function (Figure 5-17). The mapping function maps SOP rotations to EPC settings (voltages) using the dataset mentioned in the EPC verification experiment. Next, EPC applies the compensation to the photons in transition. Finally, appropriate photon counts' proportion should be seen in PCs which means the algorithm can perfectly compensate for the distortions.

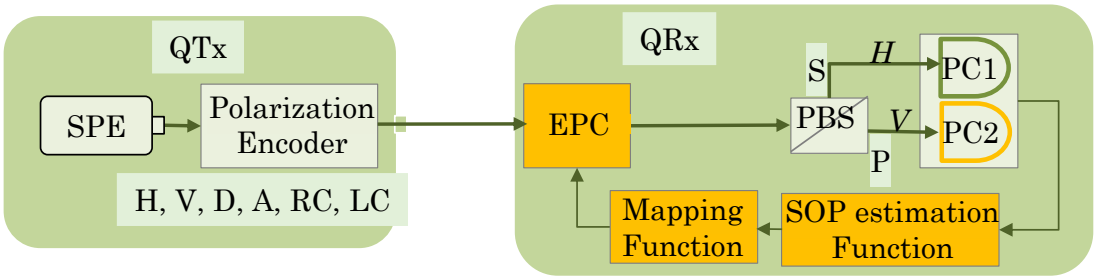


Figure 5-17- Configuration for the final experiment

Execution plan:

The experiment is run for every input polarization (six input SOPs). QTx sends photons with a specific input SOP (one of H, V, D, A, RC, LC) for 50 seconds. Each second contains 10 buckets of 1000 photons. As QRx needs more than 10000 photons to be capable of a stable measurement for each axis, five seconds (50000 photons) are devoted to each measurement. Overall, QRx receives the buckets and behaves as the following:

Phase 1: EPC voltages (0, 0, 0) for 15 seconds.

Phase 2: Three axis measurements for 15 seconds. Each five second. (EPC settings have mentioned before in the table)

Phase 3: Required EPC settings for SOP compensation (convert to **H**) are chosen and applied for 20 seconds.

All photon counts in PC1 and PC2 should be plotted in seconds for six different experiments.

Expected Results:

In all six experiments, photons should be counted 100% in PC1 and 0% in PC2 in 30 to 50 seconds time period which means all photons have H SOP after the compensation.

Execution details:

In all the experimental results, undesirable SOP changes (offsets) were observed before and after the EPC. To be more precise, from 0 to 15 seconds, photon counts proportion in PC1 and PC2 were not aligned with predefined input SOP in QTx. This was not due to the fiber between QTx and QRx but the offsets before and after the EPC. For instance, when QTx sent buckets of horizontally polarized photons (first experiment), the same photon counts' proportion should have been observed in 0 to 15 seconds and 30 to 50 seconds time periods. But as we can see in Figure 5-18, they were different and the reason was the aforementioned offsets. The EPC's settings related to three axis measurements considering these offsets were recognized.

Experimental Results:

For each input SOP in QTx, photon counts are depicted.

1- Horizontal:

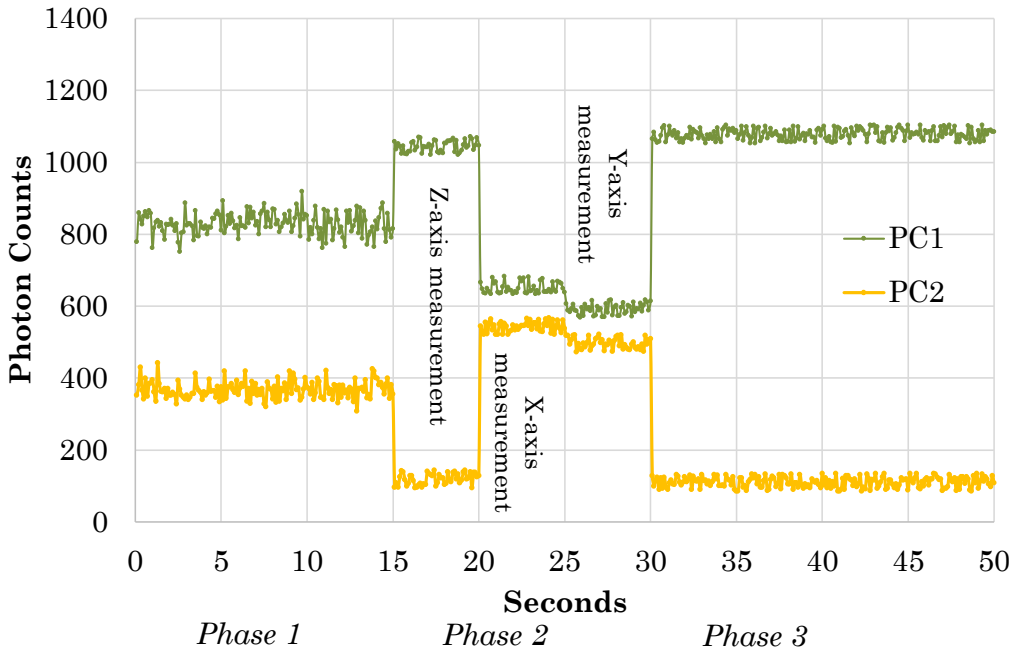


Figure 5-18- Photons counted in PC1 and PC2 in different phases

As we can see in the Figure 5-18, counted photons in PC1 between 15 to 20 seconds which represents z-axis measurement were 1047 photons on average for each bucket. Also, counted photons in PC2 for z-axis measurement were 120 photons. Moreover, photon counts' values for other axis measurements in average for each bucket were the following:

- PC1 for x-axis measurement: **660** and PC2: **543**
- PC1 for y-axis measurement: **560** and PC2: **496**

After the measurements using the SOP estimation function and considering the Dark Photon Counts as: PC1 counts 20 photons and PC2 counts 29 photons, the SOP estimation of the receiving photons became possible. The SOP was computed as:

- $qBER_{z\text{-measurement}} = (PC2 - PC2_{dark\text{-}count}) / (PC1 - PC1_{dark\text{-}count}) + (PC2 - PC2_{dark\text{-}count}) =$ **0.08**
- $qBER_{x\text{-measurement}} = (PC2 - PC2_{dark\text{-}count}) / (PC1 - PC1_{dark\text{-}count}) + (PC2 - PC2_{dark\text{-}count}) =$ **0.55**
- $qBER_{y\text{-measurement}} = (PC2 - PC2_{dark\text{-}count}) / (PC1 - PC1_{dark\text{-}count}) + (PC2 - PC2_{dark\text{-}count}) =$ **0.48**

- S1 = 1-2*$qBER_{z\text{-}measurement}$ = **0.84**
- S2 = 1-2*$qBER_{x\text{-}measurement}$ = **-0.1**
- S3 = 1-2*$qBER_{y\text{-}measurement}$ = **0.04**

As we can see, the input SOP (H) in the QTx was approximately identified. Next, the required rotation to convert H to H (compensation) was applied by the EPC. So, as we see in Figure 5-18, most of the photons were counted in PC1 between 30 to 50 seconds which means the SOP was H during this time period as expected. In the following we can see the results regarding the other input polarization in QTx.

2- Vertical:

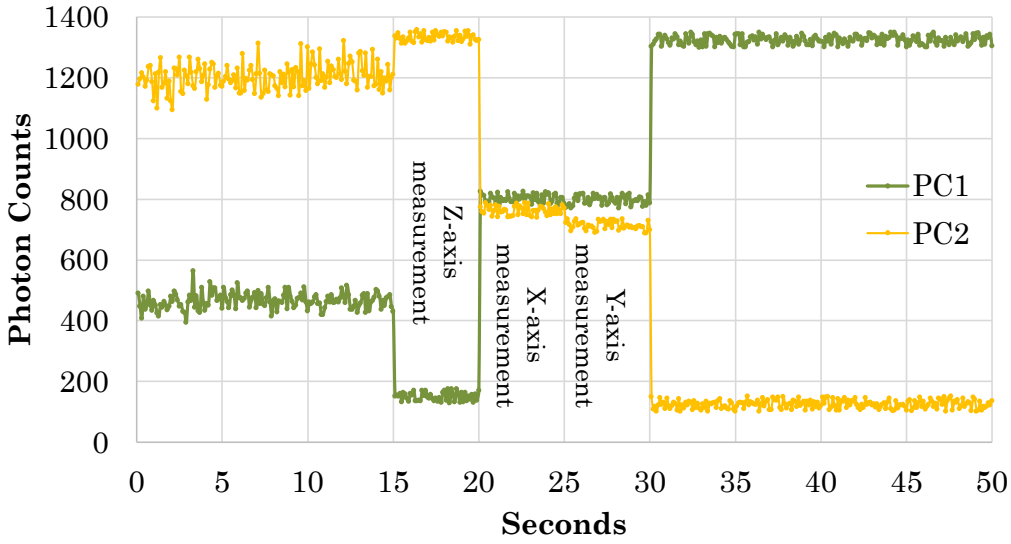


Figure 5-19- Photons counted in PC1 and PC2 in different phases

As we can see in Figure 5-19, counted photons were the following:

- PC1 for z-axis measurement: **153** and PC2: **1337** (from 15 to 20 seconds)
- PC1 for x-axis measurement: **800** and PC2: **765** (from 20 to 25 seconds)
- PC1 for x-axis measurement: **798** and PC2: **720** (from 25 to 30 seconds)

After the measurements using the SOP estimation function and considering the Dark Photon Counts as: PC1 counts 20 photons and PC2 counts 29 photons, the SOP estimation of receiving photons became possible. The SOP was computed as:

- $qBER_{z\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.9**
- $qBER_{x\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.51**
- $qBER_{y\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.52**

- S1 = 1-2*$qBER_{z\text{-}measurement}$ = **-0.8**
- S2 = 1-2*$qBER_{x\text{-}measurement}$ = **-0.02**
- S3 = 1-2*$qBER_{y\text{-}measurement}$ = **-0.04**

As we can see the input SOP (V) was approximately identified in the QTx. Next, the required rotation to convert V to H (compensation) was applied by the EPC. So, as you can see in Figure 5-19, most of the photons were counted in PC1 between 30 to 50 seconds which means the SOP was H during this time period as expected.

3- Diagonal:

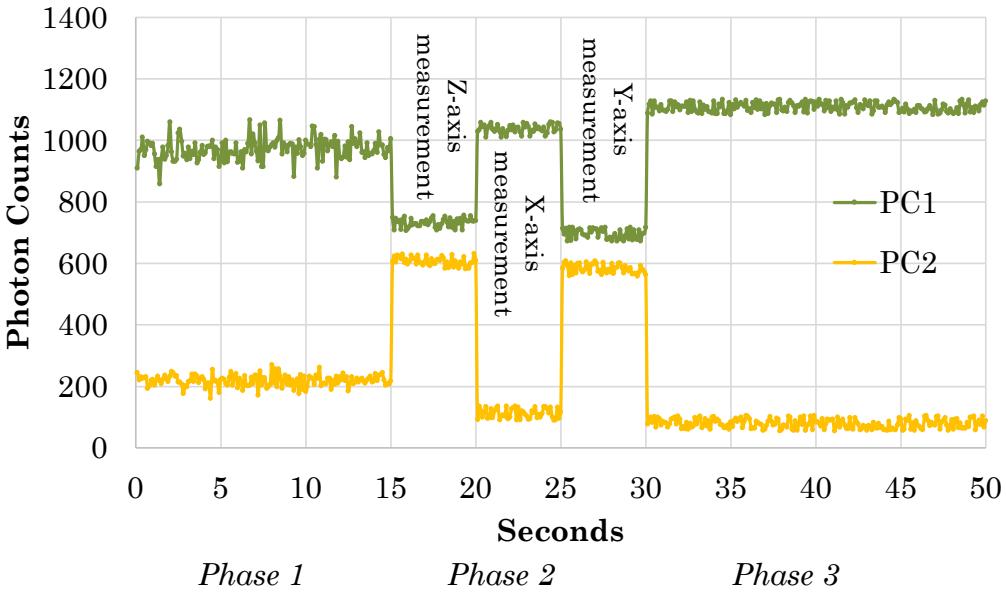


Figure 5-20- Photons counted in PC1 and PC2 in different phases

As we can see in Figure 5-20, counted photons were the following:

- PC1 for z-axis measurement: **727** and PC2: **604** (from 15 to 20 seconds)
- PC1 for x-axis measurement: **1036** and PC2: **113** (from 20 to 25 seconds)
- PC1 for x-axis measurement: **696** and PC2: **583** (from 25 to 30 seconds)

After the measurements using the SOP estimation function and considering the Dark Photon Counts as: PC1 counts 20 photons and PC2 counts 29 photons, the SOP estimation of receiving photons was computed as:

- $qBER_{z\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.45**
- $qBER_{x\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.07**
- $qBER_{y\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.45**

- S1 = 1-2*$qBER_{z\text{-}measurement}$ = **0.1**
- S2 = 1-2*$qBER_{x\text{-}measurement}$ = **0.86**
- S3 = 1-2*$qBER_{y\text{-}measurement}$ = **0.1**

As we can see, the input SOP (D) in the QTx was approximately identified. Next, the required rotation to convert D to H (compensation) was applied by the EPC. So, as you can see in Figure 5-20, most of the photons were counted in PC1 between 30 to 50 seconds which means the SOP was H during this time period as expected.

