DEEP LEARNING BASED OPTIMIZATION OF UNDERWATER QUANTUM KEY DISTRIBUTION SYSTEMS

A Thesis

by

Mostafa Nozari

Submitted to the
Graduate School of Sciences and Engineering
In Partial Fulfillment of the Requirements for
the Degree of

Master of Science

in the
Department of Electrical and Electronics Engineering

Özyeğin University
January 2024

DEEP LEARNING BASED OPTIMIZATION OF UNDERWATER QUANTUM KEY DISTRIBUTION SYSTEMS

Approved by:

Professor Murat Uysal, Advisor
Department of Electrical and Electronics Engineering
Özyeğin University

Assistant Professor Çağatay Edemen
Department of Electrical and Electronics Engineering
Özyeğin University

Professor İbrahim Altunbaş
Department of Electrical and Electronics Engineering
Istanbul Technical University

Date Approved: 25 December 2023

To my parents for their endless support and love.

ABSTRACT

The rapid advancements on quantum computers with high computational capabilities have raised concerns regarding the use of classical cryptography methods. As we enter the era of advanced quantum computing, traditional key generation methods commonly used in wireless systems will encounter substantial security vulnerabilities. These methods rely on computational complexity assumptions, which render them susceptible to attacks by powerful computers. In contrast, Quantum Key Distribution (QKD) technique leverages the principles of quantum mechanics, enabling it to provide a high level of security that is theoretically unconditional. One of the emerging applications of QKD is to provide quantum-secure communication in maritime missions, such as submarine-to-submarine communication, autonomous underwater vehicle (AUV) data offloading, underwater sensor network (USN) data fusion, etc. In this study, we consider underwater QKD systems with time-gated single photon avalanche photodiode (SPAD) and present a comprehensive performance analysis and optimization. The main contribution of this research study is to investigate the quantum bit error rate (QBER) performance of the well-known QKD protocol, namely the BB84 protocol, with respect to different system and transceiver parameters in underwater channels. Our aim is to optimize the bit time and field of view (FoV) parameters in order to minimize the QBER performance metric. Through a meticulous analysis of the propagation delay and angle of arrival results, we determine the bit time and FoV, respectively, by striking a balance between the average number of received photons and background noise. Furthermore, our study provides critical insights into determining the optimal gate time in an underwater QKD system based on the optimal bit time and FoV to minimize the QBER. Given the inherent computational complexity associated with this optimization process, we identify the most influential transceivers and channel parameters

that exert an impact on the determination of bit time and FoV, and utilize a deep learning model for the system optimization. We first perform Monte Carlo simulations for a subset of possible scenarios and train the deep learning model on them. Then, we use this model to extract the optimum values for possible underwater scenarios.

ÖZETÇE

Yüksek hesaplama kapasitesine sahip kuantum bilgisayarlarındaki hızlı ilerlemeler, klasik kriptografi yöntemlerinin kullanımıyla ilgili endişeleri artırmıştır. Gelişmiş kuantum hesaplama çağına girdiğimizde, kablosuz sistemlerde yaygın olarak kullanılan geleneksel anahtar üretme yöntemleri önemli güvenlik açıklarıyla karşılaşacaktır. Bu yöntemler, onları güçlü bilgisayarların saldırılarına açık hale getiren hesaplama karmaşıklığı varsayımlarına dayanır. Buna karşılık, QKD tekniği, kuantum mekaniği prensiplerini kullanarak teorik olarak koşulsuz bir güvenlik düzeyi sağlama yeteneğine sahiptir. QKD'nin ortaya çıkan uygulamalarından biri, denizaltından denizaltıya iletişim, AUV veri aktarımı, USN veri füzyonu vb. gibi denizcilik görevlerinde kuantum güvenli iletişim sağlamaktır. Bu çalışmada, su altı QKD sistemlerini zaman geçitli SPAD ile ele alıyor ve kapsamlı bir performans analizi ve optimizasyon sunuyoruz. Bu araştırmanın temel katkısı, su altı kanallarında farklı sistem ve alıcı-verici parametrelerine göre BB84 protokolü olarak bilinen QKD protokolünün QBER performansını incelemektir. Amacımız, QBER performans metriğini en aza indirmek için bit süresi ve FoV parametrelerini optimize etmektir. Çalışmamız, su altı QKD sistemlerinde optimal geçit süresini belirleme konusunda, optimal bit süresi ve FoV temel alınarak kapsamlı bir analiz sunmaktadır. Yayın gecikmesi ve varış açısı sonuçlarının dikkatli bir analiziyle, ortalama alınan foton sayısı ile arka plan gürültüsü arasında denge kurarak bit süresini ve FoV'yi belirlendi. Ardından, önceki adımlardan elde edilen uygun bit süresi ve FoV kullanılarak QBER'yi en aza indirmek anlamında optimal geçit sürelerini belirlendi. Bu optimizasyon süreciyle ilişkilendirilen hesaplama karmaşıklığı göz önüne alındığında, bit süresi ve FoV'nin belirlenmesinde etkili olan en önemli alıcı-verici ve kanal parametreleri belirlendi ve sistem optimizasyonu için derin öğrenme modeli kullanıldı. İlk olarak, olası senaryoların bir alt kümesi için Monte Carlo

simulasyonları gerçekleştirildi ve bu simulasyonlar üzerinde derin öğrenme modeli eğitildi. Sonra, bu model su altı senaryoların'da optimum değerleri çıkarmak için kullanıldı.

ACKNOWLEDGEMENTS

I am deeply indebted to my advisor, Prof. Dr. Murat Uysal, for his unwavering guidance and support throughout my master's study. His mentorship was not only a privilege but a pivotal factor in my academic and personal development.

I extend my heartfelt thanks to the esteemed members of my dissertation committee, Assistant Prof. Dr. Çağatay Edemen and Prof. Dr. İbrahim Altunbaş, for their invaluable insights and unwavering commitment in reviewing my thesis.

I extend my appreciation to the vibrant community at Ozyegin University, especially my friends who shared in both the joys and challenges of this journey. Their camaraderie and support were a source of strength and motivation.

Special acknowledgment is due to Gizem Bakir, the administrative officer of graduate programs, whose patience and dedication to student affairs made our academic journey smoother and more manageable.

To my beloved parents, Ahmad and Shahnaz, words cannot fully express my gratitude. Their unwavering support and unconditional love have been the bedrock of my happiness and success. They are not only my parents but my greatest advocates and sources of inspiration.

Lastly, I reflect with respect and admiration on the legacy of our ancestors. Their journeys through the annals of history have set the foundation for our own paths. Their achievements and explorations into the mysteries of life continue to inspire and influence us today. May we honor their memory and contributions through our own endeavors and discoveries.

ACRONYMS

QKD	Quantum Key Distribution
AUV	autonomous underwater vehicle
USN	underwater sensor network
QBER	quantum bit error rate
FoV	field of view
CV	Continuous Variable
DV	Discrete Variable
MDI	Measurement-Device-Independent
DPS	Differential Phase Shift
WCP	Weak Coherent Pulse
PM	Prepare and Measure
EB	Entanglement-Based
PIN	positive-intrinsic-negative
AUV	autonomous underwater vehicle
SKR	secret key rate
SPAD	single photon avalanche photodiode
FoV	field of view
ISI	inter symbol interference
AoA	angle of arrival
BS	Beam Splitter
PBS	Polarized Beam Splitter
APD	Avalanche Photodiodes
BS	Beam Splitter

DNN Deep Neural Network

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Motivation

Underwater communication is a domain that poses substantial challenges within the scope of contemporary technology and scientific research. Beneath the ocean's surface lies a complex and dynamic environment where traditional communication methods encounter numerous obstacles. The underwater medium introduces factors such as signal attenuation, absorption, scattering, and the risk of eavesdropping, all of which can disrupt system performance.

The demand for secure and reliable communication in this unique setting is critical, given its wide range of applications, from scientific exploration to maritime defense and underwater infrastructure monitoring. However, in the post quantum era, ensuring the confidentiality and integrity of data transmitted through underwater channels is a formidable challenge. In this context, QKD emerges as a revolutionary solution, offering high security and reliability for underwater communication.

The effectiveness of a QKD protocol depends significantly on system parameters [1]. To ensure optimal performance, it is essential to adjust these parameters according to the channel and environmental conditions, and neglecting this optimization can lead to a performance degradation, potentially rendering it non-operational. Nevertheless, optimizing QKD protocol with respect to system parameters in underwater channel has received relatively little attention and remains an open area of research. One of the primary aspects of QKD optimization is tuning the bit time, FoV, and the value of single photon avalanche diode gate time in a manner that maximizes the system's performance with respect to QBER performance.

1.2 Quantum Key Distribution

QKD stands at the forefront of modern cryptographic techniques, leveraging the principles of quantum mechanics to establish secure communication channels. Unlike classical encryption methods, which rely on mathematical complexity, QKD exploits the inherent properties of quantum systems, providing a theoretically unbreakable framework for transmitting cryptographic keys [2].

1.2.1 The Hilbert Space

In accordance with one of the postulates of quantum mechanics, any isolated or closed quantum physical system is linked to a complex Hilbert space. In the finite-dimensional complex vector spaces encountered in quantum computation and information processing, a Hilbert space is equivalent to a vector space with inner product. This complex vector space is recognized as the state space of the system [3]. The system is entirely defined by its state vector, which is a unit vector within the system's state space.

In classical computation and information systems, the fundamental unit is the classical bit, which can exist in one of two states, 0 or 1. In contrast, quantum information and quantum computation systems operate with Quantum bits, qubits, conceptualized by Benjamin Schumacher [4]. To characterize a quantum state in the state space, it is necessary to first select a basis that is orthonormal to this state space. The widely employed basis is typically the standard basis

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.1}$$

where $|.\rangle$ is a dirac notation. The state of qubits, $|\psi\rangle$, can be represented as a linear combination of selected basis states

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.2}$$

where α and $\beta \in \mathbb{C}$ are complex numbers, referred to as the amplitudes of the state $|\psi\rangle$.

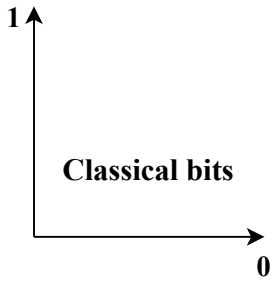


Figure 1: Vector representation of classical bit.

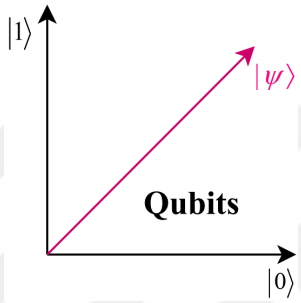


Figure 2: Vector representation of qubit.

Equation (1.2) indicates that a qubit can exist in a quantum superposition, simultaneously occupying both $|0\rangle$ and $|1\rangle$ states. This ability to exist in multiple states simultaneously is a defining feature distinguishing qubits from classical bits [5]. Fig. 1 and Fig. 2 represent the vector representation of the classical bit and qubit, respectively. However, the depiction of a qubit's state is commonly illustrated geometrically using the Bloch sphere (See Fig. 3).

1.3 QKD Design Schemes

The two main schemes used to design QKD protocols are Prepare and Measure (PM) scheme, and Entanglement-Based (EB) scheme [6].

In the PM scheme, the transmitter prepares information by generating polarized photons, which are then transmitted to the receiver. Subsequently, the receiver measures this information. The PM scheme relies on two fundamental principles of quantum mechanics—Heisenberg's uncertainty principle and the quantum no-cloning theorem.

In the EB scheme, a source produces entangled pairs of photons, i.e., the entangled

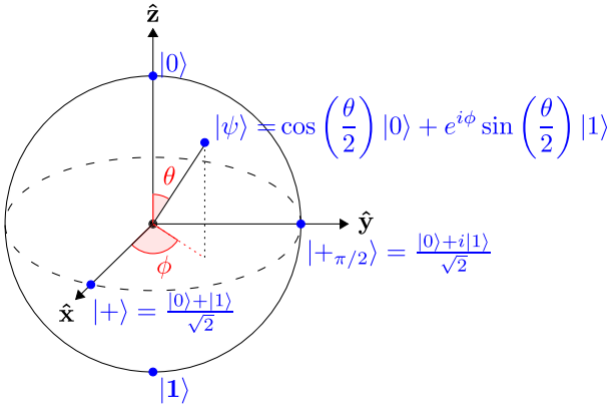


Figure 3: Geometrical representation of a qubit in spherical coordinates [3].

quantum states. These entangled pairs are then directed towards both the transmitter and the receiver. The key idea in EB-QKD is that the quantum states of entangled particles are correlated, meaning that the state of one particle instantaneously determines the state of the other, regardless of the distance between them. Any attempt to eavesdrop or intercept the quantum particles would disturb their entangled state, alerting the communicating parties to the presence of an intruder.

1.3.1 No-Cloning Theorem

In QKD, the No-Cloning Theorem states that making an exact copy of an unknown quantum key is impossible without introducing errors. In practical terms for QKD, if someone tries to intercept and clone the quantum key, they unavoidably mess it up. The No-Cloning Theorem makes perfect copying tricky and tough for an eavesdropper to replicate the key without leaving noticeable signs. This feature significantly boosts the security of QKD, making it harder for someone to duplicate the key.

1.3.2 Heisenberg Uncertainty Principle

In QKD, where properties like photon polarization are considered, the Heisenberg Uncertainty Principle becomes relevant. This principle asserts that when one property, such as

polarization along a specific axis, is precisely measured, uncertainty is unavoidably introduced in the complementary property, like polarization along a perpendicular axis. In the landscape of QKD, where emphasis is placed on precise property measurements, this principle introduces an additional layer of complexity, as uncertainties are inherently generated in related properties.

