Spring 5-8-2024

Evaluating the effect of noise on Secure Quantum Networks

Karthick Anbalagan
kanbalag@students.kennesaw.edu

Evaluating the effect of noise on Secure Quantum Networks

Karthick Anbalagan

A report submitted as part of the requirements for the degree

of Masters of Science in Computer Science

at the College of Computing and Software Engineering

Kennesaw State University

Georgia, United States of America

May 2024

Advisor: Dr. Abhishek Parakh

Committee Members:

Dr. Manohar Raavi

Dr. Kazi Aminul Islam

Declaration

I confirm that the work contained in this master's thesis project report has been composed solely by myself and has not been accepted in any previous application for a degree. All sources of information have been specifically acknowledged, and all verbatim extracts are distinguished by quotation marks.

***Signed* :** Karthick Anbalagan ***Date* :** 05/08/2024

Consent of Circulation

In presenting this thesis as a partial fulfillment of the requirements for an advanced degree from Kennesaw State University, I agree that the university library shall make it available for inspection and circulation in accordance with its regulations governing materials of this type. I agree that permission to copy from, or to publish, this thesis may be granted by the professor under whose direction it was written, or, in his absence, by the dean of the appropriate school when such copying or publication is solely for scholarly purposes and does not involve potential financial gain. It is understood that any copying from or publication of, this thesis which involves potential financial gain will not be allowed without written permission.

***Signed* :** Karthick Anbalagan ***Date* :** 05/08/2024

Dedications

I dedicate my thesis to my wife Aarthi and my son Saghan whose unwavering support, inspiration and love has been my constant strength and beacon throughout this journey.

Acknowledgements

I am profoundly grateful for the guidance and assistance provided by my advisor, Dr. Abhishek Parakh, whose insights and direction were invaluable throughout this research journey. His expertise and unwavering support have been cornerstone elements in the completion of this thesis.

I would also like to extend my heartfelt thanks to Nitin Jha, a friend and doctoral candidate, who played a significant role in the development of this document. His assistance in various sections of this thesis and his ability to elucidate the complexities of quantum theory have been instrumental in enhancing my understanding and shaping the outcome of this research.

Their combined contributions have not only enriched my academic experience but have also been pivotal in achieving the goals of this study.

Abstract

This thesis focuses on examining the resilience of secure quantum networks to environmental noise. Specifically, we evaluate the effectiveness of two well-known quantum key distribution (QKD) protocols: the Coherent One-Way (COW) protocol and Kak's Three-Stage protocol (Kak06). The thesis systematically evaluates these protocols in terms of their efficiency, operational feasibility, and resistance to noise, thereby contributing to the progress of secure quantum communications.

Using simulations, this study evaluates the protocols in realistic scenarios that include factors such as noise and decoherence. The results illustrate each protocol's relative benefits and limitations, highlighting the three-stage protocol's superior security characteristics, resistance to interference, and the COW protocol's efficient functioning and compatibility with extensive fiber networks.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

QKD, or quantum key distribution, is likely to become a mainstay in the field of secure communications, providing integrity and confidentiality of data transferred over potentially compromised channels. QKD is built on the principles of quantum mechanics, in contrast to conventional cryptography methods that rely on the presumptive difficulty of specific mathematical problems. Bennett and Brassard first proposed a QKD protocol in 1984, radically changing the field of secure communications [2].

QKD uses qubits, which is a quantum counterpart of the classical bit. Unlike classical bits, which can only exist in one state at a time, qubits can exist in superposition of states. Similarly, quantum entanglement allows two qubits to be coupled in a way that allows the state of one to instantly affect the other, regardless of the distance between them. Lastly, the no-cloning property of qubits prevents copying of unknown qubits and protects the key exchange from the eavesdropper [28].

QKD protocols have undergone a substantial evolution, with numerous schemes created to address the complexities of resource efficiency, operational simplicity, and security enhancement. These protocols have been tested on a variety of communication channels, including fiber optics, free-space links, and even underwater channels, demonstrating the feasibility of quantum communication over extended distances. Quantum cryptography has proven to be robust and feasible in the real world through the practical application of these protocols in large-scale networks, as demonstrated by projects such as the DARPA quantum network [21, 44, 45].

A critical aspect of quantum communication that has attracted extensive research is the influence of environmental noise on the integrity and security of QKD systems. Noise in quantum networks can negatively impact the quantum states used for information transmission, potentially resulting in errors in the key distribution process. Noise can originate from a variety of sources, including photon loss, equipment flaws, and external environmental factors. For quantum communication channels to be reliable and secure, it is critical to comprehend and mitigate the effects of noise [51, 63].

The main focus of this study is a thorough comparison of the Coherent One-Way (COW) protocol and Kak's Three-Stage protocol (Kak06), two well-known QKD protocols. The effectiveness of these protocols in long-distance communication is examined with a focus on their operational viability and noise resilience. The Kak06 protocol is known for its practicality, security, and resilience to different kinds of noise, whereas the COW protocol is well-known for its efficient operation and efficacy across large fiber networks. In the current context of quantum communication, this study attempts to clarify which protocol offers superior performance and reliability, which is crucial for the development of secure quantum networks.

The thesis aims to advance the field of quantum cryptography by carrying out this thorough analysis with the goal of optimizing QKD protocols for widely-used and secure quantum networks. It is anticipated that this investigation will provide important information for the strategic planning of international quantum communication networks, equipping them to resist the sophisticated risks associated with technological progress and the impending arrival of quantum computing [2, 12, 13].

1.1 About this Thesis

This is the thesis of *Karthick Anbalagan*, submitted as part of the requirements for the degree of Master of Science in Computer Science at the College of Computing and Software Engineering, Kennesaw State University, USA.

Several paragraphs detail the main expectations of this body of work.

1.2 Chapter List

A list of all chapters within the thesis and a brief summary of the content are provided below.

Chapter 2 Quantum Networking Basics. This chapter explores the fundamental elements of quantum networking, beginning with the concept of qubits, which are the quantum equivalent of classical bits. Qubits possess the remarkable property of superposition, enabling them to exist in multiple states simultaneously. This chapter explores deeper into qubit-vector algebra, a crucial aspect of quantum computing and information theory. Provides a comprehensive explanation of the mathematical framework that allows for the representation and manipulation of qubits. The chapter discusses the application of qubits, the fundamentals of qubit-vector algebra, and the practical considerations of quantum key distribution (QKD). It highlights the importance of secure communication methods such as QKD, as classical public key distribution systems are susceptible to potential vulnerabilities.

Chapter 3 Network Simulation Design. Chapter 3 presents the SeQUeNCe simulator [61], which is a tool used for modeling and analyzing quantum communication networks. It emphasizes the ability of the simulator to accurately simulate quantum channels, protocols, and network behaviors. The chapter explores the implementation of different network topologies such as point-to-point, ring, grid, and torus, along with their respective benefits and drawbacks. The chapter ends by presenting the simulation design for the COW and Kak06 protocols, offering valuable information on the practical aspects of simulating quantum key distribution.

Chapter 4 Results. This chapter provides an overview of the project's findings, with a specific focus on data processing, the implementation of the COW and Kak06 protocols. The Savitzky-Golay filter is used to reduce noise in resulting graphs due to challenges faced during large-scale simulations, including long execution times and memory constraints. The chapter provides a detailed examination of the COW and Kak06 protocols, focusing on their practicality and ability to withstand interference in quantum communications.

Chapter 5 Future Works. Chapter 5 focuses on exploring future research directions and potential improvements to the current quantum key distribution protocols and network designs. Additional investigation is required to enhance the optimization of these protocols for practical use and to enhance the efficiency and security of quantum networks. The chapter proposes a strategic plan to progress quantum communication technologies and incorporate them into practical applications.

Chapter 6 Conclusion. The conclusion chapter provides a brief summary of the primary findings presented in the thesis, emphasizing the significance of quantum key distribution in securing communications within quantum networks. This chapter highlights the importance of advanced simulation tools in advancing the field of quantum cryptography by discussing the insights gained from simulation studies and comparative analysis of various QKD protocols.

Chapter 2

Quantum Networking Basics

2.1 What are Qubits?

Qubits, also known as quantum bits, are the basic components of quantum information, serving as the quantum equivalent of classical bits. Qubits, unlike classical bits, can exist in a superposition of both the 0 and 1 states simultaneously, whereas classical bits are purely binary and can only be in either the 0 or 1 state. The superposition principle enables a qubit to represent a multitude of potential states, reflecting the inherent probabilistic aspect of quantum mechanics. The state of a qubit is characterized as a vector in a two-dimensional Hilbert space, typically denoted using the Dirac notation, i.e., using the *bra-ket* notation. A quantum state in Dirac notation can be written as in eq(2.1)

$$\psi = \alpha|0\rangle + \beta|1\rangle, \tag{2.1}$$

where α and β are complex probability amplitudes associated with the states involved. The distinct attribute of qubits is the foundation for the increased computational capability of quantum computing, enabling the parallel processing of several potential results [59].