4- Anti-diagonal:

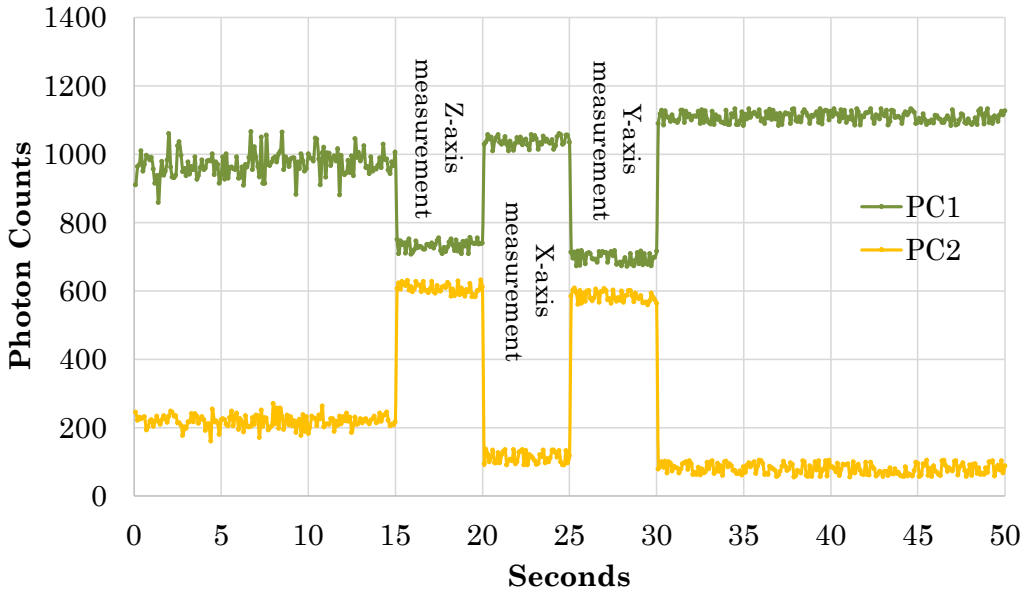


Figure 5-21- Photons counted in PC1 and PC2 in different phases

As we can see in the Figure 5-21, counted photons were the following:

- PC1 for z-axis measurement: **625** and PC2: **694** (from 15 to 20 seconds)
- PC1 for x-axis measurement: **91** and PC2: **1228** (from 20 to 25 seconds)
- PC1 for x-axis measurement: **634** and PC2: **496** (from 25 to 30 seconds)

After the measurements using the SOP estimation function and considering the Dark Photon Counts as: PC1 counts 20 photons and PC2 counts 29 photons, the SOP of receiving photons was computed as:

- $qBER_{z\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.52**
- $qBER_{x\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.94**
- $qBER_{y\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.42**

- S1 = 1-2*$qBER_{z\text{-}measurement}$ = **-0.04**
- S2 = 1-2*$qBER_{x\text{-}measurement}$ = **-0.88**
- S3 = 1-2*$qBER_{y\text{-}measurement}$ = **0.16**

As we can see, the input SOP (A) in the QTx was approximately identified. Next, the required rotation to convert A to H (compensation) was applied by the EPC. So, as you can see in Figure 5-21, most of the photons were counted in PC1 between 30 to 50 seconds, which means the SOP was H during this time period as expected.

5- Right-handed Circular:

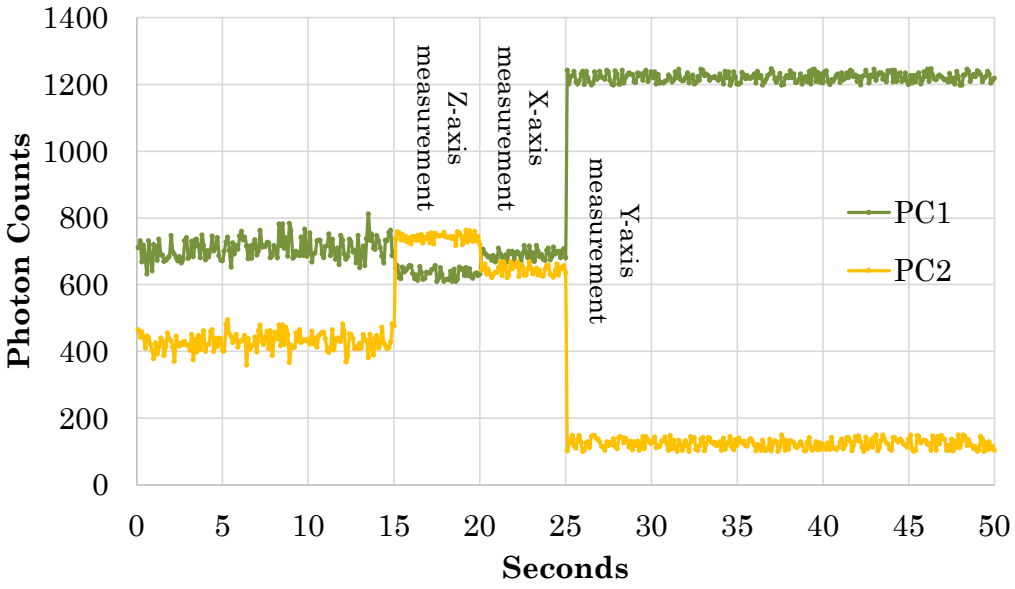


Figure 5-22- Photons counted in PC1 and PC2 in different phases

As we can see in Figure 5-22, counted photons are:

- PC1 for z-axis measurement: **629** and PC2: **737** (from 15 to 20 seconds)
- PC1 for x-axis measurement: **687** and PC2: **640** (from 20 to 25 seconds)
- PC1 for x-axis measurement: **1217** and PC2: **120** (from 25 to 30 seconds)

After the measurements using the SOP estimation function and considering the Dark Photon Counts as: PC1 counts 20 photons and PC2 counts 29 photons, the SOP of receiving photons was computed as:

- $qBER_{z\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.53**
- $qBER_{x\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.47**
- $qBER_{y\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.07**

- S1 = 1-2*$qBER_{z\text{-}measurement}$ = **-0.06**
- S2 = 1-2*$qBER_{x\text{-}measurement}$ = **0.06**
- S3 = 1-2*$qBER_{y\text{-}measurement}$ = **0.86**

As we can see, the input SOP (RC) in the QTx was approximately identified. Next, the required rotation to convert RC to H (compensation) was applied by the EPC. So, as you can see in Figure 5-22, most of the photons were counted in PC1 between 30 to 50 seconds, which means the SOP was H during this time period as expected.

6- Left-handed Circular:

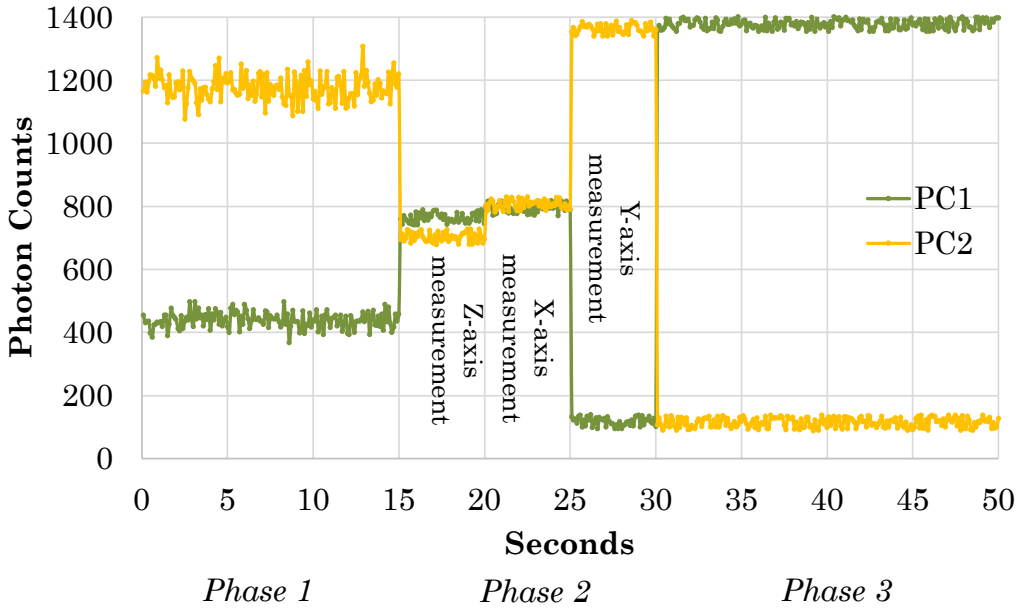


Figure 5-23- Photons counted in PC1 and PC2 in different phases

As we can see in Figure 5-23, counted photons were:

- PC1 for z-axis measurement: **760** and PC2: **698** (from 15 to 20 seconds)
- PC1 for x-axis measurement: **803** and PC2: **825** (from 20 to 25 seconds)
- PC1 for x-axis measurement: **110** and PC2: **1359** (from 25 to 30 seconds)

After the measurements using the SOP estimation function and considering the Dark Photon Counts as: PC1 counts 20 photons and PC2 counts 29 photons, the SOP of receiving photons was computed as:

- $qBER_{z\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.47**
- $qBER_{x\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.5**
- $qBER_{y\text{-}measurement}$ = (PC2 - $PC2_{dark\text{-}count}$) / (PC1 – $PC1_{dark\text{-}count}$) + (PC2 - $PC2_{dark\text{-}count}$) = **0.93**

- S1 = 1-2*$qBER_{z\text{-}measurement}$ = **0.06**
- S2 = 1-2*$qBER_{x\text{-}measurement}$ = **0**
- S3 = 1-2*$qBER_{y\text{-}measurement}$ = **-0.86**

As we can see, the input SOP (LC) in the QTx was approximately identified. Next, the required rotation to convert LC to H (compensation) was applied by the EPC. So, as you can see in Figure 5-23, most of the photons were counted in PC1 between 30 to 50 seconds, which means the SOP was H during this time period as expected.

Conclusion:

We can conclude that the novel approach can compensate for not only the intentional distortion in QTx (which represents a distortion happening in the fiber in real scenarios) but also offsets around the EPC. Therefore, the obtained results support the novel SOP distortion compensation method in true polarization encoded QKD, and enable the proposed AI aided QKD system in chapter 4.

5.4 Conclusion

The main point of this chapter was to showcase how QKD performs in difficult and practical situations. For example, the chapter examined the use of QKD in aerial cables, which can be impacted by weather conditions such as strong winds that can damage the optical fibers. This can lead to higher qBER and a decrease in the effective KER, sometimes dropping from Mb/s to Kb/s or even b/s.

In addition, the purpose of the chapter was to validate the performance of QKD in real-world scenarios such as aerial cables, through the implementation of experiments. These experiments aimed to ensure that QKD can maintain its high level of performance even when deployed in challenging environments like aerial cables.

Performed experiments show how delicate the testbed and equipment are. It illustrates the gap between theoretical simulation and experimental setup used for implementing QKD protocols. This observation motivates the need to consider every imperfection in experimental setups and opens up the opportunity to use digital twins proposed in the next chapter, e.g., based on simulation models, to be able to compensate for the imperfections and distortions and as a result to increase the key exchange rate in challenging environments where QKD protocols have been implemented. Moreover, using aforementioned techniques and models, we will be capable of faster and more safe eavesdropping detection procedures.

Chapter 6

DARIUS: A Digital Twin to Improve the Performance of Quantum Key Distribution

In this chapter we take advantage of DT called DARIUS to help QRx with eavesdropping detection as well as finer compensation of SOP distortion in the channel w.r.t the compensation described in the previous chapter.

Despite QKD's theoretical excellence based on quantum physics, commercial optical devices supporting QKD systems lack precision, which highly limits the final KER of the system. Beside optical component imperfections, eavesdropping and unpredicted environmental events occurred in the quantum channel increase qBER, which leads to further KER reduction. In this chapter, we propose DARIUS, a DT for polarization encoded QKD systems that bridges the gap between perfect theoretical QKD systems and real implementations to: *i*) address optical components' non-ideal behavior; *ii*) discern eavesdropping from high qBER; and *iii*) dynamically compensate for environmental events. Taking advantage of the DARIUS, even moderate eavesdropping rates can be distinguished from qBER. Moreover, significant improvement in proactive environmental event compensation is achieved, as DARIUS can derive proper optical component tuning.

6.1 Introduction

QKD is opening a new era for secure communications since it enables the distribution of unlimited secret keys between two distant parties [Ma17].

Nonetheless, because of the very low power of the optical signal, QKD requires devices with high-precision, which increases their cost and limits the deployment of QKD systems. In polarization-encoded QKD, the BB84 protocol proposed in [Be84] defines a QTx mapping randomly and privately selected pairs <bit, basis> (*qubit*) onto one linear SOP, namely, H, V, D and A. Then, the QTx emits a single photon polarized in the direction of the selected SOP, which is propagated through the fiber channel and received by a QRx. The QRx randomly and privately selects a binary basis and measures the received photon according to this basis. If both QTx and QRx have chosen the same basis, the binary measurement of the photon in the QRx matches the bit sent by the QTx. With this method, both parties can privately share keys with those bits that matched the bases.

Key exchange includes *key distillation*, where modules running beside the QTx and QRx exchange a percentage of bits (10% as defined in [Di17]), so the module in the receiver can estimate the qBER of the transmitted key. Keys with qBER higher than a defined threshold are discarded as they are assumed to be tampered by an eavesdropper. Authors in [Le22], proposed a high accurate method to detect eavesdropping in polarization-encoded QKD systems, where resultant qBER of keys tampered by an eavesdropper is compared to that of untapped keys. However, since QTx needs to send photons with predefined bases, key distribution has to be paused whenever the detection is required, which noticeably reduces KER of the QKD system. Authors in [Ca22] proposed a slight modification of the polarization-encoded QKD protocol to permit the detection of eavesdropping activities by calculating the randomness of the bit sequence at the QRx after the key sifting procedure, where QTx and QRx discard bits with mismatched bases. The modification entails changing the randomness of the bit and basis selection in the QTx, which would also decrease final KER of the system.