1.3.3 QKD Protocols

Over the years, several key protocols have been developed, each contributing to the evolution and improvement of quantum secure communication. These protocols can be broadly categorized into three distinct types: Discrete Variable (DV)-QKD [7], Continuous Variable (CV)-QKD [8], and Differential Phase Shift (DPS)-QKD [9]. These protocols use the principles of quantum superposition and entanglement, making them foundational in quantum cryptography. DV-QKD protocol utilizes the polarization states of photons to encode bits. One alternative approach to DV-QKD is CV-QKD. DV-QKD protocols need special equipment like single photon sources and detectors. In contrast, CV-QKD protocols make use of standard telecommunication devices, such as positive-intrinsic-negative (PIN) photodiodes. The main distinction between DV-QKD and CV-QKD lies in how they detect signals.CV-QKD replaces the photon counting method used in discrete-variable coding with a coherent detection method called homodyne detection, taking advantage of the continuous nature of certain quantum properties such as amplitude and phase. CV-QKD is particularly good for long-distance secure communication, making it a promising technology based on the principles of quantum physics. [10]. DPS-QKD is a novel quantum cryptography method. It starts by preparing a single photon in a unique state. This photon is then split into three pulses and sent from transmitter to receiver. The key information is in the phase difference between the second and third pulses, carrying the encoded bits. Receiver measures this phase difference using a technique called passive differential phase detection [11].

While the choice among DV-QKD, CV-QKD, and DPS-QKD is influenced by specific requirements of applications and hardware limitations, it is noteworthy that DV-QKD stands out as more mature method. Consequently, we maintain our focus on these types of protocols and present a chronological overview of notable DV-QKD protocols.

- **BB84 Protocol (1984):** The BB84 protocol, proposed by Charles Bennett and Gilles Brassard in 1984, stands as one of the pioneering QKD protocols. It introduces the concept of quantum bits or qubits, encoding information in two mutually unbiased bases. The sender (Alice) randomly selects one of the two bases to prepare qubits and transmits them to the receiver (Bob). Bob also randomly chooses a basis to measure the qubits. After the transmission, Alice and Bob share their basis choices publicly, discarding the bits where their choices do not match. The remaining bits form a secret key known only to Alice and Bob, and the security of the key relies on the principles of quantum mechanics, making it resistant to eavesdropping [12].

- **E91 Protocol (1991):** In 1991, Artur Ekert proposed the E91 protocol, focusing on entanglement as a resource for secure key distribution. In this protocol, two distant parties share entangled particles. They each measure their particles in one of two bases, and the correlation of their measurement outcomes is used to establish a shared secret key. The E91 protocol utilizes the phenomenon of quantum entanglement, ensuring that any eavesdropping attempt will disturb the entangled particles, alerting the communicating parties to potential security breaches [13].

- **SARG04 Protocol (2004):** The SARG04 protocol, introduced by Scarani, Acín, Ribordy, and Gisin in 2004, provides a significant advancement by combining the ideas of decoy states and parameter estimation. Decoy states involve sending additional states (signal, decoy, and vacuum) to estimate the quantum channel characteristics and enhance security against various eavesdropping strategies. The protocol employs different intensities of light pulses to create decoy states, allowing Alice and

Bob to estimate the error rates and adaptively adjust their parameters for secure key generation [14].

- **Measurement-Device-Independent (MDI)-QKD Protocol (2012):** In the MDI-QKD protocol, proposed by Lo, Curty, and Qi in 2012, security is enhanced by eliminating vulnerabilities associated with imperfect detectors. The protocol uses an intermediary quantum relay to perform joint measurements on the particles sent by Alice and Bob. By employing entanglement swapping, MDI-QKD mitigates detector side-channel attacks, providing a higher level of security [15].

Table 1 provides a summary of all the previously mentioned DV-QKD protocols.

Table 1: Summary of QKD protocols

Name and year of protocol	Protocol Scheme	Qubit Nature
BB84 (1984) [12]	PM	Discrete
E91 (1991) [13]	EB	Discrete
SARG04 (2004) [14]	PM	Discrete
MDI (2012) [15]	EB	Discrete

1.4 Literature Review

The rapid advancements on quantum computers with high computational capabilities have raised concerns regarding the use of classical cryptography methods. In the post-quantum era, classical asymmetric key generation techniques commonly employed in wireless systems will face significant security risks [16]. These methods build upon some computational complexity assumptions and can be susceptible to attacks by powerful computers. QKD relies on the principles of quantum mechanics and provides theoretically unconditional security [2, 17]. The initial QKD protocol introduced by Bennett and Brassard back in 1984, commonly referred to as BB84 [12], is a prepare-and-measure protocol. In this protocol, a qubit state is prepared and subsequently transmitted to the receiving party. Subsequently, entanglement-based protocols were developed, wherein both parties possess a

shared state and perform measurements on it. While entanglement protocols provide an added layer of security by eliminating the need to trust the quantum source, BB84 and its variants protocols have gained greater popularity primarily due to their simplicity.

QKD was successfully applied to fiber optic, satellite, and terrestrial wireless links [18, 19]. Another potential QKD application area is underwater communications. Quantum-secure communication is critical for maritime surveillance sensor networks and military applications such as submarine-to-submarine communication, AUV data offloading, etc. There has been a growing literature on the underwater QKD, see e.g., [20–30]. For example, in [20, 21], based on the Beer–Lambert path loss model, the maximum secure communication distance for the BB84 protocol in underwater environments was derived to achieve a desired level of QBER and the secret key rate (SKR). While initial works ignore the effects of turbulence, later works have demonstrated the effect of turbulence via computer simulations and analytical derivations [22–24] as well as experimental means [25, 26]. Various protocols such as decoy state BB84 [27], BB92 [28], entanglement [29] were further investigated in underwater environments. Absorption, scattering, and turbulence experienced in underwater channels severely limit the range of quantum communication links. As a potential solution to overcome range limitations, multi-hop underwater QKD where intermediate nodes (i.e., relays) between the source and destination nodes help the key distribution was also explored in [30].

In the practical implementation of the BB84 protocol, InGaAs or InP SPAD working in the Geiger mode are commonly employed as detectors [31]. To mitigate the effect of background noise, they are operated typically in the gate mode. However, selecting an inappropriate gate time can filter out a significant number of photons count and lead to performance degradation. The optimal design of time-gated single photon detection system depends on the propagation medium and has been recently studied for underwater links in [32, 33]. In [32], the underwater channel impulse response was estimated through Monte Carlo simulations. Based on the developed channel model, optimal selection of the gate

time was discussed to minimize the QBER. This evaluation was conducted for given values of receiver FoV and bit period. In [33], the bit period was first determined to avoid the inter symbol interference (ISI) arising from multiple scattering, i.e., an emitted photon within the previous bit period can arrive late due to scattering and therefore recorded in the next period. Then, based on the angle of arrival angle of arrival (AoA) of the received photons, the proper value of FoV was selected to restrict the received background noise. Finally, the SPAD gate time was optimized to minimize the QBER for the selected values of FoV and bit period.

1.5 Thesis Outlines

In this thesis, we re-visit the problem in [33] in an effort to have further insight into underwater QKD system design and optimization. Our contributions are three-fold:

- Selection of bit time and FoV were carried out independently in [33]. They are in fact related to each other and must be optimized jointly. The FoV value plays a significant role in limiting the reception of photons which deviate from the direct path between transmitter and receiver and therefore require a longer time to reach the detector due to the extended path. Consequently, the selected FoV value directly affects the required bit time. In this study, we consider the interdependence of bit time and FoV and jointly optimize these two system parameters.

- In [33], to minimize the ISI, the minimum bit period was selected as the required average time for receiving a sufficiently large number of photons. Specifically, a threshold of 99.9% of the total received photons was considered. Similarly, the FoV was selected in [33] as the angle needed to capture a significant number of photons, i.e., a threshold of 99.9%. However, the effect of background noise is ignored during these selections [33]. In this study, we mitigate the degrading effects of noise by properly adjusting the bit time and FoV with respect to QBER. However, this adjustment may result in a higher level of ISI. Consequently, we consider ISI effect in our

optimization as an additional constraint.

- Conducting an interdependence analysis of bit time and FoV with respect to QBER for every variation in the system or channel parameters is computationally expensive. Instead, we utilize a deep learning model for the system optimization. We first perform simulations for a subset of possible scenarios and train the deep learning model on them. Then, we use this model to extract the optimum values for other possible underwater scenarios.

1.6 Organization

The organization of the rest of the thesis is outlined as follows. Chapter 2 delves into the exploration of the trade-off between privacy and efficiency in the process of single photon generation through weak coherence pulses. Subsequently, mathematical derivations are presented to obtain QBER. Moving on to Chapter 3, we begin by introducing the fundamentals of the underwater channel. Following this, the system model is defined, and the interdependency of system parameters and their impact on QBER is discussed. Subsequently, the chapter covers the channel model and the analysis of ISI. In Chapter 4, the supervised-based optimization of QKD systems is expounded upon. Chapter 5 presents numerical results. Finally, Chapter 6 provides a conclusion and summary of this thesis.

CHAPTER II

PRIVACY AND EFFICIENCY

In this section, we discuss the importance of privacy and efficiency through the photon generation discussion and QBER analysis.

2.1 Photon Generation

In the realm of quantum mechanics, light exhibits a dual nature, behaving both as a wave and as a stream of discrete particles known as photons. While traditional light sources emit a multitude of photons simultaneously, the generation of single photons, one at a time, holds significant importance for various advanced technologies, including QKD.

Understanding single-photon generation begins with the concept of atomic energy levels. Electrons in an atom occupy specific energy levels, with the ground state being the lowest energy state. When a photon interacts with an atom, it can be absorbed by an electron, causing it to transition to a higher energy level. This excited state is unstable, and the electron naturally seeks to return to its ground state. During this transition, the electron releases energy in the form of a photon, with an energy equal to the difference between the excited and ground states. This phenomenon, known as spontaneous emission, is the fundamental principle behind single-photon generation.

Several techniques exploit spontaneous emission to produce single photons. One common method, particularly relevant for QKD, is the Weak Coherent Pulse (WCP) technique [34]. This method employs a laser with extremely low intensity, tuned to a specific frequency. When directed through a special crystal, the laser light interacts with the crystal's internal structure, leading to a process known as parametric down-conversion.

Generating single photons, however, presents various challenges. Precise control over the timing and energy of the emitted photons is crucial for many applications. Additionally,

maintaining the purity of the single-photon state can be difficult, as even minimal interaction with the surrounding environment can lead to the absorption or emission of additional photons, compromising the desired single-photon state.

Despite these challenges, single-photon generation remains a vital area of research due to its diverse and innovative applications. In QKD, single photons act as secure information carriers, enabling unbreakable communication protocols. Furthermore, beyond QKD, single-photon sources hold immense potential for revolutionizing fields like quantum computing, biosensing, and long-distance communication.

2.1.1 WCP

WCPs are a commonly used method for generating single photons, particularly in QKD applications. These pulses are characterized by their faintness, with an average number of photons per pulse (μ) significantly less than 1.

While not perfect single-photon sources, WCPs offer a practical approach due to their relative simplicity and stability. However, their inherent randomness leads to the emission of pulses with varying numbers of photons, necessitating a statistical analysis of their behavior.

This randomness follows the Poisson distribution, a well-established mathematical model describing the probability of discrete events occurring in a fixed interval. In the context of WCPs, the events are the emission of photons, and the fixed interval is the duration of the pulse. The Poisson distribution for WCPs can be expressed as

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

where $P(n,\mu)$ represents the probability of having n photons in a pulse. As μ increases, the percentage of pulses containing multiple photons rises sharply. This poses a significant security risk, as eavesdroppers can exploit these multi-photon pulses to gain crucial information about the transmitted key, potentially cracking the QKD system. However,

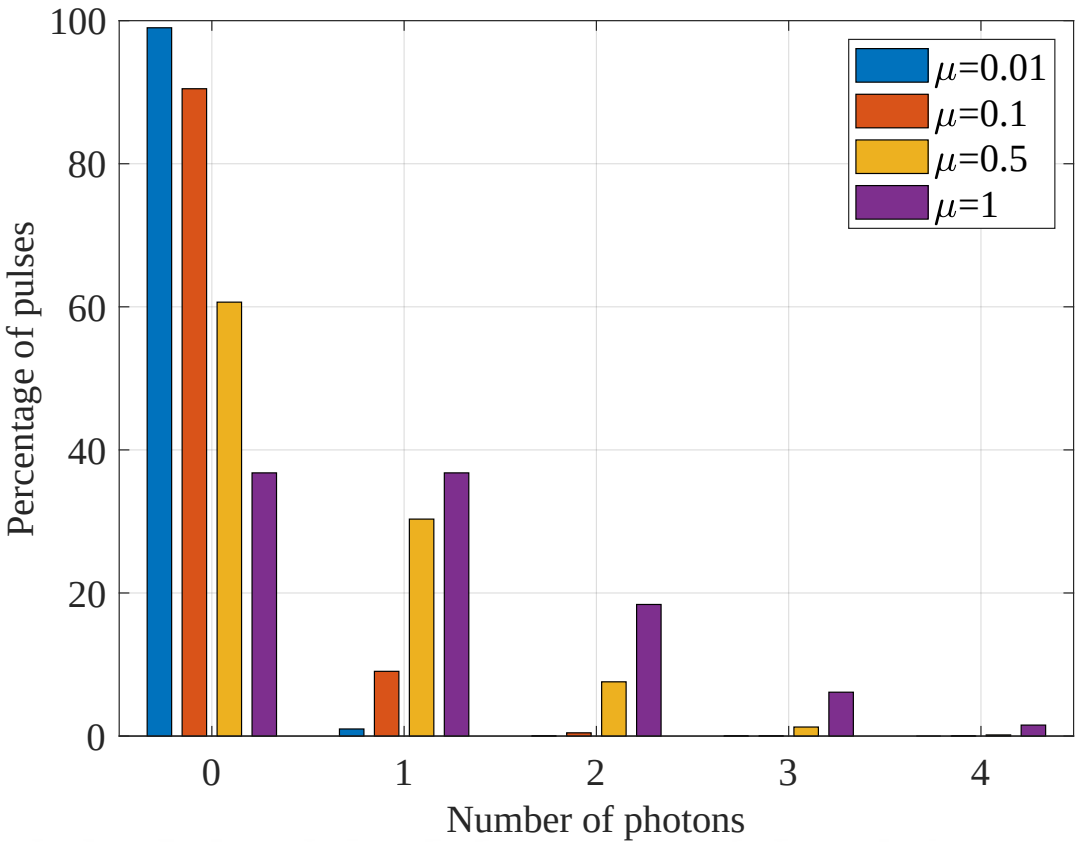


Figure 4: Percentage of Pulses with a Certain Number of Photons for $\mu = 0.01, 0.1, 0.5, 1$.

decreasing μ too drastically reduces the number of pulses containing precisely one photon, the desired outcome for secure key generation. This significantly impacts protocol efficiency, i.e., With a very low μ, most pulses are empty, resulting in wasted time and resources for Alice, who transmits numerous pulses that Bob cannot utilize. Consequently, the overall key generation rate plummets, hindering the QKD system's performance. Fig. 4 vividly depicts the role of choosing the μ in achieving a balance between efficiency and privacy.