Quantum computers leverage the properties of qubits, such as duality and superposition, to solve problems with greater efficiency compared to classical computers. This advantage is particularly evident in domains such as encryption, complex system simulation, and optimization problems. The behavior of qubits is determined by the rules of quantum physics, such as entanglement and interference, which enable the development of intricate quantum algorithms. Qubits are essential in quantum key distribution (QKD) for securely communicating cryptographic keys. They utilize the features of quantum mechanics to detect any attempts of eavesdropping on the communication channel [59].

Qubits are implemented using different physical manifestations, such as the polarization of photons or energy levels of atoms. The management and alteration of these quantum states are crucial to the advancement and functioning of quantum computers and QKD systems, representing a notable deviation from the limited options of classical computing and communication systems. The study and application of qubits in technology play a crucial role in improving the field of quantum information science, pushing the limits of what can be accomplished in computing and secure communication [59].

2.2 Some Basics of Qubit-Vector Algebra

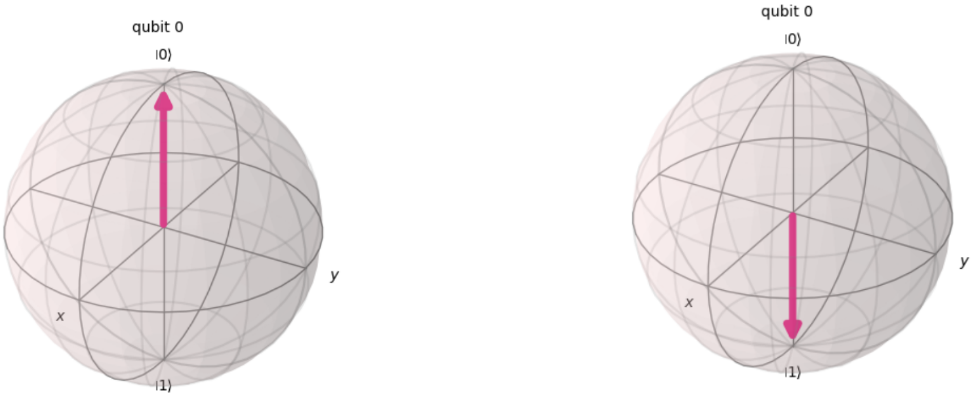
Qubit-vector algebra serves as the fundamental mathematical foundation for quantum computing and quantum information theory. It enables the description and manipulation of qubits. The qubit vector algebra is based on the use of complex numbers to represent the state of qubits in a multidimensional complex vector space [59]. In this space, each basis vector corresponds to a possible state of the qubit. This algebraic framework allows for the concise representation and calculation of quantum state evolutions and interactions, which are fundamental in executing quantum algorithms and processes.

The single qubit is represented by a basic form of qubit vector algebra, commonly expressed as eq(2.1), where α and β are complex coefficients. When squared, these coefficients represent the probabilities that the qubit is measured in state $|0\rangle$ or $|1\rangle$, respectively, and follow the constraint given in eq(2.2) when a quantum state is represented in the form given in eq(2.1).

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.2}$$

The utilization of linear superposition and complex probability amplitudes in their algebraic form allows for the intricate and probabilistic computational processes that are distinct to quantum computing.

2.2.1 Representation of a Qubit



(a) A qubit is created with Z basis

(b) A qubit is created with Z basis with a X gate applied

Figure 2.1: Quantum bits 0 and 1 in Bloch Sphere Representation [15]

Fig(2.1a and 2.1b)represents the visualization of quantum bits using the qiskit library developed by IBM [15] and it was written in Python.

2.2.2 Tensor Products

When moving to multi-qubit systems, we need to consider tensor products. Tensor products are mathematical operations in qubit-vector algebra that integrate the states of individual qubits to form the state of the entire system. In a two-qubit system, the combined state can be expressed as the tensor product of the individual qubit states, leading to a vector space with four dimensions. The basis for quantum entanglement and parallelism in quantum computing and QKD protocols are correlated quantum systems, which are described as entangled states when each qubit's quantum state cannot be described independently of the states of the other qubits. This expansion makes this possible [18].

Performing algebraic manipulations on these quantum states, such as unitary transformations and tensor products, is crucial for the design and comprehension of quantum algorithms, including those employed in QKD. Qubit-vector algebra is crucial in quantum information science since it allows us to accurately model and anticipate the behavior of complex quantum systems. This theoretical foundation not only facilitates the creation of new quantum technologies but also deepens our comprehension of the quantum world [9].

Below is the brief mathematical notation about tensor product [64].

Given two vector spaces V and V', we shall form the tensor product of two vector spaces, and denote it $V \otimes V'$. The tensor product is generated by the set of "tensors" of all vectors:

$$\{V \otimes V' \mid V \in V \text{ and } V' \in V'\},$$

where $\otimes$ is just a symbol. A typical element of $V \otimes V'$ looks like this:

$$c_0(V_0 \otimes V_0') + c_1(V_1 \otimes V_1') + \cdots + c_{p-1}(V_{p-1} \otimes V_{p-1}'),$$

where $V_0, V_1, \ldots, V_{p-1}$ are elements of V and $V_0', V_1', \ldots, V_{p-1}'$ are elements of V'. We might write this as

$$\sum_{i=0}^{p-1} c_i(V_i \otimes V_i').$$

The operations on this vector space are straightforward. For a given

$$\sum_{i=0}^{p-1} c_i(V_i \otimes V_i') \text{ and } \sum_{i=0}^{q-1} c_i(W_i \otimes W_i'),$$

addition is simply the addition of summations, i.e.,

$$\sum_{i=0}^{p-1} c_i(V_i \otimes V_i') + \sum_{i=0}^{q-1} c_i'(W_i \otimes W_i').$$

The scalar multiplication for a given $c \in \mathbb{C}$ is

$$c \cdot \sum_{i=0}^{p-1} c_i(V_i \otimes V_i') = \sum_{i=0}^{p-1} (c \times c_i)(V_i \otimes V_i').$$

We impose the following important rewriting rules for this vector space:

(i) The tensor must respect addition in both V and V':

$$(V_i + V_j) \otimes V_k' = V_i \otimes V_k' + V_j \otimes V_k',$$

$$V_i \otimes (V_j' + V_k') = V_i \otimes V_j' + V_i \otimes V_k'.$$

(ii) The tensor must respect the scalar multiplication in both V and V':

$$c \cdot (V_j \otimes V_k') = (c \cdot V_j) \otimes V_k' = V_j \otimes (c \cdot V_k').$$

Multiple qubits are represented as tensor products. For example, two qubits maybe represented using tensor notation as,

$$|00\rangle = |0\rangle \otimes |0\rangle$$

$$|11\rangle = |1\rangle \otimes |1\rangle$$

Representing Entangled Qubits

Entangled qubits refer to quantum states of multiple particles in which the individual quantum state of each particle cannot be described separately from the state of the other particles.

The Bell states (or EPR pairs) are widely recognized as some of the most prominent entangled states and play a fundamental role in quantum information theory. The Bell states for a pair of qubits are defined as:

$$|\phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\phi^{-}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\psi^{+}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\psi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

These states represent pairs of qubits that are completely entangled, meaning that the state of one qubit is instantaneously correlated with the state of the other qubit.

Another important instance of entangled states is the GHZ (Greenberger-Horne-Zeilinger) state, which extends the notion of entanglement to three or more qubits. The GHZ state for three qubits is a state that is defined as:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

2.3 Public Key Distribution

Public Key Distribution in classical cryptography [30] utilizes asymmetric key techniques, which require the use of two distinct but mathematically correlated keys - a public key openly communicated, and a private key kept confidential. The public key is employed for the encryption of messages, whereas the private key is utilized for their decryption. This approach facilitates the establishment of secure communication via unsecured channels without the necessity of transmitting the secret key through the same channel. Consequently, it solves the issue of distributing the key that poses a challenge to symmetric key cryptography.

The security of public key distribution is dependent on computational hardness assumptions, namely the difficulty of factoring huge integers (as employed in RSA) or calculating discrete logarithms (as utilized in Diffie-Hellman and elliptic curve cryptography). Nevertheless, these assumptions are vulnerable to the advancement of computational capabilities, such as a potential development of quantum computers in the future. These quantum computers could effectively solve these challenges and compromise the security of existing public key cryptosystems [11, 47, 56].

Fig(2.2) represents the public key distribution as represented in (Hellman et al. 1978).