However, many events during photon transmission through the channel can impact the measurements in the QRx, which would result into bases mismatches [Pi15]. Specifically, polarization-encoded QKD can be degraded by SOP distortion induced by the long fiber between QTx and QRx, as well as by environmental events occurred in the quantum channel. SOP distortions can be compensated using feedback-based compensation methods available in the literature [Ra20], where monitoring (*Mo*) intervals are considered. During a Mo interval, photons with predefined H SOP are generated and the Stokes parameters (<S_0, S_1, S_2, S_3>) representing the SOP of received photons are measured in the QRx. Authors in [Ra22] added D SOP to be sent during Mo interval to compensate for qBER in both Rectangular (R) and D bases. In the last chapter, we proposed an improved compensation method based on DNN that was able to predict the near future SOP based on the values measured during the last Mo intervals. However, that method assumed ideal conditions with perfectly calibrated optical components and thus, its performance might reduce in real deployments where optical components introduce unexpected photon loss, undesired polarization effects, and other non-ideal behaviors.

DT can be helpful to improve QKD systems performance. In communications systems, DT have been proposed for fault management, as they can take advantage of data, models, and algorithms [Wa21], [Se23]. In [Ah22-1], we presented a preliminary design of a DT for polarization-encoded QKD systems, aiming at improving KER under environmental events. In this chapter, we go beyond and propose DARIUS, a novel DT for polarization-encoded QKD systems. DARIUS includes methods to: *i*) discern eavesdropping from fiber stressing events without changing the randomness of <bit, basis> selection nor produce further key exchange interruption. The eavesdropping detection takes advantage of Mo intervals to monitor discrepancies in SOP, qBER, and KER between Mo and key exchange (Ke) intervals; and *ii*) help a DNN-powered compensation method to take counter actions against higher velocity events on the fiber.

The rest of the chapter is organized as follows. Section 6.2 presents the components in the quantum channel (qCh) and DARIUS use cases. Section 6.3 describes DARIUS's components. Then, proposed solutions for eavesdropping detection and higher velocity event compensator based on the information coming from key distillation are detailed. discussion is supported by the results in Section 6.4. Finally, Section 6.5 draws the main conclusion of the work.

6.2 QKD and DARIUS's Opportunities

In this section, we first present specifications of qCh components including functionalities and imperfections. Next, opportunities in which DARIUS can take advantage to improve the QKD systems are presented, and three DARIUS's use cases are eventually introduced.

6.2.1 QKD system and qCh components

We assume the qCh components presented in Figure 6-1 (bottom), with a QTx and QRx connected thought a Single Mode Fiber (SMF). The QTx includes a SPE and a Wave Plate that changes photons' SOP as a function of the qubit to be transmitted. The SMF connecting QTx to QRx impacts the SOP and introduces photon loss and variable SOP impact is produced when the fiber is affected by environmental conditions. In the QRx, a balanced BS separates the photons and acts as the random basis selection between R and D basis for the QKD system.

Note that the BS can introduce photon loss through its arms [Ba98]. Then, two EPCs for each basis change the SOP with either tunable retardation or tunable orientation of its wave plates (internal characteristics of commercially available EPCs are not precisely specified by the manufacturers) [Zh18]. These changes are used to compensate for SOP distortion through the fiber. A PBS separates the photons based on their SOP and acts as bit selector. One arm (*reflection*) passes H polarized photons

while the other (*transmission*) passes V polarized ones. The PBS also introduces photon loss through its arms. A wave plate between the EPC and PBS in the D basis is used to measure photons with D or A SOP. Next, a module with four SPDs counts photons. SPDs record more photons than the ones actually hitting them; the additional portion is known as *dark count rate*.

6.2.2 Opportunities and use cases for DARIUS

The architecture of DARIUS is presented in Figure 6-1 (top), where each block models a counterpart optical component in the qCh. Then, the DT of the QKD system is defined as a concatenation of the digital qCh component models. DARIUS takes advantage of two repositories in the AI-based SOP compensator storing SOP measurements during Mo and Ke intervals (SOP_{Mo}*_Repo* and SOP_{Ke}*_Repo*).

As in [Ah22], Mo intervals are assumed to track SOP trajectory in case of fiber stressing events. Figure 6-2 shows how keys exchange is interrupted and the QTx sends polarized photons during T_O, which the QRx can measure and tune its EPCs during T_R if needed. However, in addition to the proposed H SOP sent during Mo periods, the QTx needs to send D SOP to detect those SOP distortions aligned to the propagation direction of the transmitted photons. Note that any possible SOP evolution can be tracked by sending both H and D polarized photons. SOP trajectories starting from H and D are different but related by the universal rotation matrix [Si17], where a unique SOP distortion acts as a universal rotation matrix that converts H and D SOPs to SOPs with $S_{1(H)}$=1-2$qBER_R$ and $S_{2(D)}$=1-2$qBER_D$, respectively.

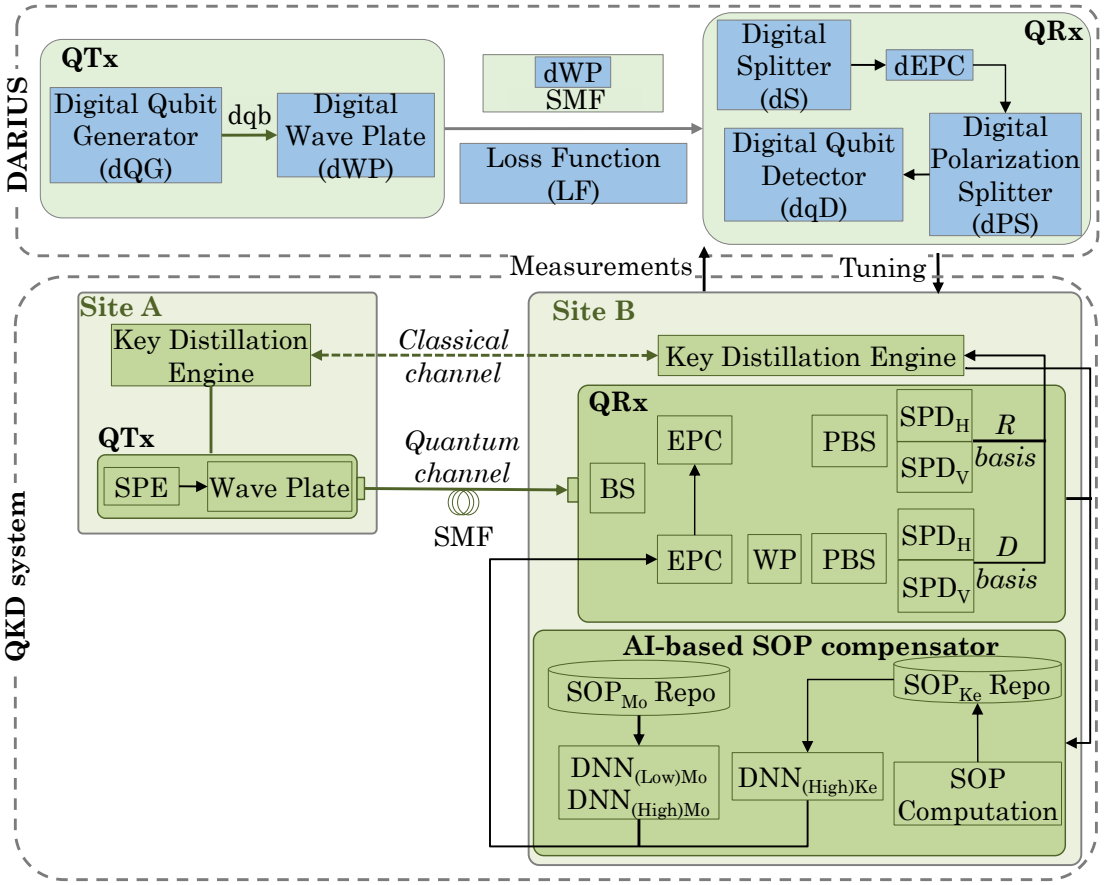


Figure 6-1- DARIUS and the QKD system equipped with AI-based SOP compensator.

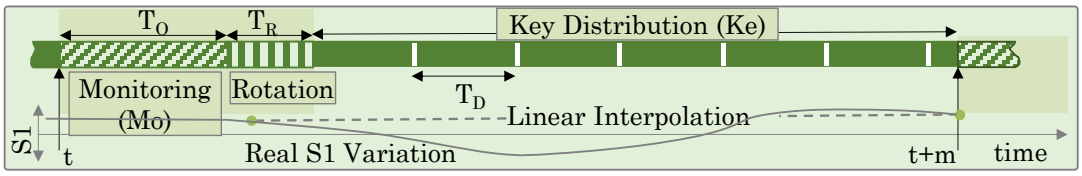


Figure 6-2- Proposed Interpolation method for high velocity events.

Mo intervals reduce KER of the QKD system and therefore, true Stokes measurements cannot be performed very frequently, which makes QKD systems especially vulnerable against episodes of large SOP variation which leads to large qBER and eavesdropping become indistinguishable. Nonetheless, the distillation process can provide useful information of the Stokes parameters, derived from the qBER estimation of the sifted keys. Particularly, the actual value of $S_{1(H)}$ and $S_{2(D)}$, as well as the absolute value of $S_{2(H)}$, $S_{3(H)}$, $S_{1(D)}$, and $S_{3(D)}$ can be obtained from the qBER estimations during the key distillation process, without the need of real monitoring. In this regard, large keys would produce more precise qBER estimations at the expense of increasing the time to obtain them. Hence, the length of the keys needs to be studied.

Apart from the length of the keys, the distance between QTx and QRx plays a major role in the time of SOP estimation during Ke intervals. For illustrative purposes, Figure 6-3 shows the workflow of the key exchange process. At the qCh, QTx (Alice) randomly generates bases and bits to prepare the polarized photons for emission (labeled 1 in Figure 6-3), whereas the bases will be used for key distillation. Once photons are received (2) and measured by QRx (Bob), bits are extracted based on their randomly generated bases (3). Xs are used for extracted bits with mismatched bases in Figure 6-3. Next, Bob sends the bases to Alice for raw key reconciliation (4), so Alice is able to detect bits with matched bases (5). Now, Alice sends some randomly chosen bits with matched bases to Bob (6) for qBER estimation (7). Therefore, two-way transmission is needed for the qBER estimation and the distance between QTx and QRx should be studied.

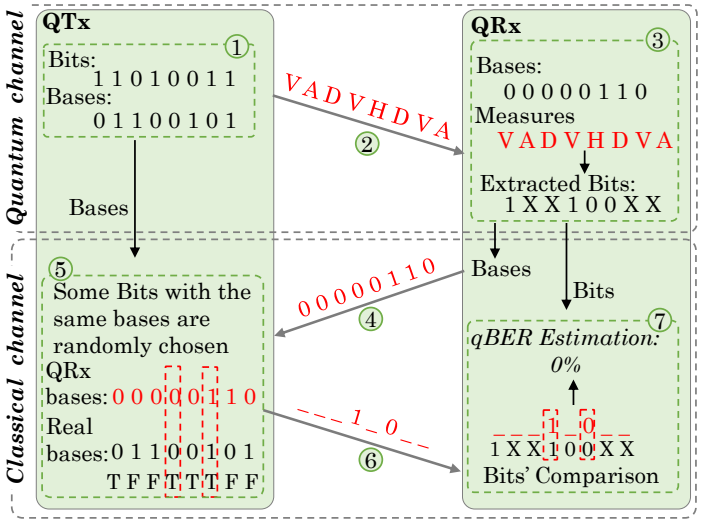


Figure 6-3- QBER estimation in the QRx based on the BB84 protocol

Several use cases can be defined that take advantage of DARIUS, e.g.: 1) DARIUS can optimize the QKD system by adjusting the tunable parameters of the optical components before starting key distribution. The tunable parameters in the qCh are related to the wave plate in the QTx, as well as the EPC and SPDs in QRx. Armed with measurements gathered from the qCh, DARIUS can provide the needed adjustments of the optical components to eventually increase KER; 2) DARIUS can distinguish between eavesdropping and excessive qBER, which will allow to continue with the key exchange in case of the latter. The SOP evolution is traceable when events caused by human operator works or environmental conditions affect the optical fiber. In contrast, eavesdropping results into unrecognizable SOP changes [Ah22]. Measurements taken from SOP trajectory repositories both during Mo and Ke intervals help DARIUS to detect eavesdropping; and 3) DARIUS can configure the AI-based SOP compensator in the QRx to take proper countermeasure actions against environmental events.

Environmental events introduce fluctuations on the SOP of transmitted photons with differential velocity as discussed in [Ah22]. In this case, the DNN model under

operation in the SOP compensator ($DNN_{Low(Mo)}$) is not able to foresee the SOP of incoming photons. Therefore, another DNN model trained for higher velocity events ($DNN_{High(Mo)}$) is needed. DARIUS can detect the increased SOP velocity and change the model under operation, which would increase KER by SOP distortion compensation in different environmental conditions.

6.3 DARIUS Specification and Intelligence

In this section, we show how DARIUS improves the performance of the QKD system by discerning eavesdropping from high qBER, as well as taking actions against diverse environmental conditions. We first present the proposed components, which provide a *digital* representation of qCh components. Next, the procedure to detect eavesdropping and differentiate it from high qBER is described. Finally, algorithms to dynamically address high qBER due to SOP fluctuation having different velocity are presented. Table 6-1 summarizes the notation that is consistently used along the rest of the chapter.