By substituting $n = 0$ in Eq. (2.1)

$$P(0,\mu) = e^{-\mu} \tag{2.2}$$

In Eq. (2.2), the probability of pulses without photons is determined, and Fig. 5 illustrates how the system's efficiency decreases as μ in Eq. (2.2) declines.

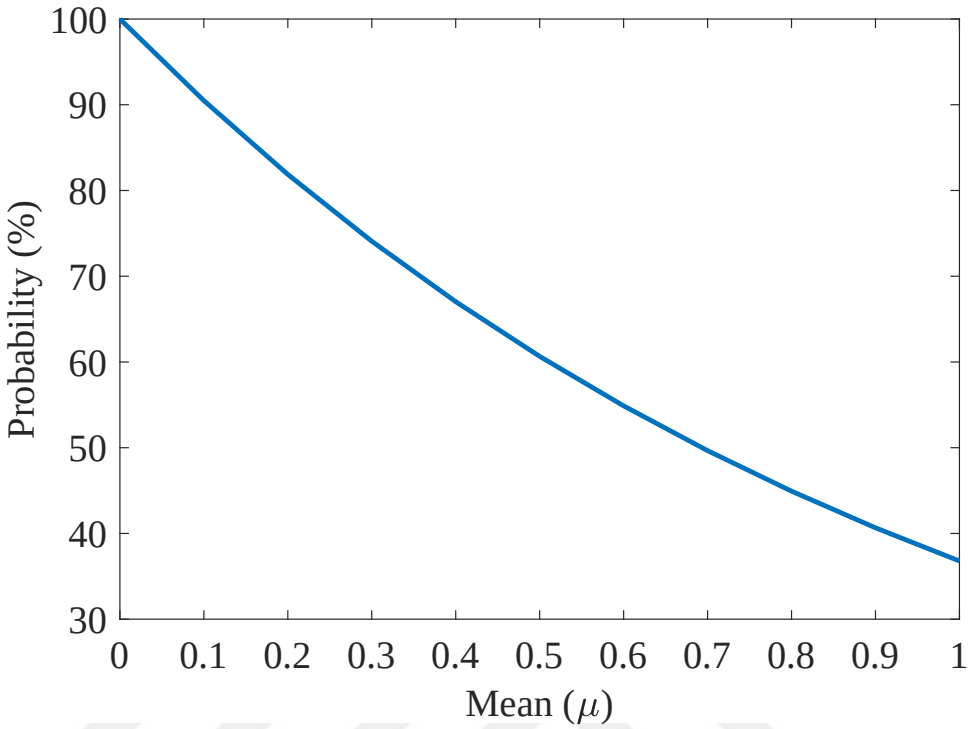


Figure 5: The probability that one pulse does not contain any photon.

$$P(1,\mu) = \mu e^{-\mu} \tag{2.3}$$

From Eq. (2.1) and Eq. (2.2), it can be concluded that the probability of a pulse containing more than one photon, given that it is not null, is equal to

$$P(n>1|n>0,\mu) = \frac{1-e^{-\mu}(1+\mu)}{1-e^{-\mu}} \tag{2.4}$$

Fig. 6 illustrates how increasing the μ negatively affects the privacy of the QKD protocol using WCPs as the single-photon source. As shown in the figure, with μ=0.1, approximately 5% of the pulses contain more than one photon. The threat amplifies further as μ increases. For instance, when μ=0.3, the percentage of pulses with more than one photon jumps to 14%, dramatically increasing the opportunity for eavesdropping and compromising the key security.

In practice, the determination of μ must consider the following key factors:

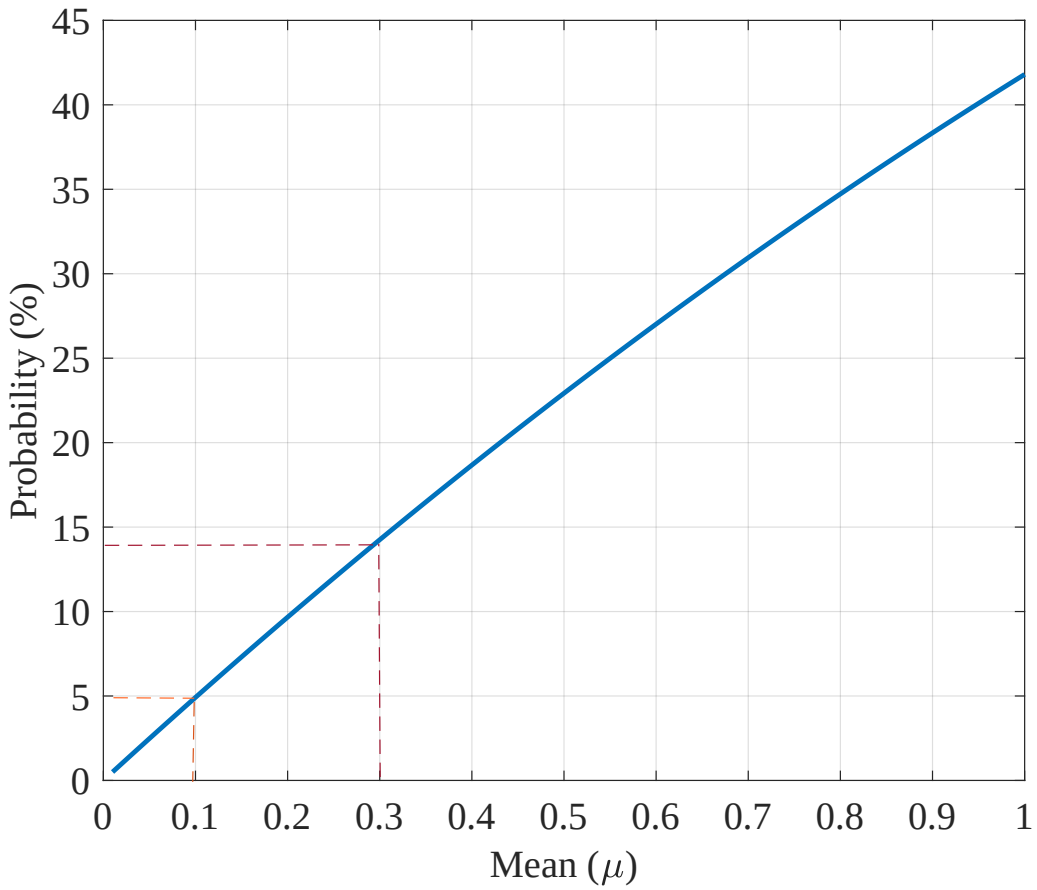


Figure 6: The probability of a pulse containing more than one photon, provided that $n > 0$.

- **Channel Loss:** The transmission channel introduces losses, reducing the number of photons Bob receives. To compensate for these losses and ensure sufficient single-photon pulses reach Bob, a higher μ might be necessary, particularly for longer transmission distances.

- **Detection Efficiency:** Bob's detector, while sensitive, is not perfect. Some single photons may remain undetected, further reducing protocol efficiency. A higher μ can help mitigate this effect, ensuring a sufficient number of single photons are received and detected by Bob.

- **Security Requirements:** The desired level of security dictates the optimal value of μ. For applications with stringent security requirements, a lower μ might be preferable, minimizing the risk of eavesdropping and ensuring the highest level of

key security.

2.2 QBER

One of the most crucial parameters in designing a QKD system is the QBER. QBER refers to the probability of a qubit being received in an incorrect state compared to the state it was transmitted in. Minimizing QBER is essential for ensuring the security and reliability of QKD communication. Several factors can contribute to QBER in QKD systems, including noise, imperfections in front-end devices, and eavesdropper intervention. QBER can be expressed as

$$QBER = \frac{P_{error}}{P_{sift}} \tag{2.5}$$

where, P_{error} is the error probability in the sift events (the events where both parties use the same polarization) and P_{sift} is the total probability of accruing the sift events.

For QBER calculation, we need to consider the average power per pulse denoted as n_s. Due to deleterious effects in the channel, such as turbulence and scattering, only a certain fraction of the photon stream arrives at Bob's destination. Upon reaching Bob, assuming the use of a pure random Beam Splitter (BS) (i.e., 50:50 BS), each pulse will be randomly directed to one of the two possible polarization bases with equal odds. Hence, the randomly selected Polarized Beam Splitter (PBS) will receive a fraction of the pulse power, expressed as $\frac{\gamma n_s}{2}$, where the γ coefficient represents the proportion of photons that reach the receiver after accounting for channel loss. If photons launch into a basis different from what Alice used before, they are randomly conducted to either of the two outputs of PBS. So, the average pulse power is equally divided between the two PBS outputs, and only $\frac{\gamma n_s}{4}$ fraction of power reaches the input of the two associated Avalanche Photodiodes (APD)s.

The pulse streams are not the only signals affecting APDs; there are also undesired signals, including background noise (n_B) and dark-count noise (n_D) mixed up with the signal. Each basis arm is contaminated with n_B, and each APD detector is exposed to n_D.

Consequently, in addition to the desired signal power, each APD is subject to additive noise $n_N = n_D + \frac{n_B}{2}$.

Taking η to represent the fraction of power that APDs are able to capture, the average received power per pulse, denoted by A_i, where Alice and Bob utilize identical polarization filters, either $x, y \in \oplus$ or $x, y \in \otimes$ ($\oplus$ is used to indicate the application of orthogonal filters at angles of 0° and 90°, whereas $\otimes$ denotes the use of diagonal filters at angles of -45° and $+45^\circ$) for the APD in an aligned direction of polarized light, i.e., $x = y$, can be expressed as

$$A_1 = \eta(\frac{\gamma n_s}{2} + n_N) \tag{2.6}$$

If Alice and Bob use the same polarization filter for the APD in a anti-aligned direction of polarized light, i.e., $x \neq y$, the average received power per pulse can be expressed as

$$A_2 = \eta n_N \tag{2.7}$$

If Alice and Bob use different polarization filter $x \in \oplus$ and $y \in \otimes$ or $x \in \otimes$ and $y \in \oplus$ the average received power per pulse for each of the APDs can be expressed as

$$A_3 = \eta(\frac{\gamma n_s}{4} + n_N) \tag{2.8}$$

Given that in each bit interval, only one photon can be captured, the probability of correct detection of photon can be formulated as

$$P_{case1} = P(n = 1|A_1)P(n = 0|A_2)[P(n = 0|A_3)]^2 \tag{2.9}$$

Similarly the probability of incorrect detection in the sift events can be calculated as

$$P_{case2} = P_{error} = P(n = 1|A_2)P(n = 0|A_1)[P(n = 0|A_3)]^2 \tag{2.10}$$

By substituting Eq.(2.2) and Eq.(2.3) into Eq (2.9) and considering $\mu = A_i$, P_{case1} can be expressed as follow

$$P_{case1} = e^{-\eta(\gamma n_s + 4n_N)} \eta (\frac{\gamma n_s}{2} + n_N) \tag{2.11}$$

Similarly, P_{case2} is equal to

$$P_{case2} = P_{error} = e^{-\eta(\gamma n_s + 4n_N)} \eta n_N \tag{2.12}$$

From Eq.(2.11) and Eq.(2.12), it can be concluded that

$$P_{sift} = P_{case1} + P_{case2} = e^{-\eta(\gamma n_s + 4n_N)} \eta (\frac{\gamma n_s}{2} + n_N) + e^{-\eta(\gamma n_s + 4n_N)} \eta n_N \tag{2.13}$$

Therefore, by substituting Eq.(2.12) and Eq.(2.13) into the Eq.(2.5) we have

$$QBER = \frac{P_{error}}{P_{sift}} = \frac{e^{-\eta(\gamma n_s + 4n_N)} \eta n_N}{e^{-\eta(\gamma n_s + 4n_N)} \eta (\frac{\gamma n_s}{2} + n_N) + e^{-\eta(\gamma n_s + 4n_N)} \eta n_N} = \frac{n_N}{\frac{\gamma n_s}{2} + 2n_N} \tag{2.14}$$

CHAPTER III

SYSTEM AND CHANNEL MODELS

3.1 Underwater Channel

The underwater environment presents a unique and challenging medium for communication purposes. Unlike terrestrial radio waves, which can propagate over long distances with minimal attenuation, underwater signals experience significant scattering, absorption, and turbulence [35].

Scattering, a significant factor in the underwater channel, results from the interaction of signals with suspended particles and irregularities in the water. This phenomenon causes signals to deviate from their original path, leading to dispersion and making it challenging to maintain the integrity of transmitted information.

Absorption, the process by which signals lose energy to the surrounding medium, is particularly pronounced in water.