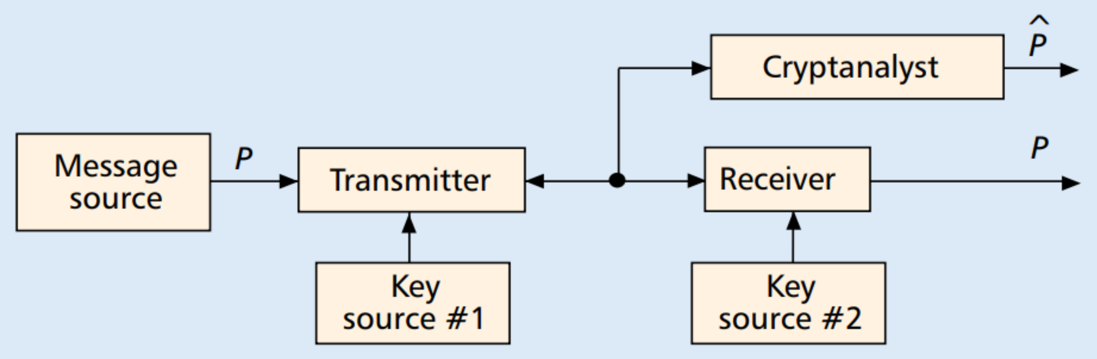


Figure 2.2: The image represents a secure communication process using asymmetric encryption between the sender and the receiver for transmitting a message. The sender uses public key of receiver to encrypt the message and the receiver uses his private key to decipher the message. The purpose of cryptanalysis is to intercept the encrypted message, thereby maintaining security in such systems. The objective of the cryptanalyst is to decipher the original message without having access to the private key employed for encryption [30]

Exploration of quantum key distribution (QKD) has arisen from the necessity for secure key distribution. QKD offers a theoretically secure approach to distribute keys by leveraging the laws of quantum physics. QKD's security is derived from the principles of physics instead of computing complexity, making it a strong alternative to conventional public key distribution methods. Given the potential risks posed by quantum computing, it is necessary for public-key distribution systems to adapt. Quantum key distribution (QKD) offers a practical approach to ensure secure communication in a future where quantum computing is prevalent.

2.4 Need for something better: Quantum Key Distribution

Quantum Key Distribution (QKD) represents a transformative approach to secure communications utilizing the fundamental principles of quantum mechanics. Unlike classical key distribution methods, QKD is unique because it is secured by the laws of physics rather than computational complexity, making it a promising solution for safeguarding data against the ever-growing computational power of potential eavesdroppers. Several quantum mechanical phenomena contribute to the robustness of the protocol, which supports the security of the QKD system. The no-cloning theorem is central to this, as it states clearly that it is impossible to create an identical copy of an unknown quantum state without destroying the original. This principle directly addresses the threat of silent eavesdropping, which is common in classical communication systems. When applied to QKD, the no-cloning theorem ensures that any attempt by an eavesdropper to clone the quantum key will inevitably introduce detectable anomalies, preserving the confidentiality of the key exchange [60].

Quantum superposition, where particles like electrons or photons can exist in multiple states simultaneously and quantum entanglement a phenomenon in which the state of one particle instantaneously influences the state of another regardless of the distance separating them, are both leveraged to ensure the security of quantum communication channels. Superposition allows QKD systems to transmit information in a way that is inherently ambiguous to an eavesdropper, while entanglement enables the detection of any interference, as any observation of entangled particles immediately alters their overall quantum state [12]. The observer effect, also known as the measurement problem in quantum mechanics, holds that measuring a quantum state always causes it to change. In the context of QKD, this means that any eavesdropping attempt, which inevitably involves some form of measurement, will disturb the quantum states encoding the key, thereby alerting authorized entities to the presence of an intruder [27].

The theoretical framework of QKD suggests that it is inherently resistant to eavesdropping. However, practical implementations [25] are not without flaws. Most QKD protocols, including BB84, rely on the transmission of single photons to transport the quantum key. However, due to technological limitations, current photon sources frequently produce multi-photon pulses. These pulses can lead to security breaches, most notably through the Photon Number Splitter (PNS) attack, in which an eavesdropper can siphon off one or more photons from a multi-photon pulse. The absence of these photons may be incorrectly attributed to normal transmission losses, masking the breach [26]. In a PNS attack, Eve could capture one photon from a pulse, leaving the rest to reach the intended recipient, Bob. Since the absence of photons can be ascribed to losses inherent in the transmission media – such as fiber optic cables – or inefficiencies in the detectors, such an attack might go undetected [23].

Advances in quantum technology continue to address these challenges and improve the practical security of QKD. Developments in single-photon sources and detectors, along with innovative error correction and privacy amplification techniques, are improving the fidelity and security of QKD systems. As these solutions mature, they have the potential to provide an impregnable communication framework that is immune to the vulnerabilities that affect classical cryptographic systems [51].

2.4.1 Coherent One-Way Protocol

The Coherent One-Way (COW) protocol is a type of Quantum Key Distribution (QKD) method designed to establish a secure communication channel between two parties. It is termed “one-way” because, unlike some other QKD protocols that require quantum communication to be bidirectional, COW QKD allows for quantum states to be sent only in one direction, typically from the sender (Alice) to the receiver (Bob). In COW QKD, the key information is carried over quantum states, using a sequence of light pulses. These pulses are in a weak coherent state, which means that they are low-intensity light beams that approximate single-photon sources. This is done to ensure that the fundamental principles of quantum mechanics can be applied, such as the uncertainty principle and the no-cloning theorem, which are essential for the security of QKD protocols. The primary advantage of COW QKD is that it can be easily integrated with existing optical communication systems. It requires only standard telecommunication fibers for the quantum channel, which simplifies the physical implementation compared to some other QKD schemes. Additionally, COW QKD’s simplicity makes it more resilient against certain types of operational imperfections and environmental disturbances. The security of the COW QKD protocol is grounded in the quantum mechanical properties of light pulses. Any attempt by an eavesdropper to intercept and measure the quantum states alters the state itself, an event that can be detected by the legitimate parties involved in the communication. This detection is typically performed by comparing the measurement results on a subset of the transmitted pulses, which can reveal the presence of any interference from the third party.

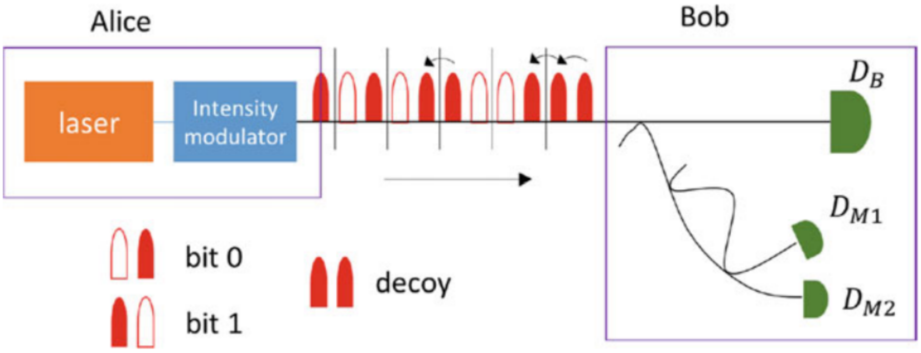


Figure 2.3: A schematic representation of the working of the standard Coherent-one-Way QKD Protocol. The arrow on tops of the encoded bits represents coherence [59]

.

Fig(2.3) represents the execution of Coherent One-way protocol as represented in (Verma et al. 2018).

The protocol also includes the use of decoy states and variations in the intensity of the pulses, which provide an additional layer of protection against sophisticated attacks such as the photon number splitting attack. These decoy states allow Alice and Bob to detect eavesdroppers who might otherwise exploit multi-photon pulses to gain information without being noticed. COW QKD, like other QKD protocols, is followed by classical post-processing steps, which include sifting, error correction, and privacy amplification. These steps are carried out over a classical channel and are necessary to ensure the final key is both secure and consistent between Alice and Bob.

Fundamental Assumptions

Before we describe our variant of the COW-QKD, the assumptions on the devices of sender Alice and receiver Bob are introduced here. In this protocol, Alice and Bob work together to encode a random bit with a quantum state made up of two pulses sent in close succession. The main assumptions are as follows,

1. We assume that Alice's device produces weak coherent pulses [13], which mimic single-photon sources and are essential to the operation of the COW protocol.

2. The encoding process at Alice's end utilizes the time-bin method [55], where logical bits are represented by the timing of the pulses, aligning with the temporal encoding strategy of the COW protocol. Encoding knowledge is discussed beforehand between Alice and Bob, and it is considered as global knowledge.

3. The simulation incorporates a fundamental technique in the COW protocol for improving security: it mixes real data pulses with decoy states (vacuum states) [22] to prevent photon number splitting attacks.

4. Since distinguishing between the legitimate signal and decoy pulses is essential to deciphering the transmitted data, it is assumed that Bob's setup can measure photon arrival times accurately [55].

5. To ensure the security integrity of the quantum channel, it is assumed that Bob has a monitoring mechanism in place to identify any phase changes that might be signs of eavesdropping attempts.