6.3.1 qCh Models

This section presents models to create a digital representation of the qCh components [Ah22-1]: *i*) the digital Qubit Generator (dQG) and the digital wave plate (dWP) modeling the physical SPE and the wave plate; *ii*) the SMF model; and *iii*) digital components for the QRx, i.e., digital splitter (dS), digital EPC (dEPC), digital polarization splitter (dPS) and digital qubit detector (dqD).

The dQG generates digital qubits (dqb) modeling their quantum states as eq. (2), where α is the phase with respect to orthogonal electric field (x,y) components polarized with orientation angle θ [Ja98]. Here, the quantum state perfectly matches the SOP of emitted photons.

$$|\psi_{dq}\rangle = \begin{pmatrix} \cos(\theta) \times e^{i\alpha_x} \\ \sin(\theta) \times e^{i\alpha_y} \end{pmatrix} \quad (2)$$

The dWP acts as a quantum gate and it affects the generated dqb in the same way that an optical wave plate changes the SOP of a photon. Eq. (3) models the quantum gate with orientation angle θ and phase retardation φ of the wave plate [Al21].

$$dWP_{\theta}(\varphi) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad (3)$$

$$a = e^{i\varphi/2}cos^2(\theta) + e^{-i\varphi/2}sin^2(\theta) \quad (4)$$

$$b = \ c = -isin(2\theta) \times sin(\varphi/2) \quad (5)$$

$$d = e^{-i\varphi/2}cos^2(\theta) + e^{i\varphi/2}sin^2(\theta) \quad (6)$$

Table 6-1: Notation

α_x	Phase difference w.r.t horizontal electric field (rad)
α_y	Phase difference w.r.t vertical electric field (rad)
θ	Orientation angle (rad)
$\|\psi_{DQ}\rangle$	Quantum state of Digital qubit
φ	Phase retardation (rad)
dq_Tx	Digital qubit transmission
dR	Digital reflection
dT	Digital transmission
$Loss_{op\_comp}$	Optical component loss (%)
$qBER_{(.)}$	qBER in: Mo/Ke interval or R/D bases (%)
m	Time between two consecutive monitoring intervals (s)
T_O	Time needed to measure SOP in Mo intervals (s)
T_R	Time needed to perform rotation in QRx (s)
T_D	Time between two SOP measurement in Ke intervals (s)
T_{tr}	Transmission time between QTx and QRx (s)
T_{comp}	Computation time for SOP estimation (s)

Table 6-2: QDT models and their tunable parameters

qCh Model	Purpose	Tunable Parameters
dQG	state initialization	θ, αx, αy
dWP	state adaptation	SOP distortion of emitted photons
SMF	Apply fiber impacts (distortion, optical loss) on the state	Fiber length and SOP distortion
LF	Apply optical components' loss	$Loss_{op\_comp}$
DS	Reflect or transmit the qubit (50%, 50%)	photon loss in each arm
PBS	Reflect or transmit the qubit based on the state	photon loss in each arm
dEPC	Apply EPC's impact to the state	Wave plates variables
dqD	Store qubit's probability in a repository	Dark count rate

$$P(dq\_Tx) = 1 - Loss_{op\_comp} \quad (7)$$

$$dEPC = dWP_{\theta_1}(\pi/2) \cdot dWP_{\theta_2}(\pi) \cdot dWP_{\theta_3}(\pi/2) \quad (8)$$

The SMF is modeled by using a dWP, which changes the SOP in the same way that birefringence in the fiber affects the photons. In addition, a loss function (LF) discards dqbs with a probability inversely proportional to the loss rate of optical components (eq.(7)).

In the digital QRx, a digital splitter (dS) receives dqbs and randomly outputs them through the digital reflection (dR) or digital transmission (dT) with equal probability.

The dEPC is modeled as three dWPs, where the orientation angles (θ_1, θ_2, θ_3) are derived from the input and output SOP [Mu06]. Eq. (8) computes the required quantum gates for a fixed-retardation EPC using the matrix multiplication of the dWPs.

Next, the digital polarization splitter (dPS) receives dqbs and outputs them through the dR or dT based on its quantum state (eq. (9)-(10)). Finally, the dqD receives P(dR) and P(dT) and adds dark counts based on physical dark count rates.

$$P(\mathrm{dR}) = P(H) = cos^2(\theta) \quad (9)$$

$$P(\mathrm{dT}) = P(V) = sin^2(\theta) \quad (10)$$

Table 6-2 summarizes the purpose of the qCh models and their tunable parameters.

6.3.2 Eavesdropping detection and Excessive qBER compensation

DARIUS collects measurements from the qCh and determines whether it stops the key distribution if eavesdropping is detected or continues the key distribution with fine SOP monitoring. DARIUS assumes two scenarios for eavesdropping: *i*) the eavesdropper has no knowledge about Mo intervals or he/she cannot perfectly synchronize with them (*scenario 1*), so any tampering would result in S_0 values noticeably lower than 1; and *ii*) the eavesdropper has detected Mo intervals and he/she can insert photons with the right polarization during Mo periods (*scenario 2*). In this case, discrepancies in $qBER_{Mo}$ and $qBER_{Ke}$ values will reveal eavesdropping.

Let us first analyze the effect of eavesdropping in scenario 1. In a QKD system, eavesdropping consists in taking photons, measuring them, and injecting new photons in the channel using extracted bits from its measurements. For the sake of simplicity, in this chapter, we also consider that tampering is performed at a location close to the QTx in site A, which theoretically is the best place for eavesdropping since the remaining optical fiber until the QRx could mask the attack. Because at photon transmission time only the QTx knows the true basis used to polarize a photon, the eavesdropper has to choose its own basis, e.g., randomly. Such decisions impact on the value of S_0, which takes values not that close to 1. Note that during Mo intervals, $S_{1(H)}$ and $S_{2(D)}$ are related to *qBER* in R and D bases when input SOPs

are H and D, respectively. S_0 can be computed as eq. (11), which should be equal to one, whereas qBER during Mo period ($qBER_{Mo}$) can be computed as eq. (12)[Ra20].

$$S_0 = \sqrt{S_1^2 + S_2^2 + S_3^2} \tag{11}$$

$$qBER_{\mathrm{Mo}} = \frac{1}{2} \times \left(\frac{1 - S_{1(\mathrm{H})}}{2} + \frac{1 - S_{2(\mathrm{D})}}{2} \right) \tag{12}$$

In scenario 2, differences between $S_{1(H)}$, $S_{2(D)}$, qBER and KER measured and estimated during Mo and Ke periods, allow eavesdropping being distinguishable from high qBER. During the Ke period, $qBER_{Ke}$ can be computed by averaging the partial ones from R and D bases, denoted $qBER_R$ and $qBER_D$ (eq. (13)), while $qBER_{(R/D)}$ can be obtained from counted photons in the SPDs (eq. (14)).

$$qBER_{\mathrm{Ke}} = \frac{1}{2} \times (qBER_{\mathrm{R}} + qBER_{\mathrm{D}}) \tag{13}$$

$$qBER_{(\cdot)} = \frac{\#\text{photons SPD}_{\mathrm{V}(\cdot)}}{\#\text{photons SPD}_{\mathrm{V}(\cdot)} + \#\text{photonsSPD}_{\mathrm{H}(\cdot)}} \tag{14}$$

Let us now analyze why the method to compensate for fiber stressing events in [Ah22] is not able to reduce *qBER* under higher velocity events that produce large SOP variations. Figure 6-2 illustrates a possible S_1 evolution between two Mo intervals (continuous line in Figure 6-2) and the linear interpolation (dotted lines). Using the latter to plan the rotations between the two Mo intervals [t, t+m] would result in that such rotations would not only not improve the *qBER* but also highly reduce *KER* in case of large SOP variations. In contrast, our proposal for *qBER* compensation is based on using information from the key distillation process to estimate the evolution of SOP between two Mo intervals, which will be applied to compute a much more accurate rotation plan.

Assuming the QRx architecture in Figure 6-1, the QRx can use the Mo intervals history, as well as the estimation of $\mathrm{SOP_H}$ and $\mathrm{SOP_D}$ computed between Mo intervals in case of high velocity events, i.e., during Ke intervals, to improve the SOP compensation. Note that such estimation can be performed with a shorter period (T_D in Figure 6-2). Rotations computed using predictions from either low or high velocity DNN models and from Mo and Ke intervals are applied by the EPCs to compensate for the SOP distortion of the received photons before being counted by the H and V SPDs in the R and D bases. It is worth mentioning that different EPCs are being used in R and D bases in polarization-encoded QKD systems [Ta05], which entails applying different rotations to compensate for SOP distortion. DARIUS is the responsible for switching between low or high DNN models, in operation in the AI-based SOP compensator, once no eavesdropping evidence is observed. Switching decision is made by measuring the speed of $S_{1(H)}$ and $S_{2(D)}$ once qBER exceeds a threshold.

6.3.3 DARIUS intelligence

Let us now detail the different algorithms that provide intelligence to DARIUS. First, Algorithm 6-I is used to estimate SOP_{Ke}. This algorithm is used by other algorithms, as well as to update the repository every T_D ms. 10% of the last sifted key are used to estimate S_1, abs(S_2), and abs(S_3) for H input SOP and abs(S_1), S_2, and abs(S_3) for D input SOP [Ra22].

Algorithm 6-I. SOP_{Ke} estimation

INPUT: $qBER_R$, $qBER_D$
OUTPUT: SOP_{Ke}

1: $S_{1(H)} \leftarrow 1 - 2 \times qBER_R$
2: $S^+_{2(H)} \leftarrow \text{sqrt}(2 \times qBER_D \times (1+S_{1(H)}))$
3: $S^+_{3(H)} \leftarrow \text{sqrt}(1-(S_{1(H)})^2-(S^+_{2(H)})^2)$
4: $S^+_{1(D)} \leftarrow \text{sqrt}(2 \times qBER_D \times (1+S_{1(H)}))$
5: $S_{2(D)} \leftarrow 1 - 2 \times qBER_D$
6: $S^+_{3(D)} \leftarrow \text{sqrt}(1-(S_1{}^+{}_{(D)})^2-(S_{2(D)})^2)$
7: **return** [$<S_{1(H)}, S^+_{2(H)}, S^+_{3(H)}>$, $< S^+_{1(D)}, S_{2(D)}, S^+_{3(D)}>$]

DARIUS includes Algorithm 6-II for eavesdropping detection and SOP compensation, which is run every Mo interval. The algorithm takes as input a reference to SOP_{Mo}_Repo and SOP_{Ke}_Repo, the value of $qBER_{Mo}$ in the current Mo interval and avg_qBER_{Ke} averaging $qBER$ captured every T_D ms in the last Ke interval. SOP in the current Mo interval is retrieved from the Mo repository and used to compute S_0 (lines 1-2). The obtained value is used, together with $qBER_{Mo}$ and avg_qBER_{Ke}, to detect eavesdropping analyzing scenarios 1 and 2 defined in Section 6.3.2(lines 3-4). If no eavesdropping is detected but avg_qBER_{Ke} is over the threshold, the velocity of $S_{1(H)}$ is measured and compared to the velocity threshold (*velocity_thr*). If both thresholds are exceeded, high velocity DNN models, $DNN_{(high)Mo}$ and $DNN_{(high)Ke}$, fed with measured SOP_{Mo} and last estimated SOP_{Ke} are used to predict the SOP of the next Mo interval, as well as the evolution of SOP between the current and the next Mo intervals considering SOP_{Ke} values (lines 5-8). Otherwise, low velocity DNN models, $DNN_{(low)Mo}$, are used to predict the SOP for the next Mo interval and linear interpolation of current and predicted SOPs is computed and used to produce the rotation plan (lines 9-11). Recall that measured SOP during Ke intervals return only the absolute values of $S_{2(H)}$, $S_{3(H)}$, $S_{1(D)}$ and $S_{3(D)}$. Those values are used to feed as inputs of an additional DNN model that predicts absolute values of SOP_{Ke} Stokes parameters for the next Ke period. Also, rotation plans are different in R and D bases. Then, the rotation plan includes the needed reversal rotations to track SOP thus, ensuring that the right trajectory is being followed. Lost photons of reversal rotations and wrong signs' selection must be considered in the results.

The interpolation method used in Algorithm 6-II (Method 1) needs at most four reversal rotations performed by the EPC for each predicted SOP_{Ke} to reveal the sign of the Stokes parameters.

Algorithm 6-II. Eavesdropping detection and SOP compensation

INPUT: SOP_{Mo}_Repo, SOP_{Ke}_Repo, $qBER_{Mo}$, avg_$qBER_{Ke}$
OUTPUT: *eaveDetected*, *rotationPlan*

1: $current\_SOP_{Mo} \leftarrow SOP_{Mo}\_Repo.getCurrent()$
2: $S_0 \leftarrow$computeS0($current\_SOP_{Mo}$)
3: **if** $S_0 < 1 - Eve\_S0thr$ OR
$qBER_{Mo}$ - avg_$qBER_{Ke} > Eve_qBERthr$ **then**
4: **return** <true, ->
5: **if** avg_$qBER_{Ke} > 0.1$ AND $S_{1(H)}$.velocity > $velocity\_thr$ **then**
6: $interm_SOPs_{Ke} \leftarrow$DNN$_{(high)Ke}$.predict($SOP_{Ke}\_Repo$)
7: $next_SOP_{Mo} \leftarrow$DNN$_{(high)Mo}$.predict(SOP_{Mo}_Repo)
8: $trajectory \leftarrow$ linearInterpol($current\_SOP_{Mo}$, $interm\_SOPs_{Ke}$, $next\_SOP_{Mo}$)
9: **else**
10: $next_SOP_{Mo} \leftarrow$DNN$_{(low)Mo}$.predict(SOP_{Mo}_Repo)
11: $trajectory \leftarrow$ linearInterpol($current\_SOP_{Mo}$, $next\_SOP_{Mo}$)
12: **return** <false, *rotationAndTracking*($trajectory$)>

After each reversal rotation $qBER_R$ and $qBER_D$ should be checked. As explained before, QRx needs to wait until all photons of the key are received, as well as the transmission time of Bob's bases (T_{tr}) and Alice's samples (T_{tr}) to estimate $qBER_R$ and $qBER_D$. In consequence, the longer the distance between Alice and Bob, the later the estimated qBER is available for the rotation plan. Moreover, the time for SOP computation from the estimated qBERs in Algorithm 6-I (T_{comp}) needs to be considered.