Turbulence adds another layer of complexity to the underwater channel. Water currents and temperature variations create dynamic conditions that can distort signals, leading to fluctuations in signal strength and introducing uncertainties in communication reliability.

3.1.1 Different Water Types and Their Impact on Communication

- **Pure Sea Water:** This type of water represents the ideal case, with minimal impurities and a constant temperature and salinity. It offers the best propagation conditions for photons, with low scattering and absorption. However, pure sea water is rarely encountered in real-world scenarios [35].

- **Clear Ocean Water:** This type of water contains some suspended particles and organisms, leading to increased scattering and absorption compared to pure sea water.

While the impact is relatively minor, it can still affect communication range and reliability [35].

- **Coastal Water:** Coastal waters are characterized by higher turbidity due to sediments, pollutants, and biological activity. This significantly increases scattering and absorption, leading to further limitations on communication range and bandwidth [35].

- **Harbor Water:** Harbor waters are the most challenging environment for underwater communication due to extreme turbidity caused by ship traffic, dredging activities, and harbor infrastructure. The combination of high scattering and absorption severely restricts communication capabilities [35].

3.2 System Model

We consider a QKD system that utilizes the BB84 protocol for underwater communication over a distance of L .For underwater QKD, an operation wavelength of λ in blue and green region is commonly preferred. The QKD BB84 protocol establishes a secure key between two trusted partners, traditionally named as Alice and Bob, to ensure that an eavesdropper (Eve) can not obtain significant information during the key exchange. At the transmitter (see Fig. 7(a)), Alice uses a laser diode followed by a set of four distinct filters to align the light's polarization in certain orientations, e.g., 0°, 90°, -45°, and $+45^\circ$. She randomly selects a filter for each bit time, denoted by Δt, and transmits either 0 or 1 using a beam splitter. The laser is assumed to have a maximum beam divergence of $\theta_{0,\max}$ and a beam width of r_0. While the initial position of photons on the transmitter plane is determined by the beam width, beam divergence affects the departure direction of photons. The directed light goes through an attenuator to ensure proper reduction in light energy and is transmitted through the underwater channel.

At the receiver side (see Fig.7(b)), a filter is used to distinguish the photon signal from the background noise. The filter spectral width, denoted by $\Delta\lambda$, determines the range of

wavelengths allowed by the optical filter for receiving photons. After that, a beamsplitter randomly directs the photon to one of two arms, each corresponding to a different polarization basis. To linearly polarize light, a half-wave plate is used. The photon is then redirected to one of the APDs through a polarizing beam splitter based on its polarization state. APDs have an aperture area of A that represents a surface area over which the incoming light is collected. SPADs working in the Geiger mode are commonly employed as APDs. The gate time of $\Delta t'$ represents a time window ($0 \leq \Delta t' \leq \Delta t$) in which Bob performs measurements on the quantum states sent by Alice, and any reception outside the gate window will cause the photon rejection. The FoV of the SPADs, denoted by Ω, determines the angular extent of the region over which the detector can effectively capture incoming photons. As a result, photons that fall outside the angular region of FoV will not be counted.

Assume that Alice wishes to send a bit string to Bob over the quantum channel to establish a key. Bob randomly selects a combination of polarization bases to measure the light in each bit interval. A "sift" event is triggered when both Alice and Bob use the same polarization basis. Alice and Bob exchange their basis strings over the classic channel and eliminate bits where bases do not match. In the presence of imperfections like interception, noisy channels, or detector issues, sift events may yield different bit values. To verify the equality of the shared key, Alice and Bob reveal a portion of their key over the classic channel. If the number of incorrect bits exceeds a predetermined threshold, the shared key is deemed unreliable. Otherwise, error correction techniques can be applied. Once Alice and Bob have agreed upon the key, they can use it for encryption over the classical channel. In Fig. 8, for instance, the submarine encrypted a plaintext message, M, using k_e and produced $\mathrm{E}_{\mathrm{K_e}}(\mathrm{M})$ to securely be send over the classic channel. Then in the receiver side, the same key, k_e, is used for the sake of decryption and retrieving M. The transceivers can make use of the key for a designated period, which is determined by the security condition of the channel, after which they must undergo the QKD BB84 protocol to generate a new key.

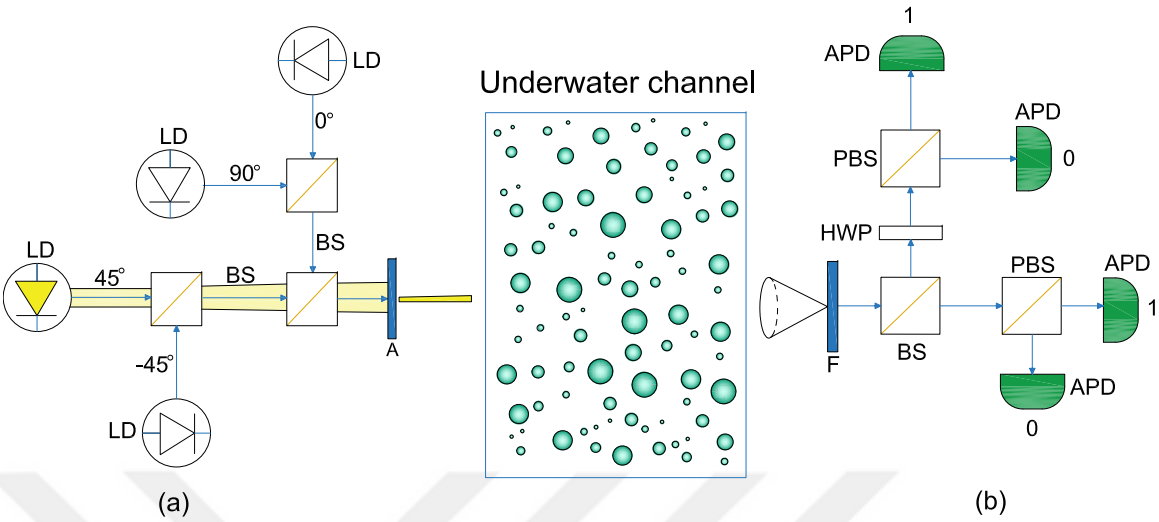


Figure 7: Underwater QKD system under consideration a) transmitter, b) receiver. Transmitter components are laser diode (LD), beam splitter (BS) and (A). Receiver components are filter (F), beam splitter (BS), polarizing beam splitter (PBS), half wave-plate (HWP), and avalanche photodiode (APD).

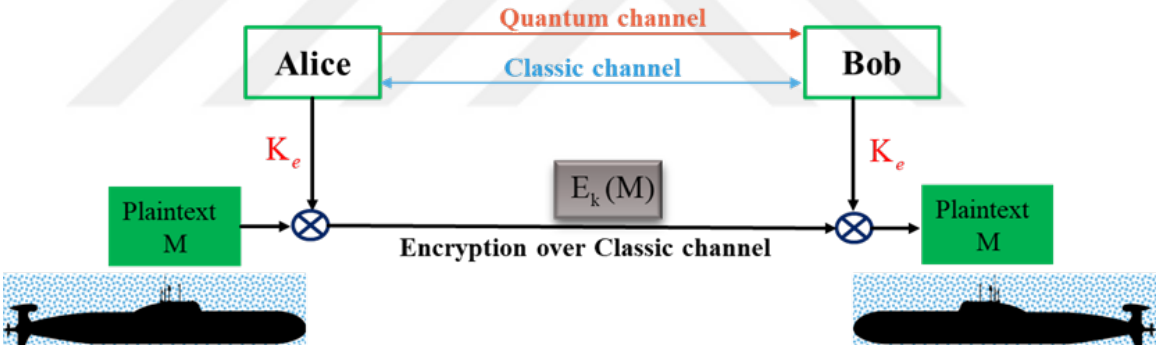


Figure 8: Underwater Secure Communication System Using BB84 for key generation.

3.3 Example of QKD BB84 establishment

In the given scenario illustrated by Fig. 9, let's break down what's happening between Alice and Bob in simpler terms. Assuming an ideal channel devoid of loss, interception, and detector imperfections, Alice wants to transmit the bit string 100110001010110100 to Bob via a quantum channel, in order to establish a cryptographic key. For each bit, Alice has two choices: she can use either linear or diagonal polarization. As shown in Fig. 9 $\otimes\oplus\oplus\otimes\otimes\oplus\otimes\oplus\otimes\oplus\oplus\oplus\otimes\otimes\oplus\otimes\oplus\otimes$ is utilized in order by Alice for the polarization

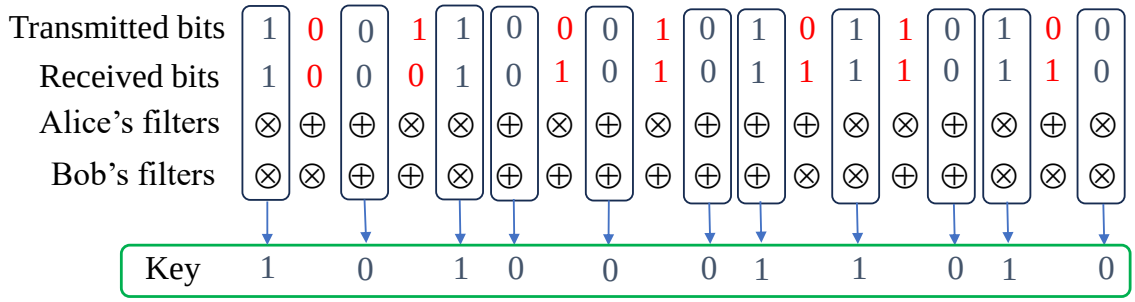


Figure 9: An example of QKD BB84 key establishment.

process. Employing the sequence of filters $\otimes\otimes\oplus\oplus\otimes\oplus\oplus\oplus\oplus\oplus\oplus\otimes\otimes\oplus\oplus\otimes\otimes\otimes$, Bob receives a new bit string 100010101011110110. Subsequently, Alice and Bob engage in the exchange of their utilized filters through a classical channel. They jointly discard the bits from the bit periods during which they employed different polarizations. The remaining bits, "sifts," correspond to the events enclosed within the boxes in Fig. 9, and they constitute the final cryptographic key: 10100011010.

Looking at Fig. 9, it becomes evident that in certain bit times where the parties did not use the same filters for transmission and decoding (e.g., the second time interval), Bob accidentally measures the same bit value as transmitted by Alice. However, since neither party possesses information about the other's actions, these instances cannot be utilized as part of the final key. In general, the probability of both parties using the same filter orientation is 50%, necessitating the transmission of an average of $2n$ bits to establish an n-bit key. It's important to note that in scenarios involving imperfections, such as Eve's interception, noisy or lossy channels, or detector issues, transmitting more than $2n$ bits may become necessary for secure key establishment.

3.4 Interdependency of system parameters and their effect on QBER

According to the QBER calculation in chapter 2, the QBER is defined as the error rate in the sifted key and can be calculated as

$$QBER = \frac{n_N}{\gamma\frac{n_S}{2} + 2n_N} \tag{3.1}$$

where n_S represents the expected number of received photons during each bit interval and the factor of ½ is introduced as a result of sifting process. Based on the well-known Beer-Lambert law, the number of photons is a function of the extinction coefficient depending on the water type.

Background noise is calculated by

$$n_N = n_D + \frac{n_B}{2} \tag{3.2}$$

where the first and second terms respectively arise from the dark current of the SPADs and environment irradiance. The first term is calculated as

$$n_D = I_{dc}\Delta t \tag{3.3}$$

where I_{dc} is the dark current count. It determines the average rate of dark current events in the absence of incident light and relates to the sensitivity of SPAD detectors. The second term is given as

$$n_B = \frac{\pi R_d A \lambda \Delta\lambda (1 - \cos(\Omega))\Delta t'}{2h_p c_0} \tag{3.4}$$

where, h_p is Planck's constant, c_0 is the speed of light, and R_d is the irradiance of the environment whose primary source is the refracted sunlight from the surface of the water [36].

It can be readily checked from Eq. (3.1) that increasing the value of n_N can result in a higher QBER. Therefore, it is crucial to limit the effect of background noise. Based on Eq. (3.3), it is observed that the level of background noise arising from dark current only depends on the bit time (Δt). On the other hand, as can be seen from Eq. (3.4), the level of background noise due to irradiance is dependent on several system parameters including

FoV , gate time, aperture area and filter spectral width. In the following, for given values of maximum beam divergence, beam width and aperture area, we will discuss how bit time and FoV values affect the QBER performance and how they interplay with each other.

A straightforward approach to determine the bit time, as adopted in [33], is based on the required time to guarantee the reception of a very high percentage of photons (99.99%). Such a conservative approach ensures reliable transmission by avoiding ISI, however requires large values of the bit time. This, in turn, increases the amount of background noise as a result of the dark current from SPADs. Similarly, the value of FoV can be selected as in [33] to allow for the inclusion of a significant number of photons. However, increasing the FoV leads to a greater number of background photons, which in turn can increase the noise as a result of the irradiance from environment. Moreover, FoV and bit time are dependent on each other. Choosing a large FoV (e.g., 180°) allows for more photons to be taken into account and deals with the worst case scenario of ISI. This helps to even capture the photons that deviate significantly from the direct propagation line. However, this increases the propagation time and accordingly necessitates a larger value of bit time, eventually leading to further increase in the background noise. As a summary, we need to carefully weigh the benefits of considering a higher percentage of photon reception against the potential drawbacks of longer required reception times and a larger FoV to achieve best QBER performance.

Based on the chosen values for bit time and FoV, an appropriate gate time for SPADs can be selected. The gate time is upper-bounded by the selected bit time, and changing the FoV usually leads to variations in the optimized gate time value. Opting for a longer gate time can reduce the probability of missing a photon; however, it may result in a higher number of ISI. As can be seen from 3.4, it also results in greater exposure to background radiation, which, in turn, amplifies noise. Thus, to attain the best QBER performance for the selected bit time and FoV, the gate time must be optimized to balance the trade-off between the probability of missing a photon and the noise levels in the system.