Steps for executing COW protocol

1. Alice generates a sequence of pulses that represent quantum bits (qubits). Each bit is encoded as a three-pulse sequence as represented in eq(2.3) and eq(2.4) for logical zero and logical one respectively.

$$\psi_0 = [\left|0\right\rangle, \text{VACUUM}, \left|0\right\rangle] \tag{2.3}$$

$$\psi_1 = [\left|1\right\rangle, \text{VACUUM}, \left|1\right\rangle] \tag{2.4}$$

2. Alice will randomly insert the vacuum sequences as represented in eq(2.5), into the pulse sequence to act as decoy states. This helps to detect eavesdropping attempts by checking the integrity of these sequences after transmission.

$$\psi_2 = [\text{VACUUM}, \text{VACUUM}, \text{VACUUM}] \tag{2.5}$$

3. The encoded sequences, mixed with the decoy sequences, traverse the quantum channel. This channel not only introduces potential errors, such as phase shifts, but also incurs loss, affecting the integrity of the transmitted pulses.

4. At Bob's end, a beam splitter routes the incoming pulses either to the data line or to the monitoring line. The data line contributes to the raw key formation, while the monitoring line helps in detecting eavesdropping by analyzing the interference patterns of the pulses.

5. Bob's detectors on both lines record the incoming pulses. Through classical communication, Alice and Bob perform sifting, discarding non-synchronized bits and retaining only those that contribute to the raw key formation.

6. After sifting, error correction is applied to the raw key to rectify any discrepancies due to channel noise or potential eavesdropping. Privacy amplification is then performed to shorten the key, ensuring any partial information gained by an eavesdropper is minimized.

2.4.2 Kak06: The Three Stage Protocol

The Three-Stage Quantum Key Distribution (QKD) protocol represents a significant advancement in quantum cryptography, merging key distribution and message encryption processes to enhance security and efficiency in quantum communications. This protocol diverges from traditional QKD systems by integrating these processes, thus streamlining the quantum communication workflow and bolstering security against potential quantum attacks.

Initially, the protocol establishes a secure foundation through the pre-sharing of a random bit sequence between the communicating entities, typically referred to as Alice and Bob. This shared sequence is pivotal for synchronizing the encoding and decoding of the transmitted quantum states during the communication process. Following this, the quantum transmission phase involves encoding the message or cryptographic key onto quantum states, such as qubits, which are then transmitted through a quantum channel. This encoding process is designed to protect the information, leveraging quantum mechanics' principles, like the no-cloning theorem, to prevent unauthorized duplication or access to the quantum states.

The protocols next step is a classical post-processing stage, where error correction and privacy amplification are conducted to rectify any transmission discrepancies and reduce the potential information accessible to eavesdroppers. The three-stage protocol's effectiveness against various quantum attacks and its operational efficiency in secure quantum communications have been thoroughly analyzed in existing research, emphasizing its potential as a foundational element in future quantum cryptographic systems [40, 53].

The adaptability of the three-stage protocol to various quantum communication scenarios highlights its practical significance, with its structure being conducive to enhancements and optimizations that address the evolving challenges of quantum cryptography. This flexibility, combined with the protocol's comprehensive security approach, establishes it as a valuable asset in the advancement of quantum technologies.

Ongoing research and academic discussion around the three-stage protocol are crucial to unlocking its full potential and identifying opportunities for improvement. Such scholarly efforts are key to advancing the field of quantum cryptography, leading to the development of more secure and efficient quantum communication networks [66].

In conclusion, the three-stage quantum key distribution protocol marks a pivotal evolution in quantum cryptography, offering a sophisticated approach to secure communication in the quantum era. Its integrated method of key distribution and message encryption, along with its proven resilience against quantum attacks, positions it as a promising framework for the next generation of quantum communication infrastructure.

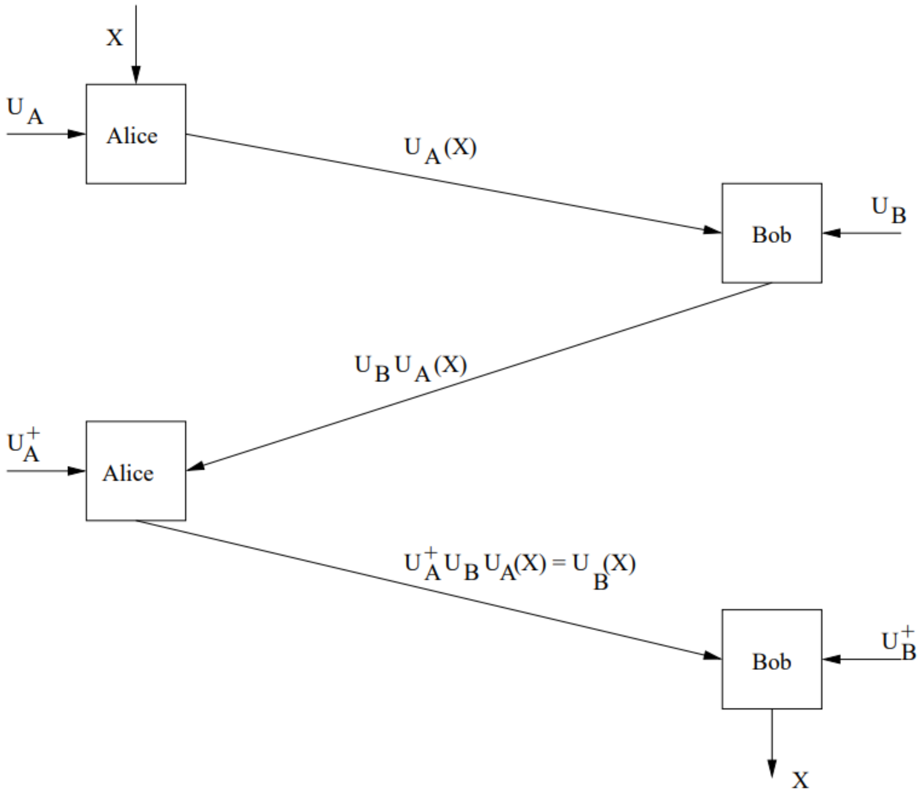


Figure 2.4: The image represents a three-stage quantum key distribution protocol: Alice and Bob apply sequential unitary transformations to a quantum state, and then reverse these transformations to retrieve the original state, demonstrating the principles of quantum cryptography [19]. Here X is the message that wants to be communicated between Alice and Bob, U_A - unitary operation known to and performed by Alice and U_B - an unitary operation known to and performed by Bob.

Fig(2.4) represents the execution of Three-Stage protocol as represented in (Kak et al. 2006).

Steps for executing Three-Stage protocol:

1. Let us consider the following scenario. Alice wants to safely send Bob a single-qubit quantum state $|\psi\rangle \in (\alpha|0\rangle + \beta|1\rangle)$. Alice and Bob have previously discussed the basis for qubit preparations, which is regarded as global knowledge.

2. The state of $|\psi\rangle \rightarrow |\psi'\rangle$ is modified by Alice using a unitary operation, $U_A = R(\theta)$, where $|\psi'\rangle = U_A|\psi\rangle$. Alice now sends Bob $|\psi'\rangle$. Equation (2.6) describes a rotation operation, which is represented by the unitary operation. eq(2.6).

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \tag{2.6}$$

   where θ is the choice of angle of rotation.

3. To change the state of the qubits from $|\psi'\rangle \rightarrow |\psi''\rangle$, Bob additionally applies another unitary transformation, $U_B = R(\phi)$, where $|\psi''\rangle = U_B U_A|\psi\rangle$. He then transmits Alice the new state. A crucial point to remember is that U_A and U_B are selected such that $[U_A, U_B] = 0$.

4. Because the unitary operators used here commute, Alice can apply $U_A^\dagger$ to reverse her transformation. Alice now sends Bob this updated state, or $|\psi'''\rangle = U_B|\psi\rangle$.

5. Bob also uses $U_B^\dagger$ to reverse his unitary operation. As a result, Bob retrieves the original message that Alice sent, or the qubits' initial state, $|\psi\rangle$.

2.5 Quantum Hardware

Quantum hardware forms the foundation of any quantum computing or communication system, consisting of intricate components that function under the principles of quantum mechanics.

2.5.1 Transmitters and Receivers in Quantum Systems

Quantum communication systems utilize transmitters to encode information into quantum states, typically employing qubits as the quantum equivalent of classical bits. Conversely, receivers are specifically intended to measure these qubits without causing any more disruption to their quantum state, which is difficult because of quantum decoherence. Within the field of quantum computing, lasers can be used as transmitters and receivers to modify the state of qubits. Alternatively, quantum gates can be employed as transmitters and receivers to conduct operations on qubits within a quantum processor [4].

2.5.2 Quantum Channel

The quantum channel serves as the conduit for the transmission of qubits from the sender to the receiver. One option is to use an optical cable in which quantum information is carried by photons. Another option is to use empty space, where qubits can be communicated using electromagnetic waves. Preserving the coherence of qubits over long distances poses a substantial engineering obstacle due to the possibility of interference and the loss of quantum state information, sometimes referred to as decoherence [20].

2.5.3 Detectors

Quantum systems employ detectors to determine the state of a qubit. They must do so delicately to avoid destroying the quantum state through the measurement process. Photon detectors are commonly used in optical quantum systems to recognize individual photons that represent qubits [14].