Algorithm 6-III. Interpolation of the rotation plan (Method 2)

INPUT: $current\_SOP_{Mo}$, $next\_SOP_{Mo}$, $interm\_SOPs_{Ke}$, m
OUTPUT: *trajectory*

1: $counter = 1$
2: **for each** SOP_{Ke} IN $interm\_SOPs_{Ke}$ **do**
3: **if** $counter \times T_D < m/2$ **then**
4: sign($SOP_{Ke}[S_2]$)$\leftarrow$sign($current\_SOP_{Mo}[S_2]$)
5: sign($SOP_{Ke}[S_3]$)$\leftarrow$sign($current\_SOP_{Mo}[S_3]$)
6: **else**
7: sign($SOP_{Ke}[S_2]$)$\leftarrow$sign($next\_SOP_{Mo}[S_2]$)
8: sign($SOP_{Ke}[S_3]$)$\leftarrow$sign($next\_SOP_{Mo}[S_3]$)
9: $counter \leftarrow counter + 1$
10: **return** linearInterpol($current\_SOP_{Mo}$, $interm\_SOPs_{Ke}$, $next\_SOP_{Mo}$)

Checking the signs of estimated SOP every T_D would entail losing photons to configure the EPC, as well as when the assumed signs are wrong. In view of this, two alternative interpolation methods to minimize the frequency of checking the signs have been investigated.

Algorithm 6-III details method 2, where the Stokes parameters' sign in next_SOPs_{Ke} are assigned similar to either measured SOP in the last Mo interval or predicted SOP for the next Mo interval based on the one closer in terms of time (lines 1-9). After sign assignments, linear interpolation is used to predict the evolution of SOP

between the current and the next Mo intervals considering SOP_{Ke} values (line 10). Although this method entails that QRx does not need to check stokes parameters' sign, its performance can be poor and result in high qBER.

Algorithm 6-IV. Interpolation of the rotation plan (method 3)

INPUT: *trajectory*, *next_SOP*$_{Ke}$, *qBER*$_{R,}$, *qBER*$_{D,}$, *intrpol_thr*
OUTPUT: *newtrajectory*

1: **if** avg(*qBER*$_{R,}$, *qBER*$_{D}$) > *intrpol_thr* **then**
2: *SOP*$_{Ke}$←estimate_*SOP*$_{Ke}$(*qBER*$_{R}$, *qBER*$_{D}$) (Algorithm 6-I)
3: **while** *qBER*$_{Ke}$ > 0.5% **do**
4: *SOP*$_{Ke}$←sign assumption for *SOP*$_{Ke}$
5: perform reversal rotation
6: *qBER*$_{Ke}$← avg(*qBER*$_{R,}$, *qBER*$_{D}$)
7: **return** linearInterpol(*SOP*$_{Ke}$, *next_SOP*$_{Ke}$)
8: **return** *trajectory*

Algorithm 6-IV describes method 3 for interpolation of the rotation plan, which is a tradeoff between checking the signs and high qBER. We use the rotation plan computed in Algorithm 6-III as the default plan. In case the average of $qBER_R$ and $qBER_D$ in the Ke interval is higher than the threshold (*intrpol_thr*), current SOP is estimated using Algorithm 6-I (lines 1-2). Then reversal rotations for checking the signs are performed (lines 3-6). Recall that QRx needs to wait ($3*T_{tr}+ T_{comp}$) after each reversal rotation to compute the $qBER_{Ke}$ (line6). If the $qBER_{Ke}$ is low enough (under 0.5%), there is no need to check more signs, and the compensational rotations till the next predicted SOP_{Ke} will be linearly planned (line 7).

6.4 Results

In this section we first present our simulation environment. Next, we illustrate the non-ideal behavior of qCh's components verified on an experimental testbed setup in [Ah22-1], [Ah22-2]. Then we show DARIUS's capability to detect eavesdropping and improve the QKD system considering some of those non-ideal behaviors.

6.4.1 Simulation environment

The architecture of DARIUS and the QKD system presented in Figure 6-1 have been evaluated on a simulation environment developed in Python, using IBM's Qiskit development tools [No20]. The simulator implements DARIUS specifications and intelligence as described in Section 6.3, i.e.: *i*) models that mimic qCh components behavior; *ii*) a light key distillation engine that computes the $qBER_R$ and $qBER_D$ from sifted keys; *iii*) DNN models for SOP predictions; *iv*) the algorithms for eavesdropping detector and high velocity event compensator; and *v*) an optical simulator for the QKD system. Emulated events using the experimental datasets in [Bo17] impact the QKD system assuming a 50km optical channel.

All three DNN models, i.e., $DNN_{(low)Mo}$, $DNN_{(high)Mo}$ and $DNN_{(high)Ke}$, are trained with 3×10^6 samples. The SOP_{Mo}_Repo includes measured SOP_{Mo} during the last 10 consecutive Mo intervals and the SOP_{Ke}_Repo contains all SOP_{Ke} = [<$S_{1(H)}$, abs($S_{2(H)}$), abs($S_{3(H)}$)>, <abs($S_{1(D)}$), $S_{2(D)}$, abs($S_{3(D)}$)>] estimated every T_D during the last 10 Mo intervals.

6.4.2 Non-ideal behavior of qCh's components

As explained and shown in the previous chapter, components' non-ideal behaviors were experimentally verified on an experimental testbed setup at UCDavis. Figure 6-4 summarizes the undesired SOP effects in the optical components. The QTx was configured to generate H polarized photons only and to reach a range of 2,500 photons per 0.1 sec: one fixed attenuator and one variable attenuator with 40 and 46 dB, respectively, were placed.

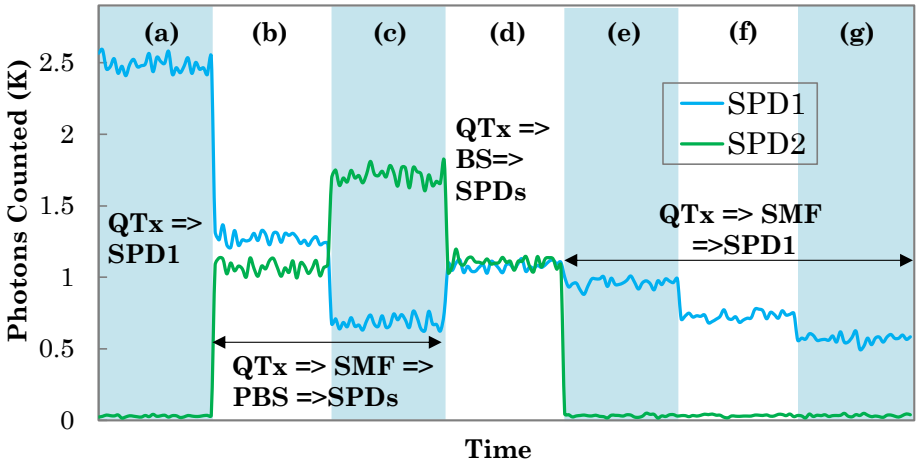


Figure 6-4- Optical component impacts on counted photons

Seven testbed configurations are represented: (a) the QTx was directly connected to SPD1; (b) the QTx was connected to a PBS with a bended SMF. The PBS was followed by SPDs; (c) same to (b) but different SMF bending radius; (d) the QTx was connected to a BS and the BS arms were connected to SPD1 and SPD2; (e, f, g) The QTx was connected to a SPD1 through a SMF of 15km, 20km, 25km, respectively. We observed that the SPDs count 2500 photons only when they are directly connected to the QTx in (a). Installing a bended SMF between QTx and QRx changed SOP of the photons, as photons were counted in SPD2 also.

Furthermore, different shapes of bended SMF introduced different SOP distortion (b-c). In (d), total counted photons in SPD1 plus in SPD2 was 1050 photons on average, i.e., the BS introduced 200 photon loss through its arms. Finally, the longer the fiber, the more the photons were linearly lost (e-g). Apart from the aforementioned results, the dark count rate in the SPD was 30 photons, when the integration time and quantum efficiency were 0.1 second and 10% respectively.

6.4.3 Reference SOPs in Mo intervals

Figure 6-5 illustrates why only H or D reference SOPs sent by the QTx would not enable the QRx to detect aligned distortion to the propagation axis of transmitted photons. Figure 6-5a shows the evolution of the Stokes parameters when the QTx sends H and D SOPs while Poincaré sphere rotates along S_1 axis. SOP evolution is not distorted when the QTx sends H polarized photons, but it is clearly distorted in the case of D polarized ones. The opposite effect on the SOP is observed in Figure 6-5b, when Poincaré sphere rotates along S_2 axis; here H polarized photons enable the QRx to detect the distortion.

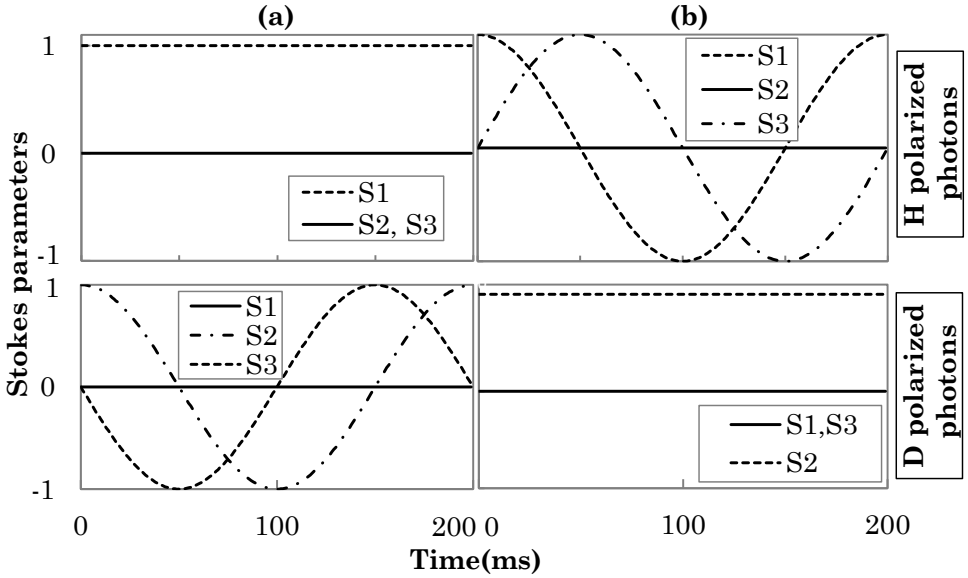


Figure 6-5- Measured SOP evolution.

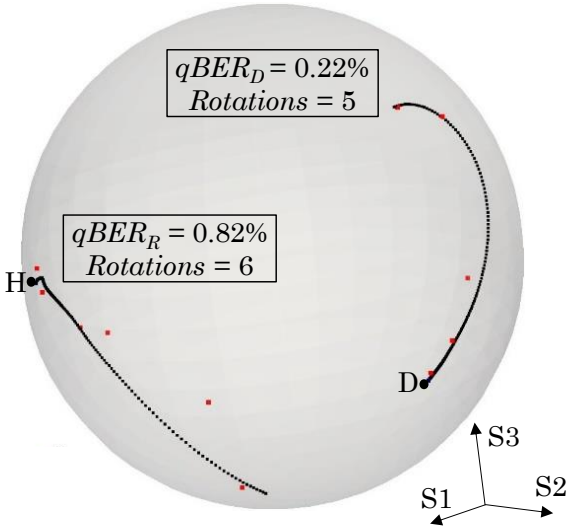


Figure 6-6- SOP trajectories and rotation plans

Figure 6-6 illustrates 0.1s of a low velocity fiber stressing event applied to the qCh considering both R and D bases in the QRx. We observe that SOP trajectories (lines) in R and D bases are clearly different. As the velocity of the event is low, using $DNN_{(low)Mo}$ and linear interpolation for the rotation plan (as proposed in [Ah22]) results in good performance since the QRx can predict both trajectories and plan and apply corresponding reversal rotations. Note that rotations (dots) are being applied at different times by the EPCs installed in R and D bases, and the resulting qBER and number of rotations is also different, as shown in Figure 6-6.

6.4.4 Eavesdropping detection and excessive qBER

Let us now evaluate eavesdropping detection and high velocity events compensation methods for the two scenarios discussed in 6.3.2. For the sake of generality, let us consider different *eavesdropping rate* computed as ratio of the transmitted photons that are actually tampered by the eavesdropper.

Under scenario 1, Figure 6-7 shows how different eavesdropping rates impact on the value of S_0 measured in Mo intervals. For each rate, all possible SOP distortions of the transmitted photons before eavesdropping are evaluated. Photons with less linear SOP are slightly less helpful for revealing the eavesdropper and vice versa, so, average, minimum and maximum S_0 values are plotted. Even extremely distorted photons reaching the eavesdropper disclose tampering in the channel after being measured by the QRx. Assuming *Eve_S0thr*=0.1 (which is actually a very large threshold), even eavesdropping rates as moderate as 14% can be detected.