3.5 Channel model

In our study, we use the Monte Carlo modeling of light transport in the multi-layered tissues (MCML) method [37]. The transmitter can be conceptualized as a circular planar aperture located at the origin of the z-axis ($z = 0$). This aperture possesses an initial radius of r_0 and a maximum initial divergence angle of $\theta_{0,\max}$. In mathematical terms, this can be expressed as follows

$$T = \{(x, y, z) \mid x^2 + y^2 \leq r^2, z = 0\} \tag{3.5}$$

The initial location of each emitted photon within the transmitter aperture is defined by its coordinates $(x, y, 0)$. The coordinates of the photons are determined using the following scheme:

1. **Azimuthal Angle:** The azimuthal angle, denoted by φ_0, specifies the direction of the photon within the plane of the aperture. This angle is generated randomly from a uniform distribution between 0 and 2π radians, i.e., $U[0, 2\pi]$.

2. **Coordinate Mapping:** The x and y coordinates are then derived from the φ_0 and the r_0 using trigonometric relationships

$$x = r_0 \cos \varphi_0 \tag{3.6}$$

$$y = r_0 \sin \varphi_0 \tag{3.7}$$

   This mapping ensures that each photon originates within the circular boundary of the transmitter aperture.

The direction of each photon is represented by a unit vector (μ_x, μ_y, μ_z). This vector defines the path along which the photon will propagate from the transmitter. The direction is determined using the following steps:

1. **Polar Angle:** The polar angle, denoted by θ_0 specifies the elevation angle of the photon's trajectory relative to the z-axis. This angle is generated randomly from a uniform distribution within a range bounded by the $\theta_{0,\max}$, i.e., $U[-\theta_{0,\max}, \theta_{0,\max}]$.

2. **Direction Vector Components:** The components of the direction vector are then computed using the polar angle and the azimuthal angle using the following equations

$$\mu_x = \sin\theta_0 \cos\varphi_0 \tag{3.8}$$

$$\mu_y = \sin\theta_0 \sin\varphi_0 \tag{3.9}$$

$$\mu_z = \cos\theta_0 \tag{3.10}$$

Once launched from the transmitter, each photon interacts with particles along the way. The initial weight of the photon is assumed to be 1. As the photon travels, it encounters particles and can be scattered or even absorbed [37]. The distance traveled before the first interaction is denoted by δ and can be calculated as follow

$$\delta = -\ln(q)/\varsigma(\lambda) \tag{3.11}$$

where q is a uniformly distributed random variable between 0 and 1, λ represents the wavelength, and $\varsigma(\lambda)$ is the extinction coefficient, which accounts for both absorption and scattering and can be expressed as $\varsigma(\lambda) = \alpha(\lambda) + \beta(\lambda)$, where $\alpha(\lambda)$ and $\beta(\lambda)$ represent absorption and scattering coefficients, respectively. In the model, we rely on the assumption that the quantum states of scattered photons remain invariant. This means that despite undergoing changes in direction due to scattering events, the polarization of the photons is preserved [33, 38]. Following each interaction with a particle in the water, the photon experiences a decrease in energy. This decrease in weight can be mathematically represented by the following formula [37]

$$w' = w\beta(\lambda)/\varsigma(\lambda) \tag{3.12}$$

where w and w' denote the photon energy before and after interaction with a particle in the water, respectively.

Given a photon's initial propagation direction (μ_x, μ_y, μ_z) and scattering parameters (ϕ,θ), the new propagation direction $\left(\mu'_x, \mu'_y, \mu'_z\right)$ can be calculated as [33]

$$\mu'_x = (\mu_x \mu_z \cos\phi - \mu_y \sin\phi) \sin\theta / \sqrt{1-\mu_z^2} + \mu_x \cos\theta \tag{3.13}$$

$$\mu'_y = (\mu_y \mu_z \cos\phi + \mu_x \sin\phi) \sin\theta / \sqrt{1-\mu_z^2} + \mu_y \cos\theta \tag{3.14}$$

$$\mu'_z = -\sin\theta \cos\phi \sqrt{1-\mu_z^2} + \mu_z \cos\theta \tag{3.15}$$

The photon's position can be updated using the following equations

$$x' = x + \mu'_x \delta \tag{3.16}$$

$$y' = y + \mu'_y \delta \tag{3.17}$$

$$z' = z + \mu'_z \delta \tag{3.18}$$

If the initial z-component of the propagation direction is very close to 1 ((i.e., $|\mu_z| > 0.9999$), then the new propagation direction can be approximated as $\mu'_x \cong \sin\theta\cos\phi$, $\mu'_y \cong \sin\theta\cos\phi$, and $\mu'_z \cong \mu_z \cos\phi / |\mu_z|$ [33].

The azimuthal angle ϕ is modeled as a random variable (RV) with a uniform distribution in the range of $U[0, 2\pi]$. The scattering angle θ is calculated based on the scattering phase function [37], which describes the angular distribution of light intensity scattered by a particle. The scattering angle can be calculated as follows

$$\chi = \int_0^\theta p(\Psi, a, g_{\mathrm{f}}, g_{\mathrm{B}}) \sin(\Psi)\, d\Psi \tag{3.19}$$

where χ is an auxiliary random variable generated with a uniform distribution in the range of $U[0,\pi]$.

The Two Term Henyey–Greenstein (TTHG) model [39] is utilized as the scattering phase function

$$p_{\mathrm{TTHG}}(\theta, a, g_{\mathrm{f}}, g_{\mathrm{B}}) = a p_{\mathrm{HG}}(\theta, g_{\mathrm{F}}) + (1-a)\, p_{\mathrm{HG}}(\theta, -g_{\mathrm{B}}) \tag{3.20}$$

where a is the weight of the forward Henyey–Greenstein (HG) phase function, and g_{F} and g_{B} are the asymmetry factors for the forward and backward-directed HG phase functions, respectively [33]. The HG phase function is given by

$$p_{\mathrm{HG}}(\theta, g) = \left(1-g^2\right) / \left[2\left(1+g^2-2g\cos\theta\right)^{1.5}\right] \tag{3.21}$$

The relationships between a, g_{B}, g_{F}, and $\overline{\cos\theta}$ can be expressed as [33, 39]

$$g_{\mathrm{B}} = -0.3061446 + 1.000568 g_{\mathrm{F}} - 0.01826338 g_{\mathrm{F}}^2 + 0.03643748 g_{\mathrm{F}}^3 \tag{3.22}$$

$$a = g_{\mathrm{B}}(1+g_{\mathrm{B}}) / [(g_{\mathrm{F}}+g_{\mathrm{B}})(1+g_{\mathrm{B}}-g_{\mathrm{F}})] \tag{3.23}$$

$$\overline{\cos\theta} = a(g_{\mathrm{F}}+g_{\mathrm{B}}) - g_{\mathrm{B}} \tag{3.24}$$

An approximation for $\overline{\cos\theta}$ is presented in [33] as

$$\overline{\cos\theta} \cong 2(1-2B)/(2+B) \tag{3.25}$$

where $B = \beta_b/\beta$ and β_b is back scattering coefficient.

The process of photon scattering continues iteratively until the photon either reaches the receiver or is lost due to multiple scattering. The inherently random trajectory of the photon during this process can introduce ISI at the receiver side if the bit time is chosen based on a portion of received photons instead of considering roughly all the received ones.

To model the ISI, let t_p denote the arrival time of a photon belonging to one of the bit times in the interval of $[1, m-1] \in \mathbb{N}$. Here, m denotes the bit time where the ISI occurs within that interval and is given by $m = \left\lfloor \frac{t_p}{\Delta t} \right\rfloor$, where $\lfloor . \rfloor$ represents the floor function. ISI occurs if the arrival time of a photon is greater than the bit time, i.e., $t_p > \Delta t$ and the inequality $m\Delta t < t_p < (m\Delta t + \Delta t')$ is satisfied. This inequality indicates that the arrival of a photon belongs to a bit time within the range of [1, m-1] and inside the gate window of the m^{th} bit time.

CHAPTER IV

SUPERVISED LEARNING-BASED QKD SYSTEM OPTIMIZATION

As discussed in the previous chapter, many system and channel parameters are related to each other and have direct or indirect effects on the QBER. Optimal underwater QKD system design taking into interdependence for every variation in the system or channel parameters is computationally expensive. To overcome this challenge, we utilize supervised learning [40] for optimization. This type of machine learning is analogous to human learning from past experiences to gain new knowledge in order to improve our ability to perform real-world tasks [40]. Since computers lack their own experience, we rely on labeled datasets in supervised learning. These datasets consist of multiple data samples. Each data sample is denoted as $(x^{(m)}, y^{(m)})$, where $x^{(m)}$ represents a feature vector for the m^{th} sample (representing the causes leading to a particular experience) and the label $y^{(m)}$associated with feature $x^{(m)}$ to reflect the experience itself.

The goal of supervised learning is to learn the underlying relationship between the features and their corresponding labels. For this purpose, it employs an appropriate deep learning architecture and trains it using a proper cost function to make accurate predictions for new combination of input features. Deep neural networks (Deep Neural Network (DNN)s) can capture intricate nonlinear relationships within the data, which can be particularly valuable in use cases where there may be complex interactions among the input features. A DNN is composed of multiple layers, including an input layer and an output layer, along with intermediate layers referred to as hidden layers. Neurons within each layer receive inputs from multiple neurons in the preceding layer and perform computations. This typically involves a weighted sum followed by a nonlinear activation function. Mathematically

speaking, it is given by

$$A_j^{[l]} = \sigma_j^{[l]} \left(\sum_i w_{ji}^{[l]} z_i^{[l]} + b_j^{[l]} \right) \tag{4.1}$$

where $A_j^{[l]}$ represents the output of the j^{th} neuron in the l^{th} layer, $\sigma(.)$ represents an activation function utilized to introduce non-linearity in the modeling process, $z_i^{[l]}$ represents an input from the i^{th} neuron of the preceding layer (in the first layer, this corresponds to the i^{th} feature from $x^{(m)}$), $w_{ji}^{[l]}$ corresponds to the weight between that input and the j^{th} neuron in the l^{th} layer, and $b_j^{[l]}$ denotes the bias term associated with the j^{th} neuron in the l^{th} layer.

Assume that the DNN includes L layers. Based on the inputs of the last layer, i.e., $z_j^{[L]} = A_j^{[L-1]}$, the predicted label value for the m^{th} sample can be calculated as

$$y_{\text{pred}}^{(m)} = \sum_i w_{1i}^{[L]} z_i^{[L]} + b_1^{[L]} \tag{4.2}$$

where $w_{1i}^{[L]}$ is the weight between i^{th} neuron in the $(L-1)^{th}$ layer and the single neuron in L^{th} layer, and $b_1^{[l]}$ is the bias term associated with the neuron in the L^{th} layer. The mappings in (5) and (6) are learned from the labeled data by adapting each neuron's weights and bias using forward-backward propagation sequences through a proper cost function [41]. The cost function compares the predicted value in (6) with the actual label across all the training data samples. The cost function averaged across the entire training set can be envisioned as a landscape with hills and valleys in the high-dimensional space of weight parameters. The negative gradient vector of the cost function indicates the direction of the steepest descent within this landscape, guiding the optimization process toward a minimum where the average output error is minimized [42]. This process is commonly referred to as backpropagation and is accompanied by forward propagation, where the updated weights are used to calculate the output. This iterative process of adjusting weights through backpropagation and calculating output through forward propagation is called the training process and continues until convergence is achieved or predetermined condition met.

4.1 Numerical Results and Discussion

In this section, we employ a DNN and train it to determine the optimal underwater QKD parameters with sufficient precision. For training, we first need to collect data samples of bit time and FoV values. Due to the lack of an off-the-shelf dataset for our specific purpose, we need to create our own by identifying the suitable feature vectors and their corresponding labels. For this purpose, we conduct a comprehensive exploration of the parameter space, meticulously examining the interdependencies among the bit time and FoV, and their impact on QBER performance as earlier described in Section III.

4.1.1 Data set generation

In this section, we explain how we generate dataset to train our DNN model. Through earlier discussions in Section 3.4, the major parameters that notably affect the bit time and FoV include beam width, beam divergence, receiver aperture diameter, link length, and water type. These constitute the elements of the five-dimensional feature vector which is the input to the DNN. As shown in Fig.10, we use a DNN with four hidden layers to learn the mapping from QKD system parameters to bit time and FoV values.

We partition both datasets of bit time and FoV into training and validation, with a ratio of 80:20, respectively. In other words, we dedicate 80% of the dataset for training purposes and 20% for the test of the model. In the simulations, we assume beam width of $r_0 = 3,\ 6$ mm, initial divergence of $\theta_{0,\max} = 20^\circ,\ 30^\circ$, receiver aperture diameter of $A = 10,\ 20,\ 30$ cm, link length of $L = 5,\ 10,\ 15,\ 20,\ 25,\ 30,\ 35,\ 40$ m and extinction coefficient of $\zeta = 0.0056,\ 0.15,\ 0.305,\ 2.17\ \mathrm{m}^{-1}$ that correspond to pure sea, clean ocean, coastal water, and harbor water. The ranges of the parameters under consideration are provided in Table 2 which leads to a dataset of 384 samples.