2.5.4 Beamsplitters

Beamsplitters are optical devices that divide a beam of light into two distinct directions. Beamsplitters play a crucial role in quantum optics by enabling the creation of entangled photon pairs. They are utilized in a range of quantum computing and communication protocols, including the configuration of Bell test experiments and quantum key distribution (QKD) systems [31].

2.5.5 Quantum Repeaters

Quantum repeaters are essential for expanding the reach of quantum communication networks because they compensate for the losses and noise that naturally occur in quantum channels. These devices utilize entanglement and teleportation to enhance and reconstruct the quantum signal while adhering to the no-cloning theorem of quantum physics. Repeaters are crucial for enabling the practicality of long-range quantum communication, such as intercontinental quantum key distribution (QKD) networks [5, 7].

Entanglement Swapping

Entanglement swapping is a quantum process that extends on the idea of entanglement, a fundamental principle of quantum mechanics in which particles become interconnected regardless of their separation in space. The procedure commences by utilizing two sets of entangled particles, denoted as (A, B) and (C, D), where A is entangled with B and C is entangled with D. The goal of entanglement swapping is to establish entanglement between particles A and D, without any direct interaction between them. By performing a Bell-state measurement on particles B and C, the entanglement between them is transferred, resulting in the creation of a new entangled pair (A, D). This enables the transmission of quantum information over long distances [65].

This technique is crucial for the functioning of quantum repeaters, which are indispensable devices for long-range quantum communication. Quantum repeaters utilize the process of entanglement swapping to overcome the challenges posed by particle loss and decoherence when transmitting quantum information across long distances. By dividing the communication channel into smaller, controllable sections, entanglement can be created between neighboring nodes. When entanglement is swapped at these nodes, the entangled state is expanded throughout the network, resulting in a continuous quantum link [5].

The significance of entanglement swapping becomes increasingly important in the field of quantum networking, as it clears the path for the development of the quantum Internet. By facilitating the transmission of entanglement over long distances, it promotes the advancement of secure quantum communication channels, which are essential for protocols like quantum key distribution and quantum teleportation. Entanglement swapping is used to transmit quantum information between different locations without physically moving the entangled particles, showcasing the non-locality of quantum mechanics [31, 39].

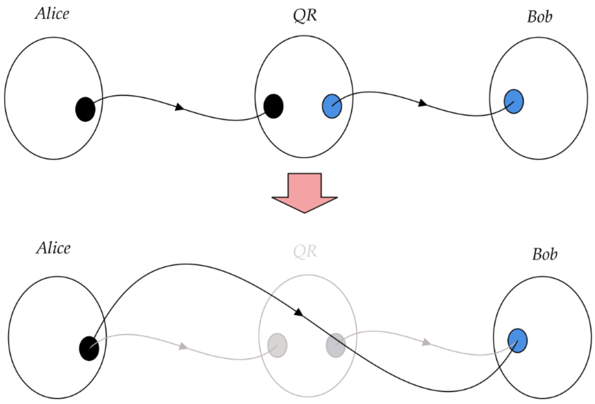


Figure 2.5: The above image represents a simple Quantum network with Quantum repeaters enabling the communication between Alice and Bob. In addition to that it shows how entanglement swapping happens enabling the increase in distance for communication [17]

.

To sum up, entanglement swapping is a crucial procedure for developing quantum networking and communication, not just an intriguing aspect of the quantum world. It acts as the central support system for quantum repeaters and is crucial for the implementation of a quantum internet, providing a plan for creating secure, long-distance quantum communication networks. As this technology advances, it holds the potential to completely transform the way we transmit and process information worldwide [49].

2.6 Practical Problems

There are several practical problems associated with the implementation of physical quantum networks. One of the most significant issue is the instability of the qubits, both during storage and transmission stages. Qubits are prone to decoherence over the transmission channels, which is basically the destruction of the superposed state just because of the interaction with the environment. There can be several other issues that can arise due to these *environmental interactions*, often referred to as *noises* in the system. Here, we discuss about the noise models in detail and how they affect the overall quality of transmission.

2.6.1 Noise Models

Understanding noise models in Quantum Key Distribution (QKD) is essential to comprehending the real-world implementation issues and constraints of these protocols. Noise in QKD systems can take many forms such as photon loss, bit-flip, phase-flip, depolarizing noise, and amplitude damping that can influence the quantum states utilized for key distribution. These errors can be induced by various environmental factors like thermal fluctuations or electromagnetic interference and can severely compromise the security of the key distribution process if not properly mitigated. All of these errors require sophisticated quantum error correction techniques to preserve the integrity of quantum information transmitted over noisy channels [13]. Fig(2.6) gives a schematic representation of the bit-flip error using the Bloch sphere representation. Mathematically, we can write the evolution of a single qubit state in the presence of noise models as [28, 46]

$$\rho = \sum_i E_i^k \rho (E_i^k)^\dagger, \tag{2.7}$$

where E_i^k are the respective Kraus operator for the noise models used and ρ is the density matrix of state of the system ($\rho = |\psi\rangle\langle\psi|$), and the subscript i represents the different noise models, i.e., like E_0 defines the Kraus operator without noise application and E_1 represents the Kraus operator under noise application [57].

Bit-Flip Noise Model

Bit-flip errors (Pauli X errors) occur when a qubit's state is involuntarily flipped from $|0\rangle$ to $|1\rangle$ or vice versa, leading to incorrect quantum state measurements. The evolution of the qubit state under the presence of bit-flip noise model can be written as,

$$\rho' = (1-p)E_0\rho E_0^\dagger + pE_1\rho E_1^\dagger, \tag{2.8}$$

where, ρ' defines the post-error state, p is the probability of application of bit-flip noise model, and E_0 and E_1 represents the Kraus operator for no noise and noise scenario respectively. They can be written as follows,

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.9}$$

Fig(2.6) shows that under the application of the Kraus operator, the Bloch sphere contracts about the $\hat{x} - \hat{z}$ plane.

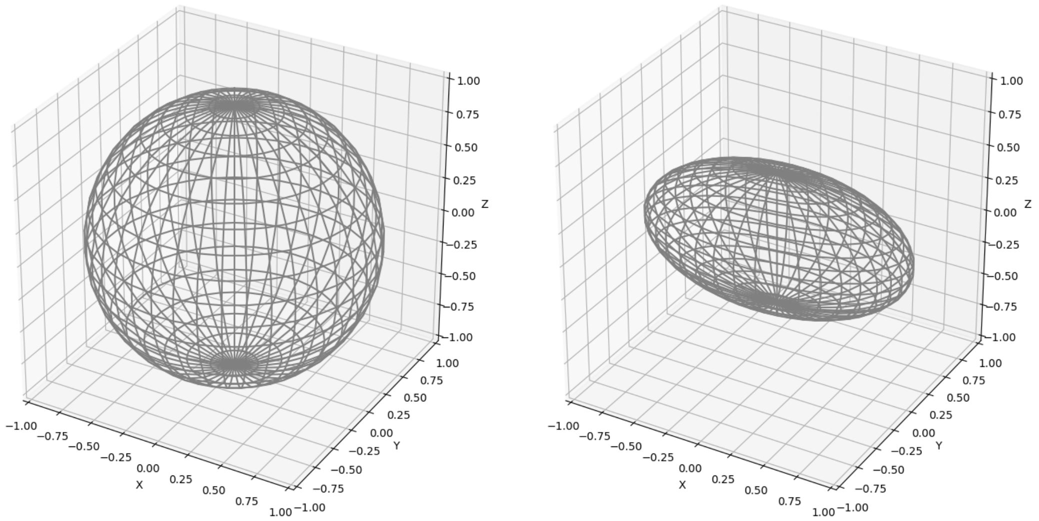


Figure 2.6: Schematic diagram for Bit-flip noise model shown using Bloch sphere representation. We can see that under the action of bit-flip error model the Bloch sphere contracts the $\hat{x} - \hat{z}$ plane uniformly by a factor of $1 - 2p$ where p is the probability of bit-flip error application [50].