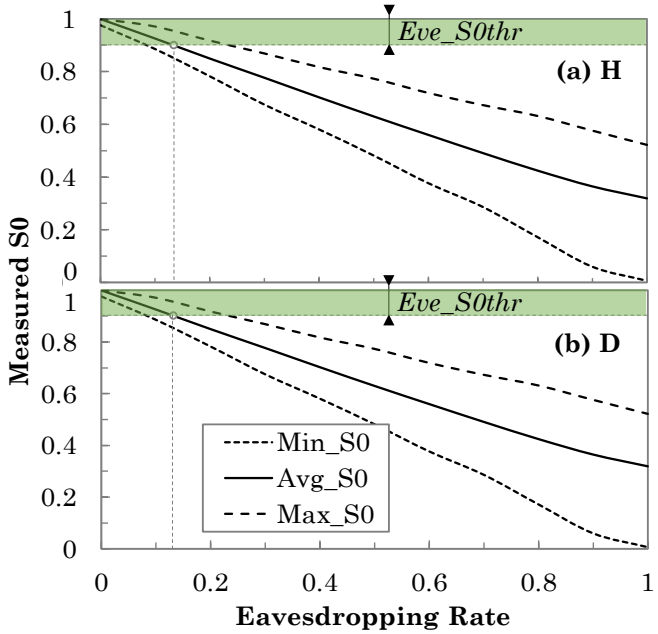


Figure 6-7- Eve detection under scenario 1

Because, the QTx sends H and D polarized photons in Mo intervals to enable QRx to track all sorts of distortions in the qCh, measured S_0 of the received photons in Mo intervals with either polarization is similarly decreased due to the eavesdropping actions.

Figure 6-8 shows eavesdropping detection under scenario 2. $S_{1(H)}$ and $S_{2(D)}$ are measured in both Mo and Ke intervals. In the considered set-up (50 km), T_{Tr} would be about 250µs and T_{SOP_Est} = 500 µs (round-trip time). We also consider T_{comp} = 50µs. Then, total time for SOP estimation is about 550 µs, which is short enough to allow the QRx to estimate $S_{1(H)}$ and $S_{2(D)}$ every 10ms. We observe that the values of $S_{1(H)}$ in Figure 6-8a and $S_{2(D)}$ in Figure 6-8b clearly drop when the eavesdropper tampers the qCh, which enables eavesdropping detection. Such behavior can be analyzed together with the difference between expected $qBER_{Mo}$ and $qBER_{Ke}$ versus the real ones (Figure 6-8c). Considering $Eve\_qBERthr$ = 2%, the analysis clearly reveals eavesdropping even with only 10% eavesdropping rate. Note also that KER significantly reduces when the eavesdropping rate increases following qBER increment, which could lead to false diagnosis if SOP measurements in Ke intervals are not analyzed.

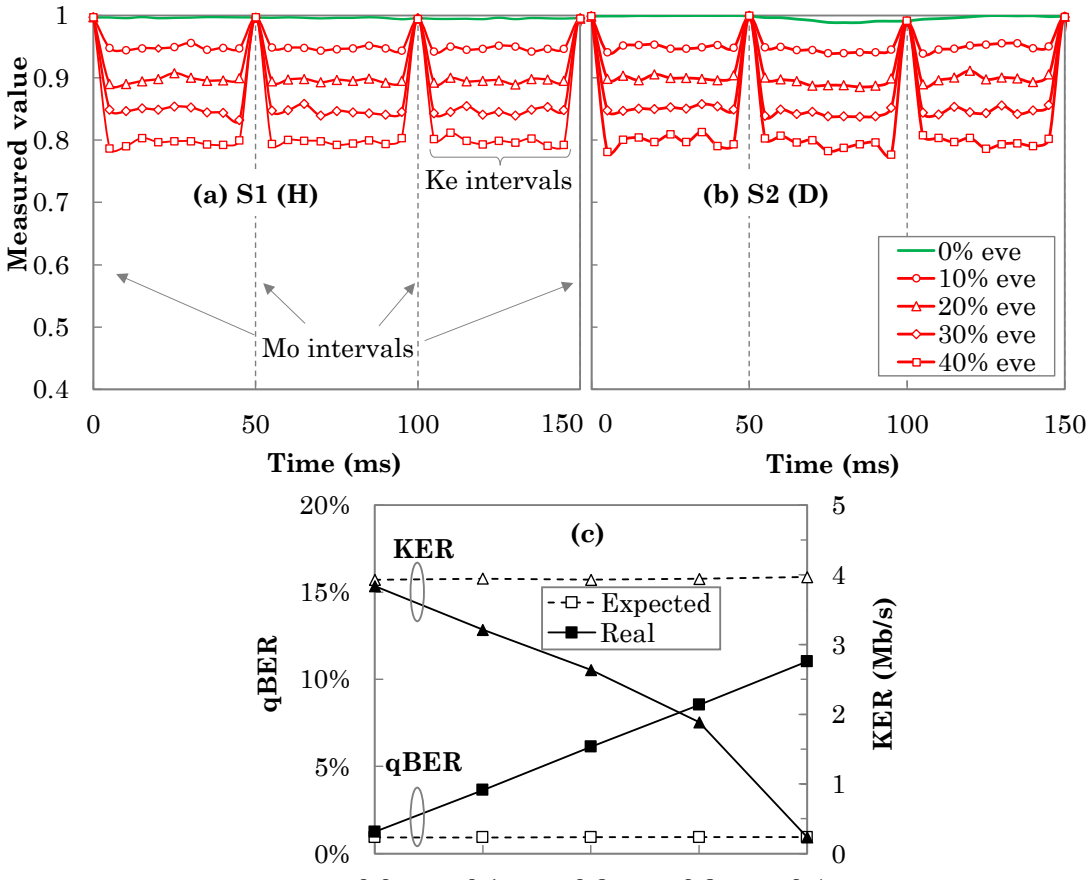


Figure 6-8- Eve detection under scenario 2

Figure 6-9 complements the previous study in the presence of an environmental event affecting the qCh. Even in this case, $S_{1(H)}$ (Figure 6-9a) and $S_{2(D)}$ (Figure 6-9b) values can still disclose the eavesdropping actions in the channel. In this case, qBER is higher than the qBER threshold (10%) and keys are discarded. However, qBER estimation during key distillation can show that $qBER_{Mo}$ and $qBER_{Ke}$ (expected and real *qBER*) are clearly different (Figure 6-9c). Therefore, considering *Eve_qBERthr* = 2%, as in the case where no environmental events affected the qCh, eavesdropping rates as low as 10% can be detected.

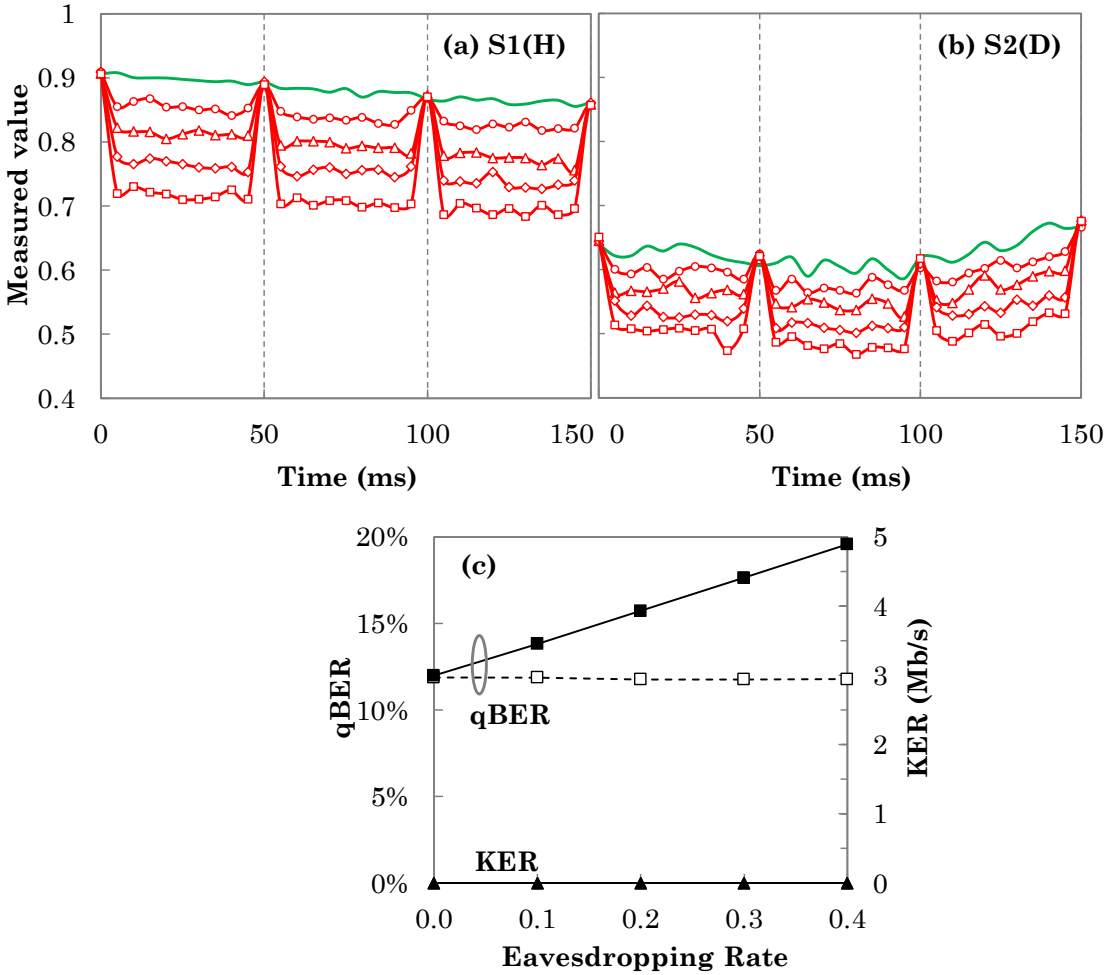


Figure 6-9- Eve detection together with an environmental event under scenario 2

Let us now analyze the case of high qBER coming from high velocity events. For this analysis, we assume a back-to-back (B2B) set up. Let us first analyze the influence of the size of the keys on the precision of the SOP estimation during Ke periods (Figure 6-10a). We observe that keys longer than 22k photons result in very precise SOP estimation using key distillation information. Figure 6-10b-c show the performance of the method of interpolation described in Algorithm 6-II. In Figure 6-10b we observe that keys with 30k photons decrease qBER by 75%. We found that

the average reversal rotation applied by EPC is 1.12, which entails that the first rotation for checking the signs, which assumes the signs similar to the last SOP measurement, almost compensates for the high qBER. In Figure 6-10c, we observe that 30k photons improve KER by 24% Therefore, keys of 30k photons length maximize the precision of SOP estimation and the final KER.

Next, we focus on comparing the different methods for interpolation of the rotation plan (Section 6.3.3) for the B2B scenario. Figure 6-11a illustrates how linear interpolation can be improved by the three proposed interpolation methods taking advantage of the predicted SOP_{Ke}. Method 1 can improve KER by 14% by just using predicted SOP_{Ke} without any reversal rotations for checking stokes' sign. Method 2 improve the linear interpolation by 24% by always checking the signs every 10ms. Finally, the third interpolation method (threshold-based) can improve the QKD system by 31% as it needs less reversal rotations. Note that distance would impact the performance of methods 2 and 3 because of the round-trip-time needed for sign checking.

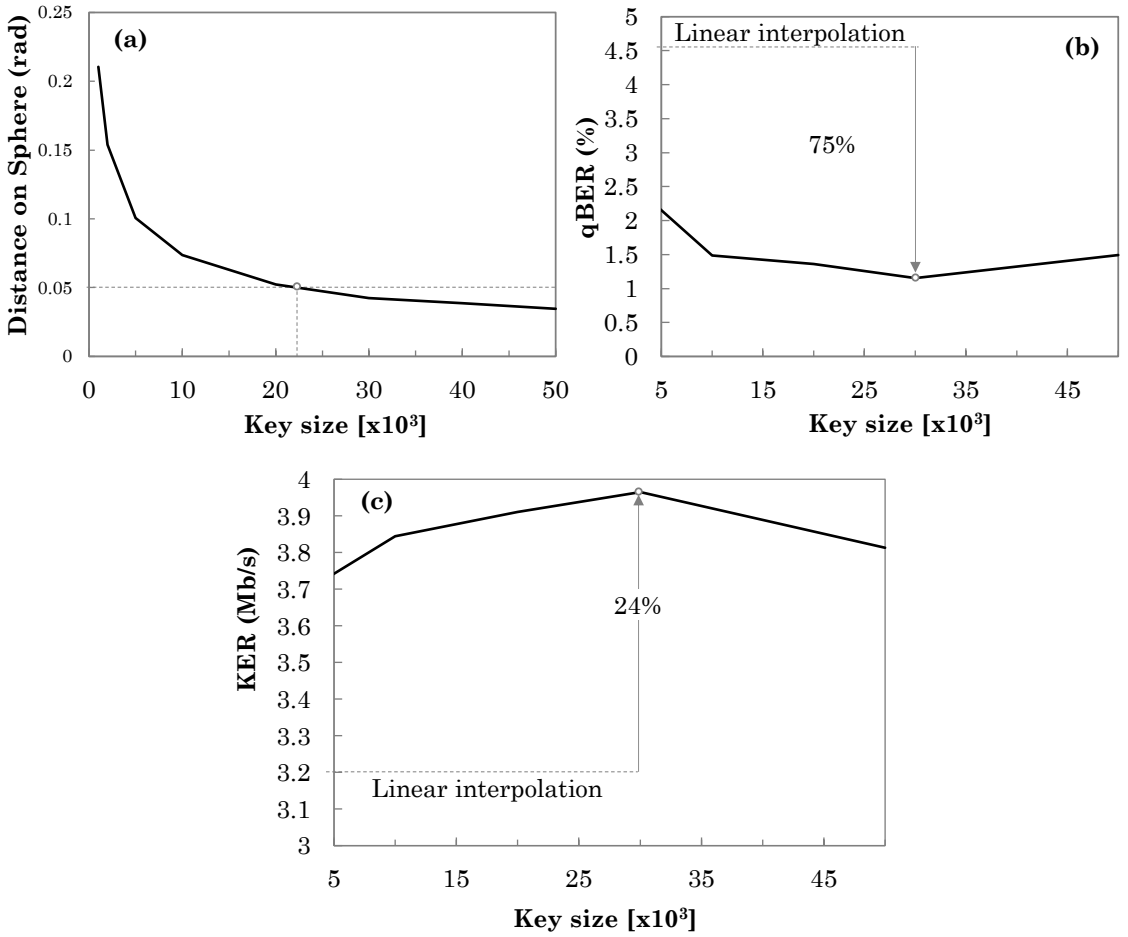


Figure 6-10- Precision of SOP_{Ke} estimation (a), compensation performance w.r.t. qBER (b), and KER (c) in a B2B scenario.