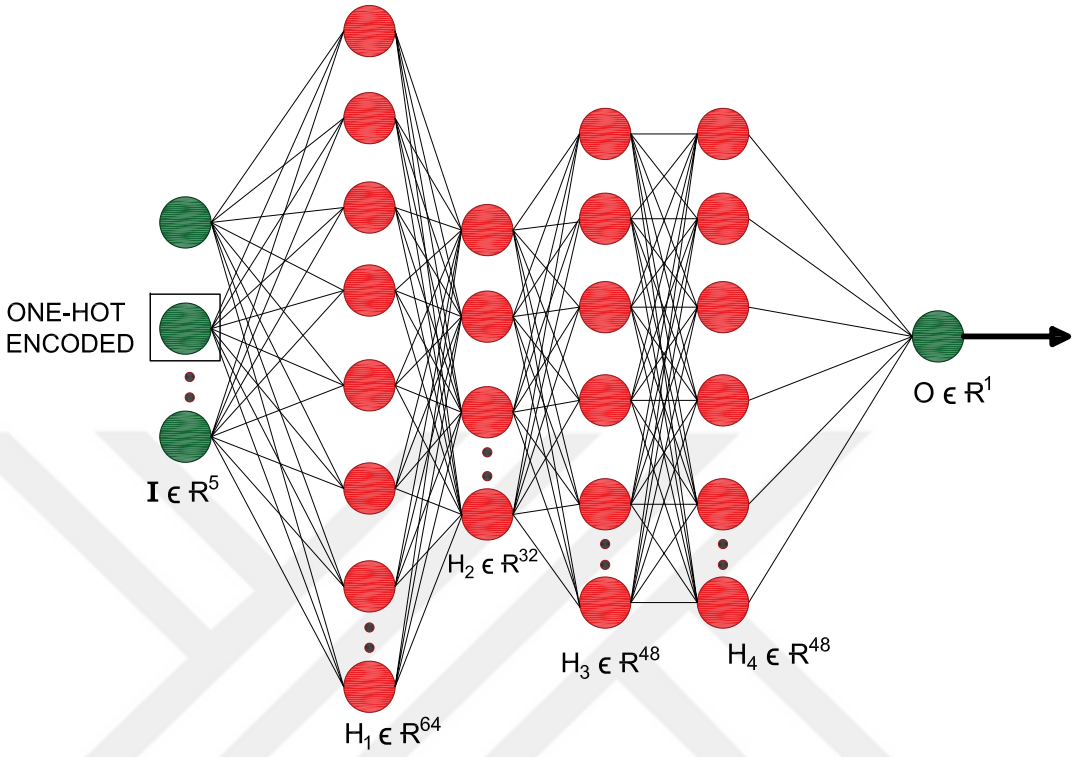


Figure 10: DNN with five features and four fully connected hidden layers with 64, 32, 48, 48 units, respectively, and utilizing the Rectified Linear Unit (ReLU).

4.2 Evaluation Method

We train the model using the adaptive moment estimation (Adam) optimizer [44] and use the mean squared error (MSE) as our cost function

$$MSE = \frac{1}{n}\sum_{i=0}^{n-1}\left(y_{\text{pred}}^{(i)} - y^{(i)}\right)^2 \tag{4.3}$$

where n is the number of samples and $y_{pred}^{(i)}$, $y^{(i)}$ are respectively the predicted value and the actual value corresponding to the i^{th} sample. In the training, we adopt early stopping [45] with a learning rate schedule to prevent divergence and to reduce the learning time. In addition, we use model checkpointing [46] to save the best-performing model during training.

Table 2: System and Channel Parameters

Parameter	Definition	Numerical Value
p	Photon power	1W
λ	Wavelength	532 nm [29]
I_{dc}	Dark current count rate	60 Hz [29]
$\Delta\lambda$	Filter spectral width	30 nm [29]
K_∞	Asymptotic diffuse attenuation coefficient	0.08 m^{-1} [43]
z_d	Depth	100 m [29]
$R_d(\lambda,0)$	Irradiance of the underwater environment at sea surface	$10^{-3}\,W/m^2$ [29]
r_0	Transmitter beam width	3, 6 mm
$\theta_{0,\max}$	Maximum beam divergence	20°, 30°
A	Receiver aperture diameter	10, 20, 30 cm
L	Link length	5, 10, 15, 20, 25, 30, 35, 40 m
ζ	Extinction coefficient (water type: Pure sea, Clear ocean, Coastal water, Harbor water)	0.056, 0.15, 0.305, 2.17 m^{-1} [36]

To describe the goodness of our model, we consider the R-squared criterion [47]

$$R^2 = 1 - \frac{\sum_{i=0}^{n-1}\left(y^{(i)} - y_{\text{pred}}^{(i)}\right)^2}{\sum_{i=0}^{n-1}\left(y^{(i)} - \bar{y}\right)^2} \tag{4.4}$$

where $\bar{y}$ represents the mean value of labels $y^{(i)}$, i=0,1... N-1. This is upper bounded by unity which is reached in the case of fitting a perfect model. The R-squared criterion is unable to check the bias in the model and is typically utilized in conjunction with residual plots [47] for model evaluation. A residual is a measure of the vertical deviation of dependent variables from the prediction model and can be calculated as $r = y - y_{pred}$. To estimate the probability density function (PDF) of residuals and obtain smoothed representation of histogram shape of residuals, we employ kernel density estimation (KDE) as

$$\widehat{f}(r) = \frac{1}{nh}\sum_{i=0}^{n-1} k\left(\frac{r - r^{(i)}}{h}\right) \tag{4.5}$$

where h is smoothing parameter and k is a Gaussian kernel function given by

$$k(x) = \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{x^2}{2}\right) \tag{4.6}$$

4.3 Generalization Assessment

During the training process, we accounted for all the different water types introduced in [37], ensuring our model's adaptability to various underwater environments. Through the Monte Carlo simulations, we made a significant observation: the majority of photons fail to reach the receiver plane for link distances larger than L=40 meters, leading to a near elimination of system performance. Consequently, the trained model can be described as a generalized model for channel parameters, effectively predicting bit time and FoV within the specified range of beam width, beam divergence, and receiver aperture diameter. The joint effect of channel parameters, i.e., link length and water type, within the considered range of parameters emerge as more influential factor in determining bit time and FoV. Therefore, the few numbers of values considered for each system parameter, namely beam width, beam divergence, and receiver aperture diameter, along with the inclusion of all different water types and frequent variations in link length with small intervals between values (5 meters intervals), will allow for extracting the variation in dependent variables across various new scenarios within the predefined ranges. However, it is essential to acknowledge the restriction of the model when considering values outside the training range of system parameters. Such deviations may introduce errors in predicting bit time and FoV, and the severity of these errors depends on the extent of deviation from the training range.

CHAPTER V

OPTIMIZATION RESULTS

In our simulation study, we generate $5 * 10^7$ photons that travel from the transmitter to the receiver through the underwater channel. For each scenario, we consider the interdependency of bit time and FoV and analyze the joint effect of them on the QBER performance to determine their appropriate values.

As the first example, we consider a scenario where we assume coastal water, $\theta_{0,\max}$ =20°, r_0=3 mm, and A =20 cm. In order to highlight the tradeoff between ISI and noise, we investigate the propagation delay of received photons for various link distances. Fig. 11 presents the CDF of received photons for L=10, 20, 30, and 40 meters under the assumption of using a FoV of Ω=180°. It is observed that propagation times for 99% of the received photons for link lengths of L=10, 20, 30, and 40 m, are respectively Δt =0.11, 0.68, 1.7, and 3.3 nanoseconds (ns). By increasing the threshold from the 99% to the 99.9%, the required bit time values increase to Δt=0.8, 3.5, 7.5, and 10.5 ns. Determining the bit time based on the threshold of 99.9% of photons instead of 99% of photons can reduce the probability of ISI occurrences. However, the significant increase in the bit time leads to much higher dark noise.

In our above example, we consider FoV of $\Omega = 180°$ to account for the worst case of ISI. In Fig.4, we illustrate the influence of both the bit time and the FoV on the reception count and the occurrences of ISI for a link length of L = 40 m. It is evident from Fig. 12(a) that by increasing the bit time, the count of received photons (see Fig. 12(b)) increases as the ISI decreases. As expected, increasing the FoV also increases the number of received photons. However, after a certain value of FoV, the number of received photons decreases as the count of ISI increases. For example, consider a bit time of $\Delta t = 0.05$ ns. It is observed from

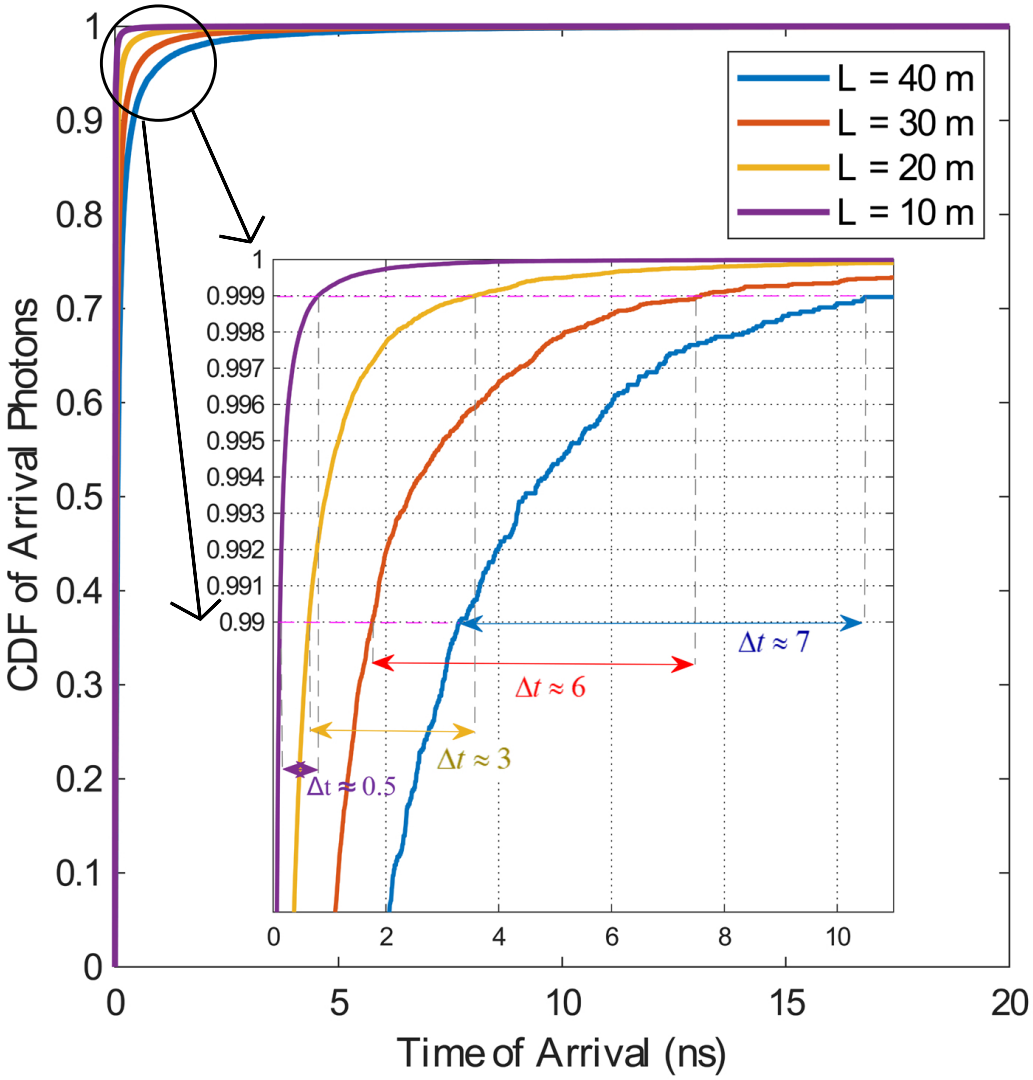


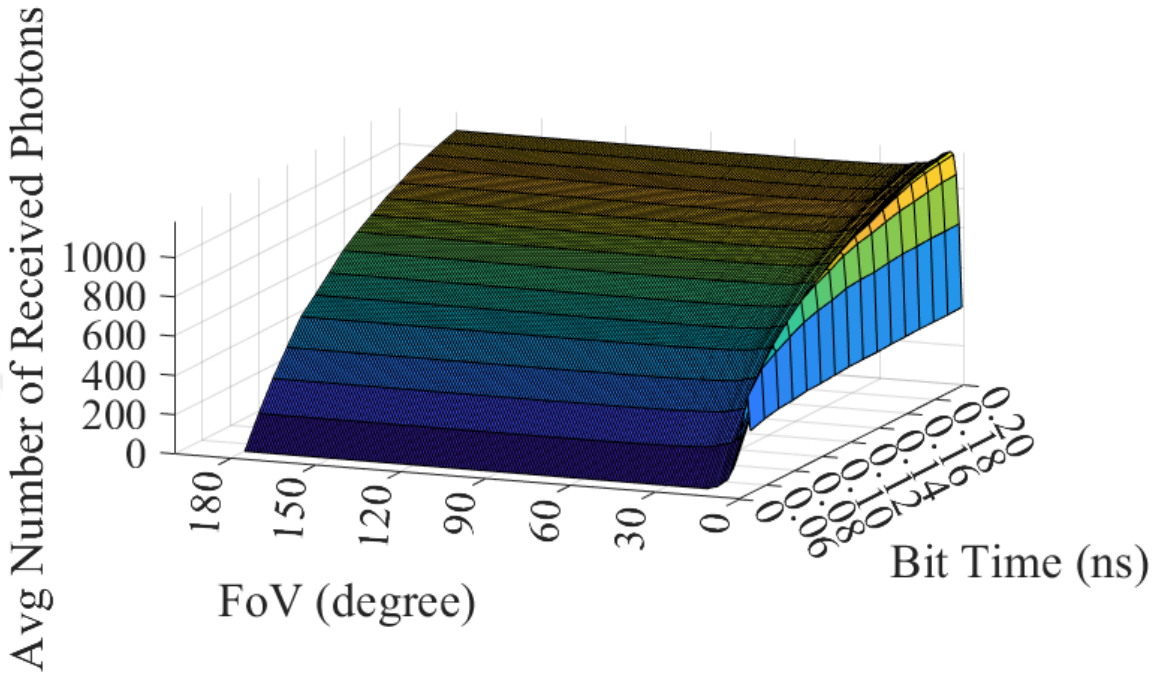
Figure 11: CDF of arrival photons versus time of arrival.