Phase-Flip Error

Phase-flip errors (Pauli Z errors), on the other hand, affect the phase of the qubit without changing its amplitude. The density matrix [16] for a probability p can be written as

$$\rho' = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger, \tag{2.10}$$

where ρ is the density matrix denoting the state of the qubit before the error, and ρ' is the state after the error. E_0 and E_1 are the Kraus operator for the no-error and error cases respectively and they can be described in the matrix form as given in eq(2.11).

$$E_0 = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad E_1 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.11}$$

On further simplification eq(2.10), we can write the equation in form of Pauli's Z-gate as,

$$\rho' = (1-p)\rho + pZ\rho Z \tag{2.12}$$

where Z is the Pauli-Z matrix which can be written as,

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

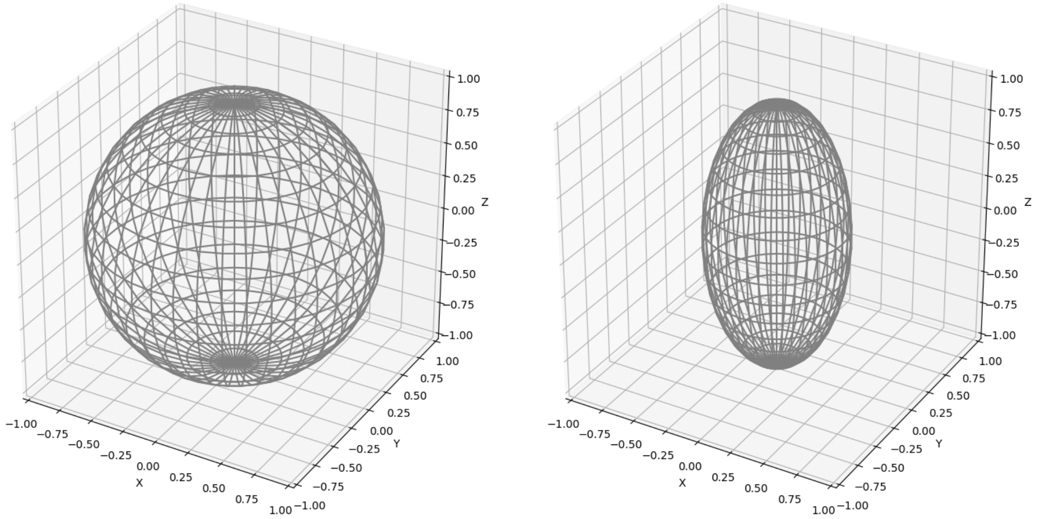


Figure 2.7: Schematic diagram for phase noise model shown using Bloch sphere representation. We can see that under the action of phase-flip error model the Bloch sphere contracts the $\hat{y} - \hat{x}$ plane uniformly by a factor of $1 - 2p$ where p is the probability of phase-flip error application [50].

Bit-Phase Flip Noise Model

The Bit-Phase Flip Noise Model model is the combination of two noise models discussed earlier. For a given probability p, both X and Z gates are applied the the qubits. This is called Pauli's Y-gate [16]. The change in the state is denoted by

$$\rho' = (1-p)\rho + pY\rho Y^{\dagger}, \tag{2.14}$$

where ρ is the density matrix of the qubit state before error, and ρ' with the inclusion of the error and Y is the Pauli's Y-gate. The Kraus operator for bit-phase flip noise model can be written as,

$$E_Y = \sqrt{p}\,Y, \tag{2.15}$$

where p is the probability of the noise affecting the system and, as mentioned earlier, Y is the Pauli's $Y-$gate described as follows in eq(2.16).

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{2.16}$$

Fig(2.8) shows a schematic representation of the contraction of the Bloch sphere under the presence of Bit-flip channel.

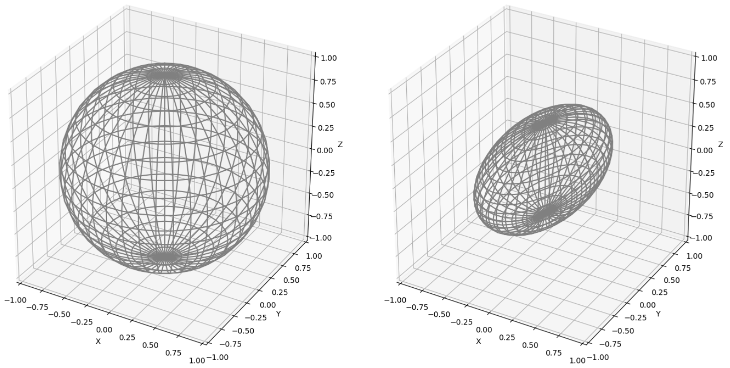


Figure 2.8: Schematic diagram for Bit-flip noise model shown using Bloch sphere representation. We can see that under the action of phase-bit-flip error model the Bloch sphere contracts and rotates the sphere by an angle π about the Y-axis [50].

Depolarization Noise Model

Depolarizing noise is a type of error that affects the state of a qubit in a more uniformly distributed manner, causing it to randomly switch to any possible quantum state. This noise model captures the effect of environmental interactions that cause the qubit to lose its polarization, leading to a decline in information fidelity. Depolarizing noise is particularly challenging in quantum communication, as it represents a fundamental limit to the fidelity that can be achieved, which makes it essential to devise QKD protocols that are robust against such uniformly distributed noise sources [51]. Fig(2.9) represents the contraction of the Bloch sphere under the application of depolarization channel.

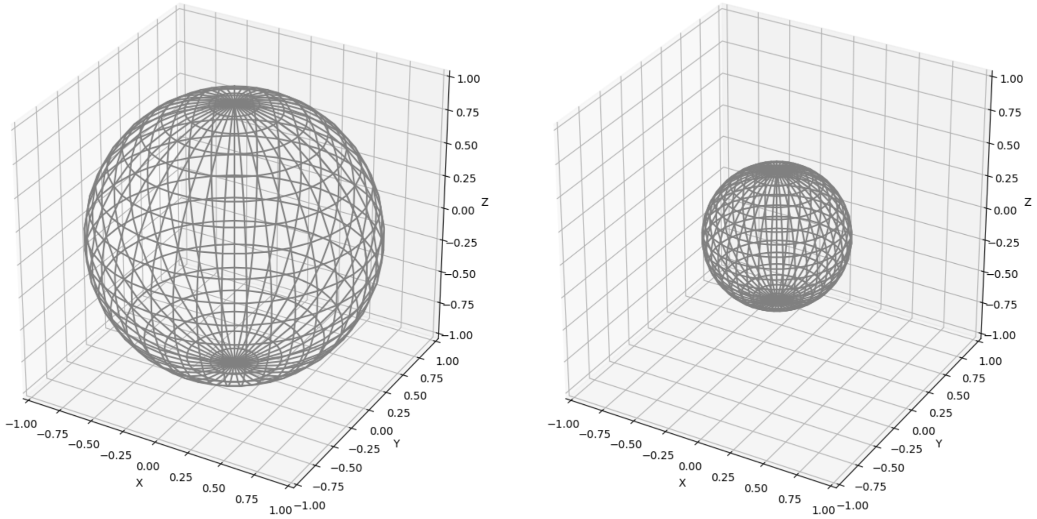


Figure 2.9: Schematic diagram for depolarizing noise model shown using Bloch sphere representation. We can see that under the action of depolarizing error model the Bloch sphere contracts the sphere uniformly by a factor of $1 - 2p$ where p is the probability of depolarizing error application [50].

Photon Loss or Attenuation:

Photon loss, also known as attenuation, significantly affects the transmission efficiency of quantum states across a communication channel. This phenomenon is typically represented by an exponential decay in signal strength as a function of distance, where the decay rate is influenced by the properties of the transmission medium. In QKD, photon loss can lead to a reduced number of detectable photons at the receiver's end, impacting the key rate and potentially compromising security. The exponential nature of photon loss means that the probability of a photon surviving through the channel decreases logarithmically with distance, necessitating efficient error correction and privacy amplification mechanisms to ensure secure communication over longer distances [26]. The loss is often dictated by the attenuation equation,

$$P = 10^{-\alpha L/10}, \tag{2.17}$$

where, α is the attenuation constant, L is the distance between Alice and Bob, and P denotes the probability of the qubit successfully reaching the distance.

Amplitude Damping

Amplitude damping represents the loss of energy from a quantum system and is critical in the context of QKD. Models the natural decay process in quantum states, such as the transition of a photon from an excited state to a ground state, leading to a decrease in the amplitude of the quantum state. This form of noise directly impacts the qubit's ability to convey information accurately over distances, highlighting the need for effective quantum state preservation and recovery strategies in long-distance quantum communication [23]. This can be represented using Kraus Operator as, [**Thapliyal2015**, 28, 46]

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}, \tag{2.18}$$

where p is the decoherence rate. The representation of density matrix is as follows.

$$\rho' = E_0 \rho E_0^{\dagger} + E_1 \rho E_1^{\dagger}, \tag{2.19}$$

where ρ is the density matrix of the quantum state before the noise application, and ρ' is the change in state after the application of noise in the system. Fig(2.10) represents the shrinking of the Bloch sphere under the application of amplitude damping noise model.

In the realm of NISQ-era devices, these noise models play an integral role in simulating the operational conditions faced by quantum communication systems. Incorporating such detailed noise simulations allows researchers and engineers to evaluate the durability and security of QKD protocols under realistic conditions, paving the way for the development of more reliable and secure quantum communication technologies.