In view of these results, we focus on compensation method 3 and study the impact of the value of intrpol_thr and the distance between the QTx and the QRx. Figure 6-11b compares the performance of method 3 as a function of different thresholds assuming 50 km between QTx and QRx. We observe that *intrpol_thr* = 2% is the best candidate to take the countermeasure action against deficient interpolation. Lower values would waste photons for reversal rotations applied by the EPC and consequently decreases KER, whereas higher values would delay rotation decision making, which would also reduce KER. Finally, Figure 6-11c studies the impact of distance between QTx and QRx assuming *intrpol_thr* = 2%. We observe that although KER reduces with distance, KER is always better than that of linear interpolation for the studied distances.

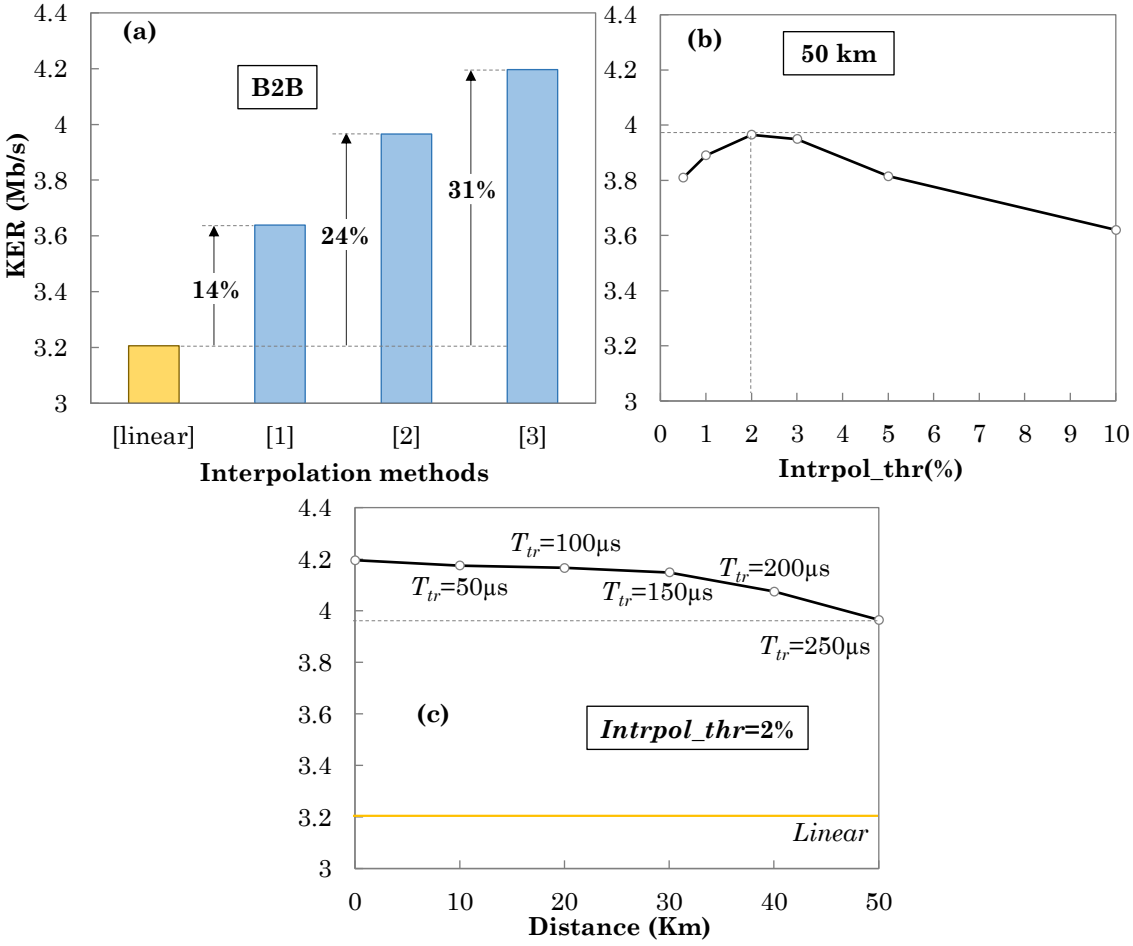


Figure 6-11- Comparison of compensation methods (a) and the performance of compensation method 3 w.r.t the threshold (b) and distance (c).

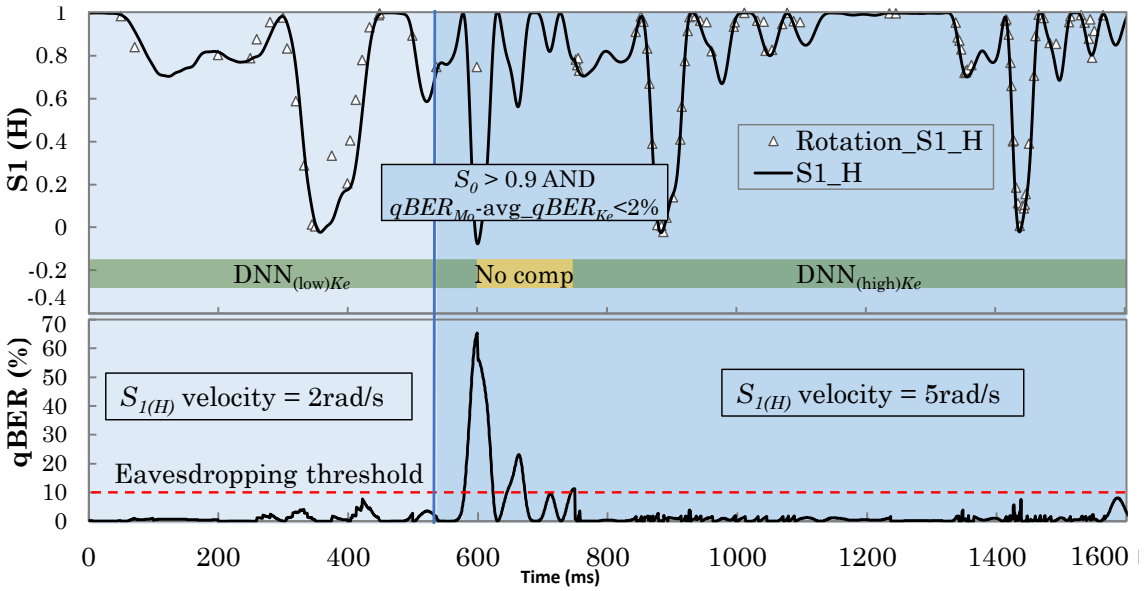


Figure 6-12- Illustrative example of DARIUS operation

A complete example is eventually showcased to illustrate how DARIUS can help the QKD system to address the high qBER in case of higher velocity events is presented. Figure 6-12 reproduces such example, where the evolution of $S_{1(H)}$ (as a SOP representative) and qBER are plotted. Initially, the $DNN_{(low)Mo}$ model is in operation in the AI-based SOP compensator, which uses linear interpolation to compensate for low speed events, and qBER is well under the eavesdropping threshold (10%). At time 300ms, an event of speed 2 rad/s affects the qCh. We observe that the rotation points follow the SOP trajectory with good precision, so qBER remain under the eavesdropping threshold. From 550ms on, the velocity of the events increases and violates the *velocity_thr* (3rad/s), so DARIUS stops compensation until learning the new conditions. As a result, qBER exceeds the threshold and keys are discarded. DARIUS checks for eavesdropping and both scenarios are checked and results detailed in Figure 6-12 confirm no attack. During that period, DARIUS also collects adequate Mo and Ke intervals' SOP measurements to feed $DNN_{(high)Mo}$ and $DNN_{(high)Ke}$ models, in case no eavesdropping is detected. Then, DARIUS checks the velocity of $S_{1(H)}$ before and after the increased qBER and determines that velocity has increased from 2rad/s to 5 rad/s. In consequence, the AI model in operation is changed to $DNN_{(high)Mo}$, and threshold-based interpolation using $DNN_{(high)Ke}$ model is applied. Now, the AI-based SOP compensation method can take advantage of good predictions in the Mo and Ke intervals, and it can perfectly compensate for the higher velocity events and keep the qBER under the threshold.

6.5 Conclusion

A DT named DARIUS has been proposed to improve the performance of polarization-encoded QKD systems. Precise quantum measurement of received photons enable DARIUS to achieve its three main objectives: *i*) consider optical components' non-ideal behaviors in the QKD system to help the QRx discern polarization distortions in the qCh from optical components loss; *ii*) help distillation engines to distinguish between eavesdropping and high qBER in the channel; and *iii*) assist QRx with fine proactive compensation of distortion due to environmental events having different velocity. Including D polarized photons along with H ones for reference SOPs in Mo intervals, enable the QRx to detect a larger sort of SOP distortions in the qCh. Taking advantage of the Mo intervals, DARIUS might not only recognize SOP distortions but also distinguish them from eavesdropping, as both rise the qBER.

DARIUS exhibited extraordinary accuracy in detecting eavesdropping by analyzing its effects on SOP. Even moderate eavesdropping rate of 14% could decrease S_0 by 10% when attacks are performed without knowledge of Mo intervals, whereas eavesdropping rates as low as 10% were detected when they are performed during Ke intervals only, as SOP during those intervals is changed, as compared to that measured during Mo ones.

DARIUS assists the QRx with proper actions against different velocity of fiber stressing events in the qCh. Results showed that DARIUS is able to measure the velocity and choose the best solution to compensate for the effects of the events. DARIUS compensation method improved KER by 31% w.r.t. linear interpolation.

Chapter 7

Closing Discussion

7.1 Main Contributions

This Ph. D. thesis focuses on applying ML techniques for quantum communication. The main contributions are summarized as following:

- First, in Chapter 4, a ML-based SOP tracking and polarization compensator has been presented that might significantly reduce the cost of polarization encoded QKD systems by simplifying the specifications of QTx and QRx and enabling the use of aerial optical fiber cables. The proposed system is based on three main components: i) a SOP monitoring procedure able to precisely estimate the current SOP while minimizing overhead; ii) a lightweight ML-based SOP prediction that is able to accurately forecast future SOP evolution with fine granularity; iii) a Poincaré sphere rotation planner, which decides when rotations need to be performed and the magnitude of such rotations to compensate polarization drift and keep QBER under a given threshold.
- In Chapter 5, part of proposed ML-based SOP compensation in DV-QKD has been experimentally assessed. This assessment performed at UCDavis and planned at UPC in the framework of a NGI Atlantic project. During the experiments, the imperfection and defects of optical equipment in DV-QKD deployment were captured. The experiments caused to come up with employing DT to address the optical components' imperfections.
- In Chapter 6, DARIUS has been presented to address the undesired behavior of optical components being hired in polarization encoded QKD systems. DARIUS encourages the use of aerial optical fiber as the channel and assists QRx with proper and precise quantum measurement of transmitting photons.

The proposed DARIUS aims at three main objectives: i) considers optical components' non-ideal behaviors in the QKD system to help QRx discern polarization distortions in the channel from the loss of optical components. ii) help distillation engines distinguish between eavesdropping and high qBER in the channel. iii) assist QRx with finer proactive compensation of distortion due to environmental events having different velocity.

7.2 List of Publications

7.2.1 Publications in Journals

[JLT22] M. Ahmadian, M. Ruiz, J. Comellas, and L. Velasco, "Cost-Effective ML-Powered Polarization-Encoded Quantum Key Distribution," IEEE/OPTICA J. of Lightwave Technology (JLT), vol. 40, pp. 4119-4128, 2022. DOI: 10.1109/JLT.2022.3157527

[JLT23] M. Ahmadian, M. Ruiz, J. Comellas, and L. Velasco, "DARIUS: A Digital Twin to Improve the Performance of Quantum Key Distribution," submitted in IEEE/OPTICA J. of Lightwave Technology (JLT), 2023.

7.2.2 Publications in Conferences

[ECOC22] M. Ahmadian, M. Ruiz, M. B. On, S. K. Singh, J. Comellas, R. Proietti, S. J. B. Yoo, and L. Velasco, "Designing a Digital Twin for Quantum Key Distribution," in Proc. European Conference on Optical Communication ECOC, 2022.

[ICTON23] M. Ahmadian, M. Ruiz, J. Comellas, and L. Velasco, "ML-Aided SOP Compensation to Increase Key Exchange Rate in QKD Systems," ICTON, 2023

7.3 List of Research Projects

7.3.1 EU-US Funded Projects

- **NGI-ATLANTIC** (Open Call 3) *Experimental Assessment of Fast Quantum Key Distribution*, 2021-2022.
- **ALLEGRO**: *Agile Ultra-Low Energy Secure Networks*, HORIZON-CL4-2022-DIGITAL-EMERGING-01, G.A.: 101092766, 2023-2026.