Fig. 12(a) that the maximum number of received photons is 482 and achieved with a FoV of $\Omega = 2^{\circ}$. However, with a further increase in FoV, the reception count steadily declines, ultimately reaching zero at a FoV of $\Omega = 10^{\circ}$. The decrease in photon reception with an increase in FoV can be explained by referring to Fig. 12(b). Due to the short bit time of $\Delta t = 0.05$ns considered in this example, the system experiences high ISI. Expanding the FoV for this particular bit time leads to more photons reaching the receiver plane, and this results in increase of ISI, ultimately corrupting all received photons at the FoV of

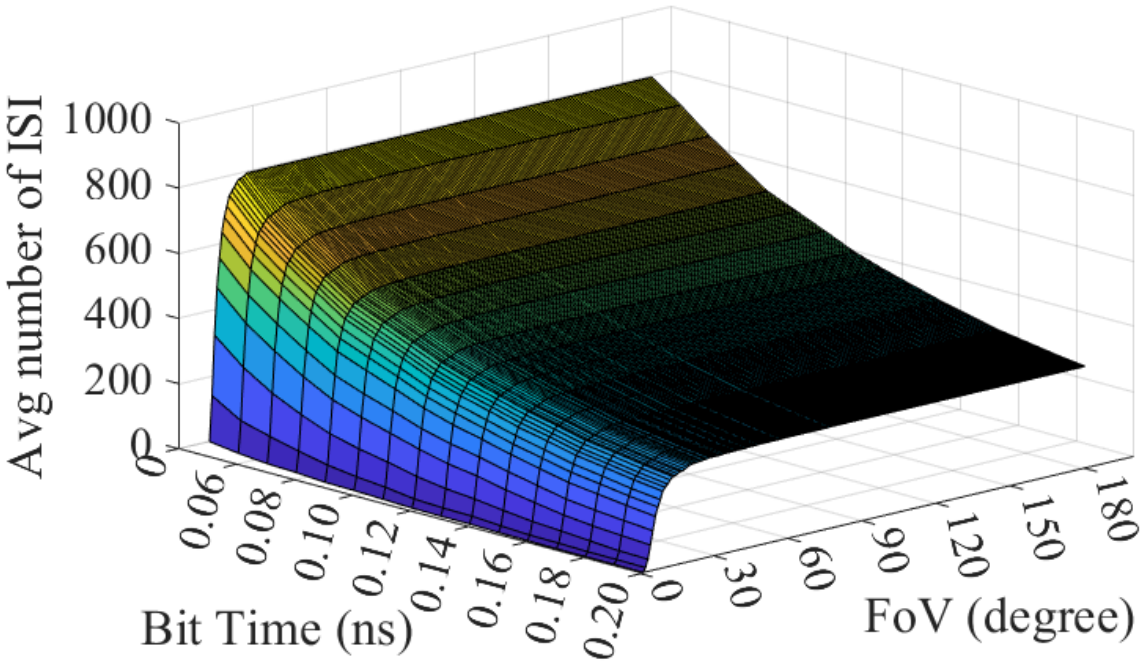
$\Omega = 10^{\circ}$. In summary, increasing the FoV necessitates the selection of a longer bit time value. However, failing to properly adjust the bit time when expanding the FoV leads to a rise in ISI levels, potentially causing the system performance to deteriorate to the point of non-functionality.

In Fig. 13, we illustrate the combined effect of bit time, FoV, and gate time on the QBER performance while the ISI is taken into account. We assume a link length of L = 40 m. For each selected bit time and FoV, the optimized gate time is determined through the exhaustive search and is used to calculate the corresponding QBER. The interdependency of optimum bit time and FoV values can be realized by assessing the figure. For example, for a $\Omega = 1^{\circ}$, the optimum bit time (in sense of QBER minimization) is $\Delta t = 0.05$ ns. For a FoV of $\Omega = 10^{\circ}$, the optimum bit time shifts to $\Delta t = 0.13$ ns. For $\Delta t = 0.05$ ns, increasing the FoV significantly reduces the number of received photons as a result of ISI, and the QBER reaches around 0.046 for $\Omega = 180^{\circ}$. This implies that the system requires a larger bit time if a larger FoV will be selected to avoid performance degradation. The red circle in the figure indicates the optimal point where the joint selection of bit time and FoV results in the minimum QBER. The bit time and FoV corresponding to this optimal point are $\Delta t = 0.06$ ns and $\Omega = 2^{\circ}$, respectively, and the corresponding minimum QBER value is 1.25×10^{-4}.

In Fig. 14, we present the QBER as a function of gate time and provide a comparison of the achieved performance in our study with that reported in [33] for various link distances. Note that the attained QBER values in [33] for link lengths of L=10, 20, 30, and 40 meters, are respectively 8.4×10^{-6}, 2.5×10^{-4}, 2.2×10^{-3}, and 1.0×10^{-2}. In our case, for the same link lengths, we achieve QBER values of 5×10^{-7}, 3.8×10^{-6}, 2.1×10^{-5}, and 1.2×10^{-4}, respectively indicating significant improvements up to 2 order magnitudes. Specifically, in our study, we are able to transmit a larger proportion of photons in a shorter time interval with judicious choices of bit time and FoV, thereby



(a)



(b)

Figure 12: Effect of bit time and FoV on the a) average number of received photons, b) average number of ISI.

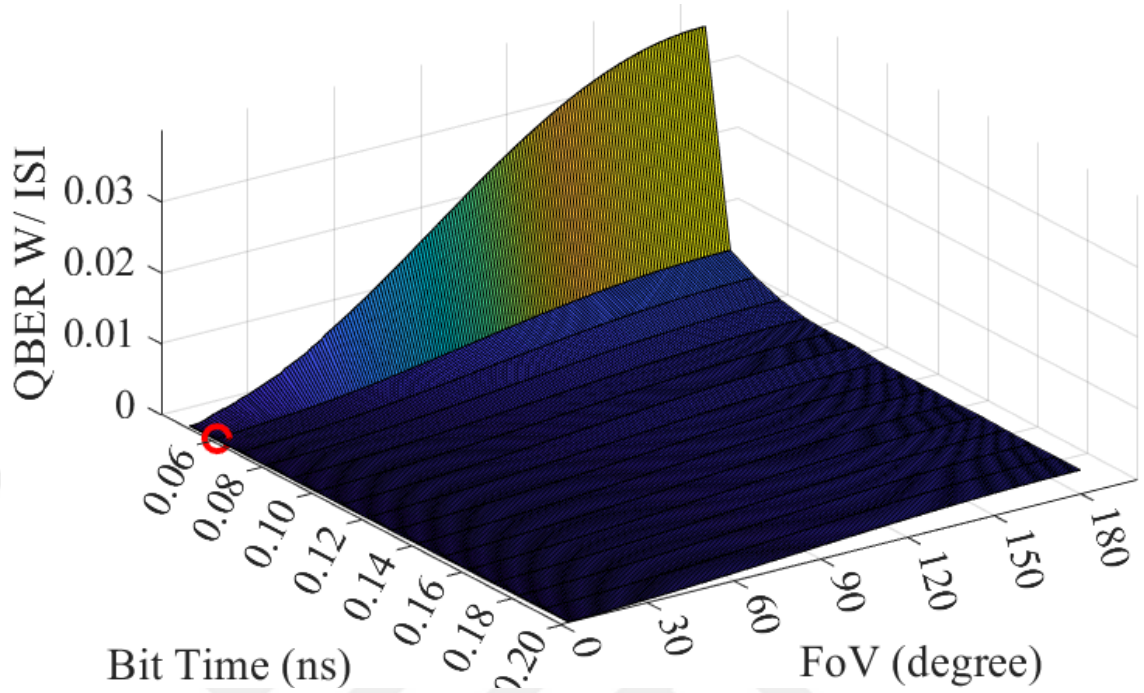


Figure 13: QBER versus bit time and FoV for optimized gate time.

significantly enhancing the system's efficiency. Specifically, in our study, we use optimized bit times of Δt =0.05, 0.05, 0.05, and 0.06 ns for link lengths of L =10, 20, 30, and 40 meters. The corresponding dark current noise for $I_{dc} = 60$ Hz are calculated as $n_D = 3 \times 10^{-9}$, 3×10^{-9}, 3×10^{-9}, and 3.6×10^{-9}. The irradiance background noise with the optimized FoVs of $\Omega = 4^\circ$, 3°, 3°, and 2° and optimized gate time values of $\Delta t' = 28,\ 50,\ 50$, and 60 picoseconds can be further calculated as $n_B = 9 \times 10^{-11}$, 9.1×10^{-11}, 9.1×10^{-11}, and 4.85×10^{-11}, respectively, for L =10, 20, 30, and 40 meters. In comparison, the utilized bit times in [33] are Δt =0.8, 3.5, 7.5, and 10.5 nanoseconds for the corresponding link lengths. The dark current noise levels for $I_{dc} = 60$ Hz are measured as $n_D = 4.8 \times 10^{-8}$, 2.1×10^{-7}, 4.5×10^{-7}, and 6.3×10^{-7} in [33] while the irradiance background noise are $n_B = 3.3 \times 10^{-9}$, 2.2×10^{-8}, 7.3×10^{-8}, and 1.3×10^{-7}. In comparison to [33], it is observed that our judiciously selected values of bit time result in significant reductions of the dark current noise and irradiance background noise values eventually leading to a better QBER performance.

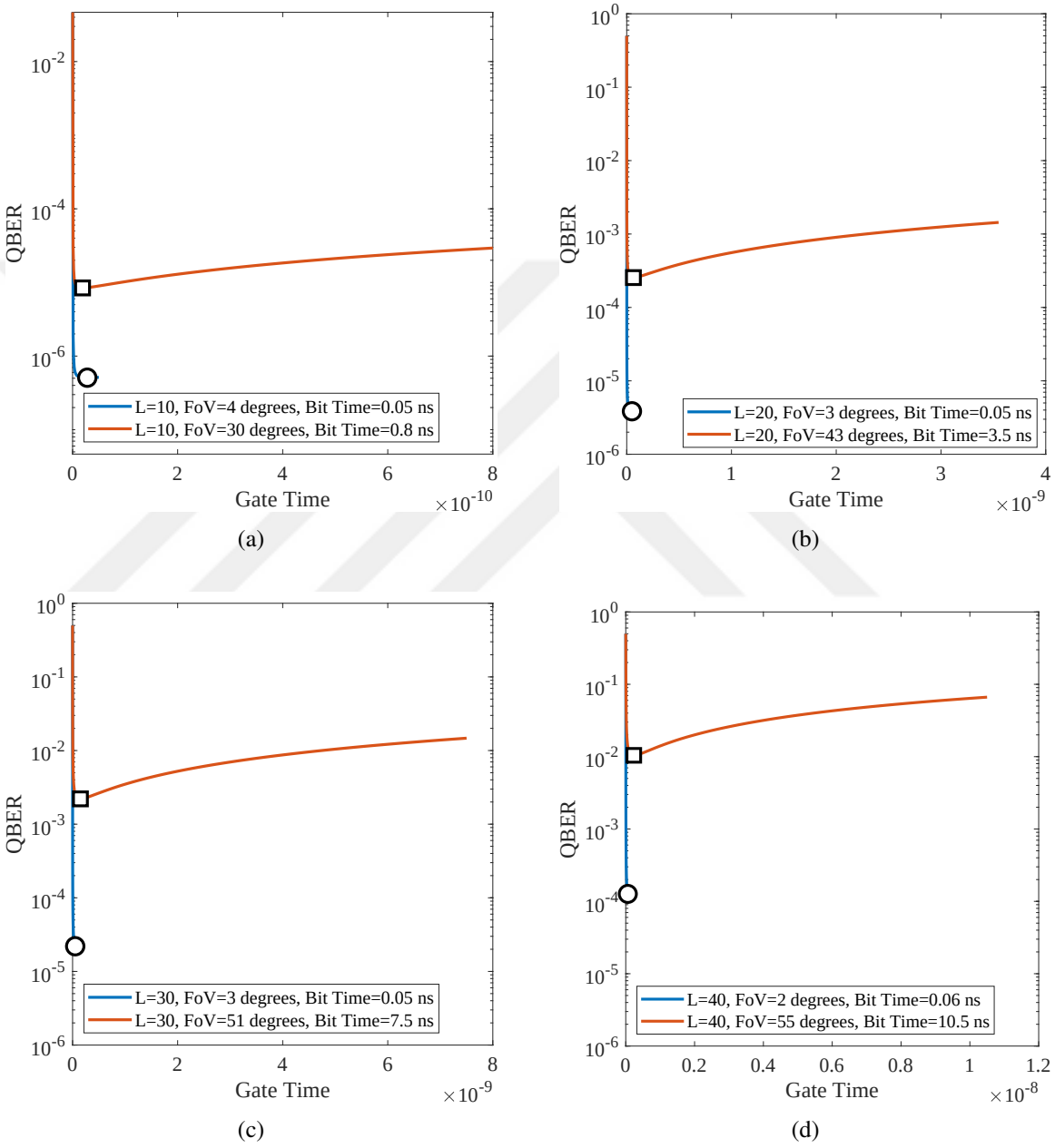


Figure 14: QBER performance with respect to the gate time for link distances of a) L = 10 m, b) L = 20 m, c) L = 30 m and d) L = 40 m.