To conclude, this chapter speaks about how quantum networking is a system that creates an essential framework for secure communication by applying the principles of quantum mechanics. This chapter explores the key elements of quantum networking, with a primary emphasis on qubits, which are the basic building blocks of quantum

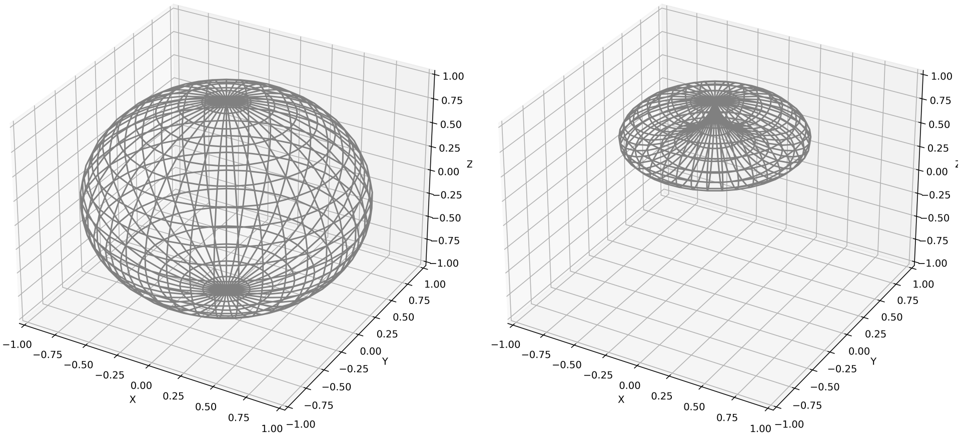


Figure 2.10: Contraction of the Bloch sphere to the lower energy state ($|0\rangle$) under the presence of amplitude damping

information. This text explores into the unique characteristics of qubits, such as superposition and entanglement, which serve as the foundation for quantum networks to accomplish tasks that surpass the capabilities of classical systems. The chapter also presents qubit-vector algebra as an essential mathematical tool for describing and manipulating quantum states. This chapter establishes the foundation for understanding the potential of quantum networks to transform data transmission. It highlights the importance of reliable quantum key distribution (QKD) mechanisms in safeguarding against emerging cybersecurity risks. The chapter concludes by emphasizing the significant impact of quantum networking on improving secure communication. It highlights the crucial role of qubit mechanics and vector algebra in advancing the field of quantum information science.

Chapter 3

Network Simulation Design

3.1 What is SeQUeNCe?

The SeQUeNCe (Simulator of Quantum Network Communication) [62, 33] is an advanced tool in the field of quantum computing, designed specifically for the detailed modeling and analysis of quantum communication networks. It is a comprehensive framework for detailed simulation of quantum network operations. It includes various components such as quantum channels, protocols, and devices. The robust design of this system is crucial for researchers who want to explore the intricate dynamics of quantum information transfer and for network engineers responsible for creating scalable and efficient quantum networks.

SeQUeNCe's quantum channel modeling is one of its fundamental features. This feature enables the simulation of quantum state transmission through various environmental conditions that commonly affect qubit coherence and integrity. SeQUeNCe accurately models the behavior of quantum channels by taking into account factors such as noise, decoherence, and physical loss of qubits during transmission. This level of precision allows for the evaluation of quantum communication protocols in practical operational scenarios, establishing the foundation for more robust quantum communication techniques.

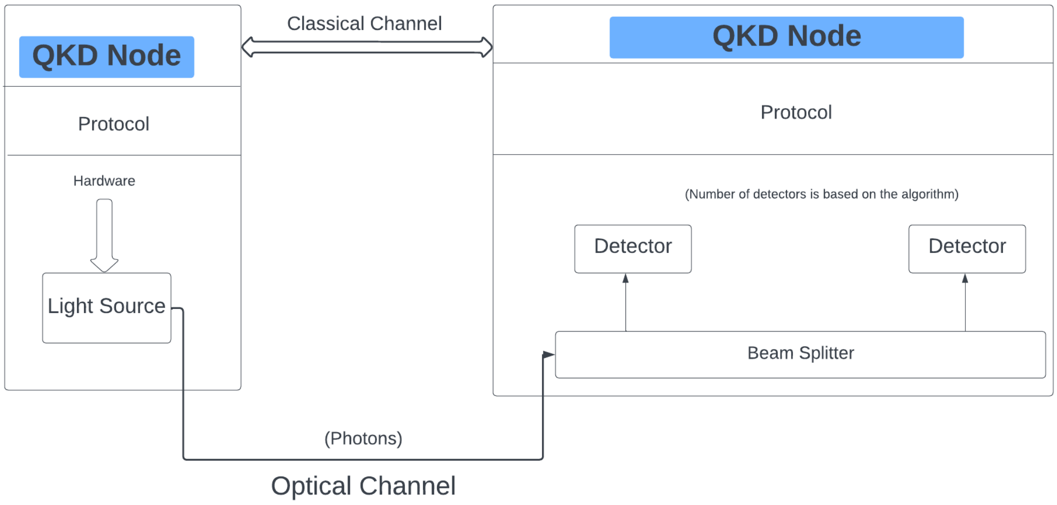
Quantum networking relies on a set of specialized protocols that regulate the exchange of quantum information. SeQUeNCe provides comprehensive assistance for simulating a wide range of protocols, such as quantum key distribution, teleportation, superdense coding, and entanglement distribution. The protocol simulation capabilities are essential for validating theoretical predictions, optimizing protocol parameters, and developing new communication strategies in a virtual and safe environment.

Moreover, SeQUeNCe's expertise also encompasses the ability to accurately reproduce the specific network layer behaviors that are distinct to quantum networks. Quantum networks, in contrast to classical networks, operate based on the principles of quantum mechanics. These networks require a completely different approach to tasks like routing [41] and node communication due to the utilization of concepts like entanglement. The simulator allows users to create intricate network topologies, ranging from simple star or ring structures to complex graph-based configurations. Through the process of experimenting with these topologies, users can ascertain the most optimal routes for distributing entanglement and identify any potential obstacles in the design of quantum networks.

SeQUeNCe is capable of simulating physical layer operations and includes models of important quantum devices such as quantum memories, quantum repeaters, and photon detectors. These components are crucial for the implementation of a quantum network, as they affect the storage, restoration, and measurement of quantum states. By accurately simulating the physical layer, SeQUeNCe can effectively predict the performance of quantum networks, thereby assisting in the development of practical quantum devices and systems [58].

SeQUeNCe is intentionally designed to be modular and extensible, allowing for ongoing development and improvement. As quantum technologies advance, the simulator can be enhanced with additional modules and features, enabling it to keep up with the latest industry developments. The adaptability of this platform benefits both the quantum research community, by promoting collaboration and shared progress, and educational purposes, by providing a dynamic platform for teaching quantum network principles [3, 24, 35, 37, 36, 43].

SeQUeNCe is a highly advanced tool designed for the field of quantum computing. It provides comprehensive capabilities for simulating and comprehending the complex behaviors of quantum networks. This asset is crucial for the advancement and improvement of quantum communication technologies. It also acts as a guiding force for collaborative and educational efforts in the field of quantum information science.



Note: For this thesis the source and destination algorithm will be either COW or 3-stage

Figure 3.1: The diagram illustrates a Quantum Key Distribution (QKD) setup where two QKD Nodes exchange photons via an optical channel and synchronize through a classical channel, with the process governed by a specific protocol and utilizing beam splitters and detectors as per the algorithm employed.

3.2 Topologies Implemented

Topology, in the context of networking, pertains to the configuration or structure of different components (such as nodes, links, devices) within a network. It establishes the physical or logical connections between these elements and determines how they communicate with each other in the network. The performance, scalability, and fault tolerance of a network can be influenced by various topologies [6].

3.2.1 Point-to-Point topology

Point-to-Point topology [48] refers to a network configuration where there is a direct connection between two devices, allowing for communication between them without the need for any intermediate devices. This topology serves as the fundamental building block for all other topologies, as it represents a fundamental network connection. It is utilized in situations where a dedicated connection is needed between two endpoints, such as in leased line networks or in establishing a connection between a client and a server over the internet. The simplicity of the system enables it to achieve high levels of performance and reliability. However, it lacks the ability to scale beyond the two devices Fig(3.2).

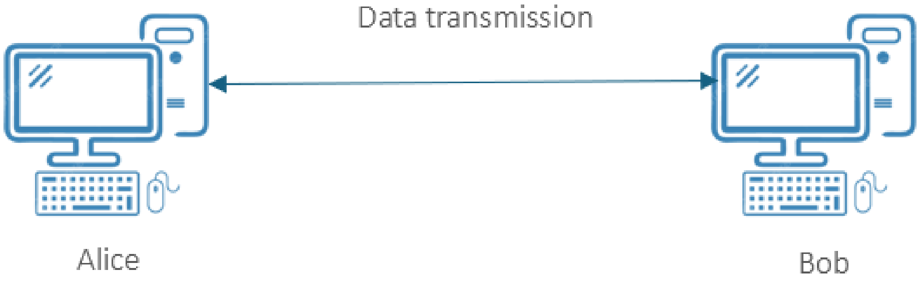


Figure 3.2: The image shows a simple diagram of data transmission between two nodes, labeled Alice and Bob, indicating a direct communication link. The connection happens both-ways, but the routing path chosen is uni-directional.