7.3.2 National Funded Projects

- **IBON:** *AI-Powered Intent-Based Packet and Optical Transport Networks and Edge and Cloud Computing for Beyond 5G*, Ref: PID2020-114135RB-I00, 2021-2024.

7.3.3 Pre-doctoral Scholarship

- Pre-doctoral scholarship related to FI AGAUR 2020-2023 awards.

7.4 Collaborations

I had the opportunity to collaborate with:

- University of California, Davis in the framework of NGI-ATLANTIC project.

7.5 Topics for Further Research

Algorithms and architectures devised in this Ph. D. thesis are being implemented experimentally in the framework of the ALLEGRO project.

List of Acronyms

A	Anti-diagonal
AI	Artificial intelligence
ANN	Artificial Neural Networks
BB84	Bennett and Brassard 1984
BS	Beam Splitter
Comp	Computation
D	Diagonal
DNN	Deep Neural Networks
DV	Discrete Variable
EPC	Electronic Polarization Controller
Est	Estimation
EG	Exhaustive Greedy
ESU	Enumerate Subgraphs
H	Horizontal
KER	Key Exchange Rate
KNN	K-Nearest Neighbors
LC	Left-handed Circular
LSTM	Long Short-Term Memory
ML	Machine Learning
MPC	Manual Polarization Controller
PBS	Polarizing Beam Splitter

PC	Photon Counter
PD	power Sensors
PMD	Polarization Mode Dispersion
qBER	quantum Bit Error Rate
QDT	Quantum Digital Twin
QKD	Quantum Key Distribution
QRx	Quantum Receiver
QTx	Quantum Transmitter
RC	Right-handed Circular
qubit	Quantum Bit
SOP	State of Polarization
SPE	Single Photon Emitter
SPD	Single Photon Detector
SVM	Support Vector Machines
tr	Transmitter
TDM	Time Division Multiplexer
V	Vertical
VOA	Variable Optical Attenuator
WDM	Wavelength Division Multiplexer
WCP	Weak Coherent Pulses

References

[Yu12] P. Yuen, “Fundamental Security Issues in Continuous Variable Quantum Key Distribution,” Quantum Physics, 2012.

[Ra20] M. Ramos, N. Silva, N. Muga, and A. Pinto, “Reversal operator to compensate polarization random drifts in quantum communications,” OSA Optics Express, vol. 28, pp. 5035-5049, 2020.

[Mi01] N. Michael, L. Chuang, “Quantum computation and quantum information,” Cambridge Univ. Press, 2001, ISBN 978-0521635035.

[Ag20] C. Agnesi *et al.*, “Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder,” OSA Optica, vol. 7, pp. 284-290, 2020.

[Di17] Y. Ding, W. Chen, C. Wang *et al.*, “Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits,” Optics Letters, vol. 42, pp. 1023-1026, 2017.

[Ch17] Y. Ding, W. Chen, C. Wang *et al.*, “Polarization variations in installed fibers and their influence on quantum key distribution systems,” OSA Optics Express, vol. 25, pp. 29923-29936, 2017.

[Li19] R. Liu, H. Yu, J. Zan *et al.*, “Analysis of polarization fluctuation in long-distance aerial fiber for QKD system design,” Optical Fiber Technology, vol. 48, pp. 28–33, 2018.

[Ma21] D. Ma, X. Liu, C. Huang *et al.*, “Simple quantum key distribution using a stable transmitter-receiver scheme,” OSA Optics Letters, vol. 46, pp. 2152-2155, 2021.

[Y19] Y. Li, H. Li, H. Xie *et al.*, “High-speed robust polarization modulation for quantum key distribution,” OSA Optics Letters, vol. 44, pp. 5262-5265, 2019.

[Li18] D. Li, S. Gao, G. Li *et al*., "Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback," OSA Optics Express, vol. 26, pp. 22793-22800, 2018.

[Xa09] G. Xavier, N. Walenta, G. De Faria *et al*., "Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation," New Journal of Physics, vol. 11, pp. 45015-45028, 2009.

[Ko02] B. Koch, R. Noé, "PMD-tolerant 20 krad/s endless polarization and phase control for BB84-based QKD with TDM pilot signals," ITG-Fachtagung Photonische Netze, pp. 5424-5426, 2020.

[Wa19] T. Wang, P. Huang, S. Wang, G. Zeng, "Polarization-state tracking based on Kalman filter in continuous-variable quantum key distribution," OSA Optics Express, vol. 27, pp. 26689-26800, 2019.

[Qi20] Liao. Qin, Xiao. Gang, Zhong. Hai, and Guo. Ying, "Multi-label learning for improving discretely-modulated continuous-variable quantum key distribution," New Journal of Physics, 2020.

[Di19] J. Y. Liu, H. J. Ding, C. M. Zhang, S. P. Xie, Q. Wang, "Practical Phase-Modulation Stabilization in Quantum Key Distribution via Machine Learning," Physical Review Applied, vol. 12, 2019.

[Ch21] H. M. Chin, N. Jain, D. Zibar, U. L. Andersen, T. Gehring, "Machine learning aided carrier recovery in continuous-variable quantum key distribution," Npj Quantum Information, vol. 7, pp. 1–6, 2021.

[Du22] Y. Du, X. Zhu, X. Hua, Z. Zhao, Z. Hu, Y. Qian, K, Wei, "Silicon-based decoder for polarization-encoding quantum key distribution," Quantum Physics, 2022.

[Re21] Z. A. Ren, Y. P. Chen, J. Y. Liu, H. J. Ding, Q. Wang, "Implementation of ML in Quantum Key Distributions," IEEE Communications Letters, vol. 25, pp. 940–944, 2021.

[Ne21] S. Neumann, D. Ribezzo, M. Bohmann, R. Ursin, "Experimentally optimizing QKD rates via nonlocal dispersion compensation," Quantum Sci. Technol, vol.6, 2021.

[Co22] H. Costa, N. Muga, N. Silva, A. Pinto, "Optimization of a Polarization-Encoding System for Practical Quantum Key Distribution," WQUANTUM, 2022.

[Qi21] Qiskit Development Team, "Qiskit 0.27.0", (qiskit.org), 2021

[To21] Pytorch community, pytorch 1.9, (pytorch.org), 2021

[Ma20] A. Manzalini, “Quantum Communications in Future Networks and Services,” quantum reports, 2020

[Am22] M. Amir, “What can we expect from Quantum (Digital) Twins?”, 2022

[Lv22] Z. Lv, C.Cheng, H.Song, “Digital Twins Based on Quantum Networking,” IEEE Network, vol. 36, 2022.

[Ma17] V. Martin, J. Martinez-Mateo, M. Peev, “Introduction to Quantum Key Distribution,” Wiley Encyclopedia of Electrical and Electronics Engineering, 2017.

[Ag19] A. Aguado et al., “The Engineering of Software-Defined Quantum Key Distribution Networks,” IEEE Communications Magazine, vol. 57, pp. 20-26, 2019.

[Kh20] M. Khan et al., “Analysis of achievable distances of BB84 and KMB09 QKD protocols,” International Journal of Quantum Information, vol. 18, 2020.

[Ou18] Y. Ou et al. “Field-Trial of ML-Assisted Quantum Key Distribution (QKD) Networking with SDN,” in Proc. ECOC, 2018.

[Me20] M. Mehic et al., “Quantum Key Distribution: A Networking Perspective,” ACM Computing Surveys, vol. 53, 2020.

[Be84] C. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, pp. 175-179, 1984.

[Sh00] P. Shor et al., “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol,” Physical Review Letters, vol. 85, pp. 441-446, 2000.

[Fr17] B. Fröhlich et al., “Long-distance quantum key distribution secure against coherent attacks,” Optica, vol. 4, pp. 163-167, 2017.

[Ru20] M. Ruiz et al., “Predictive Autonomic Transmission for Low-Cost Low-Margin Metro Optical Networks,” Springer Photonic Network Communications, vol. 40, pp. 68-81, 2020.

[Ra18] D. Rafique and L. Velasco, “ML for Optical Network Automation: Overview, Architecture and Applications,” IEEE/OSA J. of Optical Communications and Networking, vol. 10, pp. D126-D143, 2018.

[Be06] I. Bengtsson and K. Zyczkowski, Geometry of Quantum States, Cambridge University Press, 2006.

[To19] E. Toninelli et al., “Concepts in quantum state tomography and classical implementation with intense light: a tutorial,” Advances in Optics and Photonics, vol. 11, pp. 67-133, 2019.

[Wo13] D. Wolfgang et al., “What we can learn about quantum physics from a single qubit,” Quantum Physics, 2013.

[No20] H. Norlen, Quantum Computing in Practice with Qiskit® and IBM Quantum Experience®: Practical recipes for quantum computer coding at the gate and algorithm level with Python, Packt Publishing, 2020.

[ID21] IDQuantique Cerberis3 QKD System. [On-line] https://www.idquantique.com/quantum-safe-security/products/ [Accessed August 2021]

[Pi15] S. Pillay, A. Mirza, F. Petruccione, “Towards polarisation-encoded quantum key distribution in optical fibre networks,” South African Journal of Science, vol.111 pp.7-8, 2015, DOI: 10.17159/SAIS.2015/20130380

[Ra22] M. Ramos, N. Silva, N. Muga, A. Pinto, “Full polarization random drift compensation method for quantum communication,” Optics Express, Vol. 30 pp.9607-9620, 2022.

[Ah22] M. Ahmadian, M. Ruiz, J. Comellas, and L. Velasco, “Cost-Effective ML-Powered Polarization-Encoded Quantum Key Distribution,” IEEE/OPTICA J. of Lightwave Technology (JLT), Vol. 40, pp. 4119-4128, 2022. DOI: 10.1109/JLT.2022.3157527

[Le22] C. Lee, I. Sohn, W, Lee, “Eavesdropping Detection in BB84 Quantum Key Distribution Protocols,” IEEE Transactions on Network and Service Management, Vol. 19 pp.2689-1701, 2022.

[Ca22] G. Castro, R. Ramos, “Enhancing eavesdropping detection in quantum key distribution using disentropy measure of randomness,” Quantum Information Processing, Vol. 21, pp. 79, 2022. DOI: 10.1007/s11128-022-03422-y

[Wa21] D. Wang, Z. Zhang, M. Zhang, M. Fu, J. Li, S. Cai, C, Zhang, X. Chen, “Role of Digital Twin in Optical Communication: Fault Management, Hardware Configuration, and Transmission Simulation,” IEEE Communications Magazine, Vol.59 no.1 pp.133-139, 2021, DOI: 10.48550/arXiv.2011.04877

[Se23] D. Sequeira, M. Ruiz, N. Costa, A. Napoli, J. Pedro, and L. Velasco, “OCATA: A Deep Learning-based Digital Twin for the Optical Time Domain,” J. of Optical Communications and Networking, vol. 15, pp. 87-97, 2023.

[Ba98] S. Barnett, J Jeffers, A. Gatti, “Quantum optics of lossy beam splitters,” Physical Review A, vol. 57, 1998, DOI: 10.1364/OE.24.016440

[Zh18] X. Zhang, Y. Zheng, “Classical Areas of Phenomenology: The number of least degrees of freedom required for a polarization controller to transform any state of polarization to any other output covering the entire Poincaré sphere,” Chinese Physics B vol. 17, pp. 2509-2513, 2018, DOI: 10.1088/1674- 1056/17/7/027

[Si17] A. Sit, et al., “General lossless spatial polarization transformations,” Journal of Optics, Vol. 19, 2017

[Ja98] J. Jackson, Classical Electrodynamics, 3nd ed. Hoboken, NJ: John Wiley & Sons, Inc., 1998. ISBN: 978- 0-471-30932-1

[Al21] M. Al-Mahmoud, H. Hristova, V. Coda, A. Rangelov, N. Vitanov, “Non-reciprocal wave retarder based on optical rotators combination,” OSA Continuum, vol. 4, pp.2695- 2702, 2021, DOI: 10.1364/OSAC.439325

[Mu06] N. Muga, A. Nolasco, M. Ferreira, J. da Rocha, “Uniform Polarization Scattering With Fiber-Coil-Based Polarization Controllers,” IEEE/OPTICA J. of Lightwave Technology, vol. 24, pp 3932-3943, 2006, DOI: 10.1109/JLT.2006.883642

[Ah22-1] M. Ahmadian, M. Ruiz, S. K. Singh, M. B. On, J. Comellas, R. Proietti, S.J. Ben Yoo, and L. Velasco, “Designing a Digital Twin for Quantum Key Distribution,” in Proc. ECOC, 2022

[Ah22-2] M. Ahmadian, M. Ruiz, S. K. Singh, M. B. On, D. Careglio, J. Comellas, R. Proietti, S.J. Ben Yoo, and L. Velasco, “Replication data for Fast Quantum Key Distribution,” https://dataverse.csuc.cat, 2022.

[Bo17] F. Boitier, V. Lemaire, J. Pesic, L. Chavarria, P. Layec, S. Bigo, E. Dutisseuil, “Proactive fiber damage detection in real-time coherent receiver,” in Proc. ECOC, 2017.

[Ta05] X. Tang, L. Ma, A. Mink, A. Nakassis, “High speed fiber-based quantum key distribution using polarization encoding,” in Proc. Optics and Photonics Conference, 2005.

[Sa20] S. Salloum, “ML and Deep Learning Techniques for Cybersecurity: A Review,” Advances in Intelligent Systems and Computing, Vol 1153, 2020.

[Tr09] A. Trongratsameethong, “Exhaustive Greedy Algorithm for Optimizing Intermediate Result Sizes of Join Queries,” International Conference on Computer and Information Science (ACIS), 2009.