The optimization process described up to here is applied for each of the samples in the dataset and corresponding values of bit time and FoV are recorded for the training process of DNN. The optimization resolution for the bit time is set at 1 picosecond, and for the FoV, it is $\frac{\pi}{4}$. In Fig.15(a) and Fig.15(b), we depict MSE with respect to epochs for bit time and FoV, respectively. Our model achieves an average MSE value of less than 1.5 for bit time, and 0.5 for FoV on the test data. The overall behavior of MSE curve illustrates the efficiency of the deep learning model without experiencing overfitting or high bias. The slight fluctuations in the curves are as a result of utilizing mini-batch gradient descent. Furthermore, the R-squared criterion reaches above 0.99 for both bit time and FoV. This indicates that the model is estimated to capture 99% of variation in the dependent variables and is therefore able to effectively explain the underlying relationship between variables. Fig.15(c) and Fig.15(d) illustrate the associated residual plots. These demonstrate that the variance of residuals from the fitted model is around 0.77 picoseconds for the bit time and $0.15 \cdot \frac{\pi}{4}$ for the FoV. Finally, Fig.15(e) and Fig.15(f) present the PDF of residuals. They demonstrate that the density of residuals around zero is high and the residuals approximate the normal distribution in both cases.

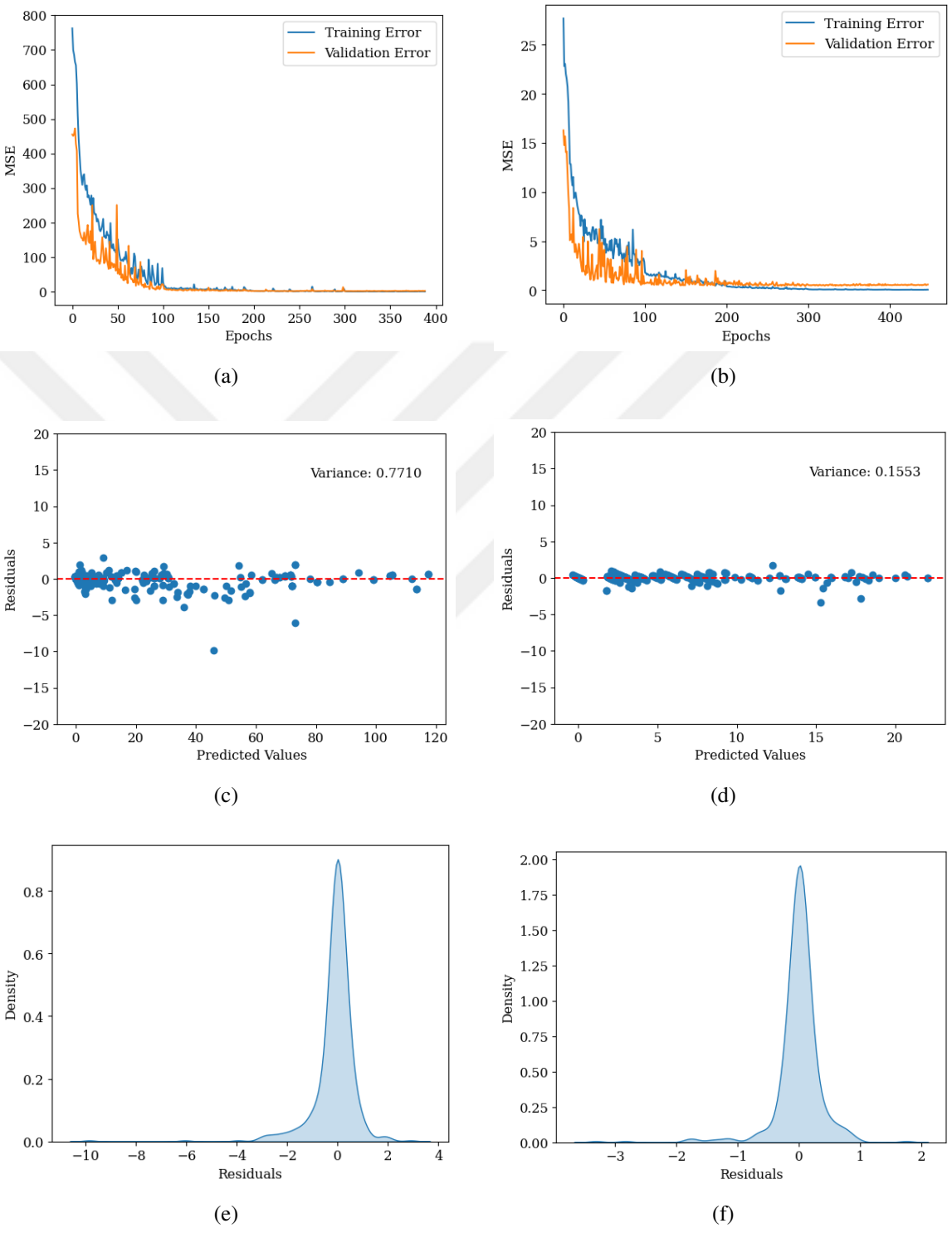


Figure 15: a) MSE with respect to epochs for bit time , b) MSE with respect to epochs for FoV, c) Residual plot for bit time, d) Residual plot for FoV, e) Density plot of residuals for bit time, f) Density plot of residuals for FoV.

CHAPTER VI

CONCLUSIONS

In this study, we have investigated the impact of bit time, FoV, and gate time on the QBER performance of an underwater QKD system in the presence of ISI. The optimal bit time was selected with the goal of minimizing QBER based on the propagation delay taking into account the interdependency between bit time and FoV. To determine FoV based on the AoA, we explored various thresholds on the average number of received photons to strike a balance between the number of photon arrivals and background noise, aiming to reduce the QBER. In other word, during the optimization process, we carefully weigh the benefits of considering a higher percentage of photon reception against the potential drawbacks of longer required reception times and a larger FoV to achieve best QBER performance. Finally for the selected values of bit time and FoV and a given propagation environment, we optimized the SPAD gate time in terms of minimizing the QBER. For optimization purposes, we built a dataset to leverage on-board deep learning techniques to instantly predict optimal bit time and FoV for a given set of system parameters and propagation environment. Our results indicate that conducting interdependency analysis between parameters and considering background photons during the optimization process leads to significant improvements in QBER.

REFERENCES

[1] F.-Y. Lu, Z.-Q. Yin, C. Wang, C.-H. Cui, J. Teng, S. Wang, W. Chen, W. Huang, B.-J. Xu, G.-C. Guo, *et al.*, "Parameter optimization and real-time calibration of a measurement-device-independent quantum key distribution network based on a back propagation artificial neural network," *JOSA B*, vol. 36, no. 3, pp. B92–B98, 2019.

[2] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Physical review letters*, vol. 85, no. 2, p. 441, 2000.

[3] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum internet," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3808–3833, 2020.

[4] B. Schumacher, "Quantum coding," *Physical Review A*, vol. 51, no. 4, p. 2738, 1995.

[5] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, and A. K. Mishra, "Quantum key distribution secured optical networks: A survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2049–2083, 2021.

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

[7] I. B. Djordjevic and I. B. Djordjevic, "Discrete variable (dv) qkd," *Physical-layer security and quantum key distribution*, pp. 267–322, 2019.

[8] T. C. Ralph, "Continuous variable quantum cryptography," *Physical Review A*, vol. 61, no. 1, p. 010303, 1999.

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

[10] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical review letters*, vol. 88, no. 5, p. 057902, 2002.

[11] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Physical review letters*, vol. 89, no. 3, p. 037902, 2002.

[12] C. H. Bennett, G. Brassard, *et al.*, "Proceedings of the ieee international conference on computers, systems and signal processing," 1984.

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

[14] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical review letters*, vol. 92, no. 5, p. 057901, 2004.

[15] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130503, 2012.

[16] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.

[17] D. Mayers, "Unconditional security in quantum cryptography," *Journal of the ACM (JACM)*, vol. 48, no. 3, pp. 351–406, 2001.

[18] P. V. Trinh, A. T. Pham, A. Carrasco-Casado, and M. Toyoshima, "Quantum key distribution over fso: Current development and future perspectives," in *2018 Progress in Electromagnetics Research Symposium (PIERS-Toyama)*, pp. 1672–1679, IEEE, 2018.

[19] C. Wang and A. Rahman, "Quantum-enabled 6g wireless networks: Opportunities and challenges," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 58–69, 2022.

[20] S.-C. Zhao, X.-H. Han, Y. Xiao, Y. Shen, Y.-J. Gu, and W.-D. Li, "Performance of underwater quantum key distribution with polarization encoding," *JOSA A*, vol. 36, no. 5, pp. 883–892, 2019.

[21] M. Lanzagorta and J. Uhlmann, "Assessing feasibility of secure quantum communications involving underwater assets," *IEEE Journal of Oceanic Engineering*, vol. 45, no. 3, pp. 1138–1147, 2019.

[22] Y. Guo, C. Xie, P. Huang, J. Li, L. Zhang, D. Huang, and G. Zeng, "Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution," *Physical Review A*, vol. 97, no. 5, p. 052326, 2018.

[23] J. Gariano and I. B. Djordjevic, "Theoretical study of a submarine to submarine quantum key distribution systems," *Optics express*, vol. 27, no. 3, pp. 3055–3064, 2019.

[24] A. H. F. Raouf, M. Safari, and M. Uysal, "Performance analysis of quantum key distribution in underwater turbulence channels," *JOSA B*, vol. 37, no. 2, pp. 564–573, 2020.

[25] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, E. Karimi, *et al.*, "Quantum cryptography with twisted photons through an outdoor underwater channel," *Optics express*, vol. 26, no. 17, pp. 22563–22573, 2018.

[26] F. Hufnagel, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, B. J. Sussman, R. W. Boyd, G. Leuchs, *et al.*, "Characterization of an underwater channel for quantum communications in the ottawa river," *Optics express*, vol. 27, no. 19, pp. 26346–26354, 2019.

[27] A. H. F. Raouf, M. Safari, and M. Uysal, "Performance analysis of decoy state quantum key distribution over underwater turbulence channels," *JOSA B*, vol. 39, no. 6, pp. 1470–1478, 2022.

[28] J. Gariano, I. B. Djordjecvic, and Y. Xiang, "Simulation of a submarine to submarine qkd system," in *Quantum Information Science and Technology IV*, vol. 10803, pp. 14–21, SPIE, 2018.

[29] W. Zhao, R. Shi, X. Ruan, Y. Guo, Y. Mao, and Y. Feng, "Monte carlo-based security analysis for multi-mode continuous-variable quantum key distribution over underwater channel," *Quantum Information Processing*, vol. 21, no. 5, p. 186, 2022.

[30] A. H. F. Raouf, M. Safari, and M. Uysal, "Multi-hop quantum key distribution with passive relays over underwater turbulence channels," *JOSA B*, vol. 37, no. 12, pp. 3614–3621, 2020.

[31] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, "Advances in ingaas/inp single-photon detector systems for quantum communication," *Light: Science & Applications*, vol. 4, no. 5, pp. e286–e286, 2015.

[32] S. Jiang, W. O. Popoola, and M. Safari, "Quantum key distribution using time-gated spads over turbid underwater channels," in *CLEO: Applications and Technology*, pp. JW1A–125, Optica Publishing Group, 2021.

[33] A. H. F. Raouf and M. Uysal, "On the optimization of underwater quantum key distribution systems with time-gated spads," *JOSA B*, vol. 39, no. 8, pp. 2013–2019, 2022.

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

[35] R. J. Urick, *Principles of Underwater Sound 3rd Edition*. Peninsula, 1996.

[36] M. Lanzagorta, *Underwater communications*. Morgan & Claypool Publishers, 2012.

[37] C. Gabriel, M.-A. Khalighi, S. Bourennane, P. Léon, and V. Rigaud, "Monte-carlo-based channel characterization for underwater optical communication systems," *Journal of Optical Communications and Networking*, vol. 5, no. 1, pp. 1–12, 2013.

[38] C.-Q. Hu, Z.-Q. Yan, J. Gao, Z.-Q. Jiao, Z.-M. Li, W.-G. Shen, Y. Chen, R.-J. Ren, L.-F. Qiao, A.-L. Yang, *et al.*, "Transmission of photonic polarization states through 55-m water: towards air-to-sea quantum communication," *Photonics Research*, vol. 7, no. 8, pp. A40–A44, 2019.

[39] V. I. Haltrin, "Two-term henyey-greenstein light scattering phase function for seawater," in *IEEE 1999 International Geoscience and Remote Sensing Symposium. IGARSS'99 (Cat. No. 99CH36293)*, vol. 2, pp. 1423–1425, IEEE, 1999.

[40] B. Liu and B. Liu, "Supervised learning," *Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data*, pp. 63–132, 2011.

[41] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," *nature*, vol. 323, no. 6088, pp. 533–536, 1986.

[42] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[43] Z.-P. Lee, K.-P. Du, and R. Arnone, "A model for the diffuse attenuation coefficient of downwelling irradiance," *Journal of Geophysical Research: Oceans*, vol. 110, no. C2, 2005.

[44] D. P. Kingma, J. Ba, Y. Bengio, and Y. LeCun, "3rd international conference on learning representations, iclr 2015, san diego, ca, usa, may 7-9, 2015, conference track proceedings," *arXiv preprint arXiv:1412.6980*, 2015.

[45] L. Prechelt, "Early stopping-but when?," in *Neural Networks: Tricks of the trade*, pp. 55–69, Springer, 2002.

[46] A. Gulli and S. Pal, *Deep learning with Keras*. Packt Publishing Ltd, 2017.

[47] R. Christensen, *Log-linear models and logistic regression*. Springer Science & Business Media, 2006.

VITA

Mostafa Nozari joined the Communication Theory and Technologies (CT&T) Research Group at Ozyegin University, Istanbul, Turkey, in 2021 as a research assistant under the guidance of Prof. Dr. Murat Uysal. Prior to this affiliation, he was a student at Isfahan University of Technology (IUT), studying telecommunication engineering. His research pursuits center around wireless communication/networks and machine learning (ML).