3.2.2 Ring topology

A ring topology [8] is defined by each node being connected to exactly two other nodes, creating a continuous pathway for signals to pass through each node in a circular manner. In a ring topology, data generally moves in a unidirectional manner, which minimizes the likelihood of packet collisions. This configuration facilitates the effortless recognition of issues and the separation of defective devices. Nevertheless, in the event that a single node or connection becomes disrupted, the entire network is susceptible to failure. Ring topology is evident in older LANs (Local Area Networks) or in SONET networks Fig(3.3).

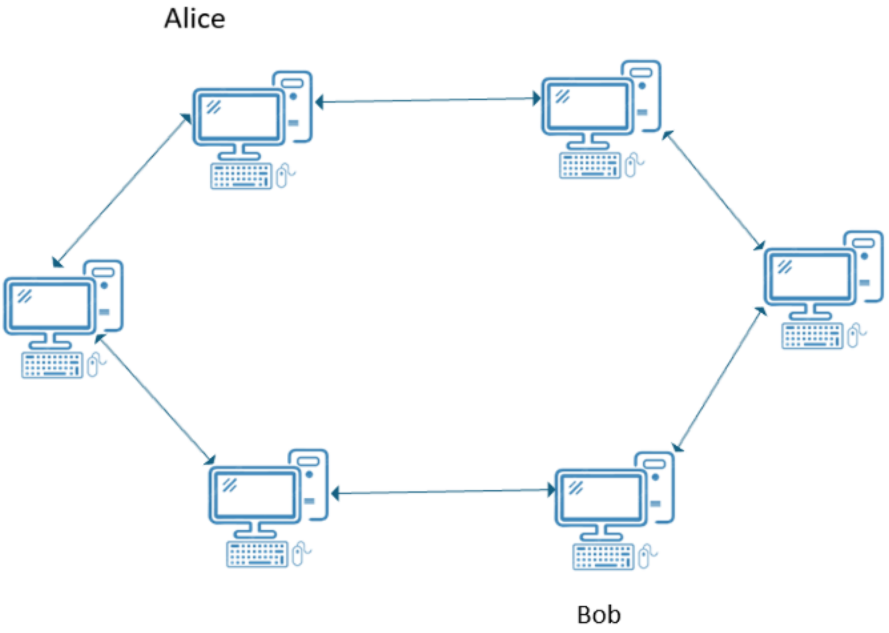


Figure 3.3: Schematic representation of the ring topology. The connection happens both-ways, but the routing path chosen is uni-directional.

3.2.3 Grid topology

Grid topology [1] is a network configuration where nodes are interconnected in a grid-like pattern. The nodes are interconnected in a manner that creates a grid-like structure. This feature offers various routes for data transmission, thereby improving the network's ability to withstand failures and ensuring its dependability. In the event of a failure in one pathway, data packets have the capability to be redirected through an alternative pathway. The grid topology is commonly employed in extensive computing networks or distributed computing systems where robustness and multiple pathways are essential Fig(3.4).

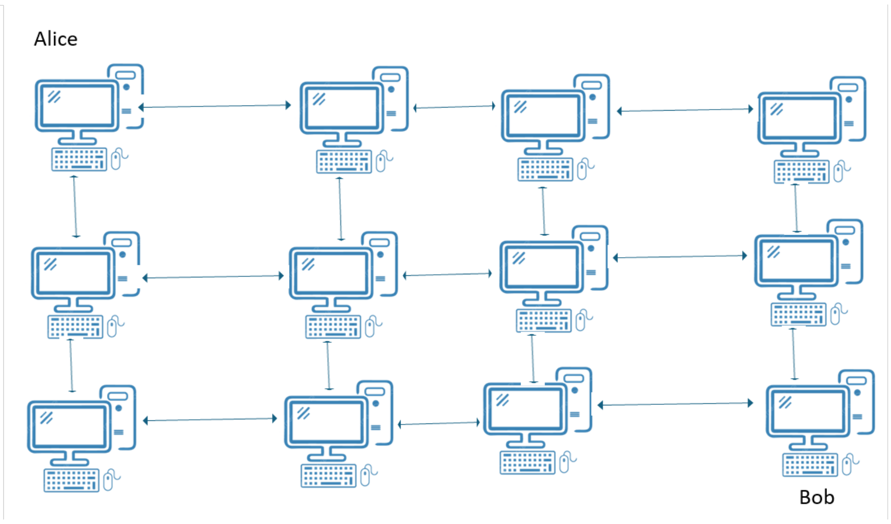


Figure 3.4: The image portrays a grid topology with multiple nodes, organized in a matrix layout, showcasing a network configuration where Alice and Bob's computers serve as terminal nodes. The connection happens both-ways, but the routing path chosen is uni-directional.

3.2.4 Torus topology

Torus topology [10] is an advanced variant of grid topology where the edges of the grid are interconnected to form a continuous loop in both the row and column directions. This results in the creation of a three-dimensional shape resembling a doughnut or torus. This network topology minimizes the number of intermediate connections that data must traverse in order to reach its intended destination. Additionally, it offers two distinct routes to each destination node, resulting in enhanced network resilience and performance. It is frequently utilized in high-performance computing settings, such as supercomputers Fig(3.5).

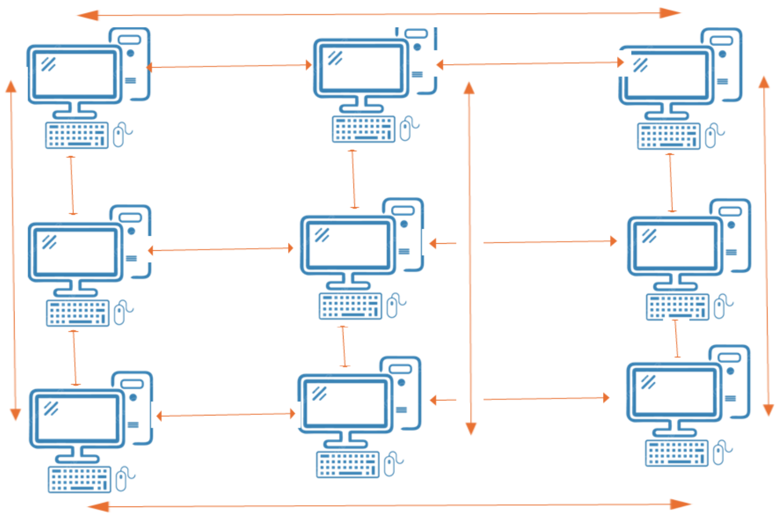


Figure 3.5: Schematic representation of a 3 × 3 torus topology. Torus is a advanced form of grid where the edges connect both horizontally as well as vertically.

3.2.5 Topologies Advantages and Disadvantages

Topology	Advantages	Disadvantages
Ring	- Data flows in one direction, reducing collision risk - Easy to identify and isolate problems	- Failure in one node or connection can disrupt the entire network - Adding or removing devices can disrupt the network
Point-to-Point	- Simple and reliable for direct connection - High performance due to dedicated link	- Only connects two devices; not scalable for large networks - Costly for connecting many devices due to individual links required
Grid	- Provides multiple paths for data, enhancing reliability - Good fault tolerance as failure in one path can be bypassed	- More complex to setup and manage compared to simpler topologies - Requires more cables and network hardware, increasing cost
Torus	- Reduces the number of hops between nodes - Provides high resilience and fault tolerance	- Complex to design and implement - More difficult to troubleshoot and maintain

Table 3.1: Advantages and Disadvantages of Network Topologies

3.3 Implementing Coherent One Way Protocol

The Coherent One-Way (COW) protocol simulation is an essential tool for studying and validating quantum key distribution (QKD) mechanisms. It accurately reproduces the complex quantum processes, such as the creation and transfer of weak coherent pulses, in a regulated setting. This enables a precise evaluation of the behavior of these quantum states under different circumstances, such as noise and potential eavesdropping, which are replicated within the simulation framework.

In this simulated environment, the main objective is to accurately measure and maintain the quality and reliability of quantum states as they pass through a simulated quantum channel. The simulation incorporates factors such as loss and noise to evaluate the durability and adaptability of the communication process. An in-depth analysis is conducted to evaluate the protocol's ability to protect transmitted information from environmental disturbances and malicious interventions. This analysis provides valuable insights into the protocol's operational effectiveness and security level.

The simulation covers both the physical transmission of quantum bits and the subsequent phase of decoding and measuring quantum states. This stage is crucial for assessing the effectiveness of the protocol in obtaining a secure quantum key from the quantum transmission. By iterating the process across multiple rounds, the simulation gathers extensive data on performance metrics, such as the quantum bit error rate (QBER), enabling a thorough analysis of the protocol's efficiency and security aspects.

In simple terms, the simulation offers an in-depth analysis of the COW protocol, highlighting its possibilities and difficulties in practical quantum communication situations. Simulation serves as an intermediary between theoretical research and practical application, providing a platform to thoroughly examine, improve, and optimize the design and implementation of the protocol for upcoming quantum communication networks.

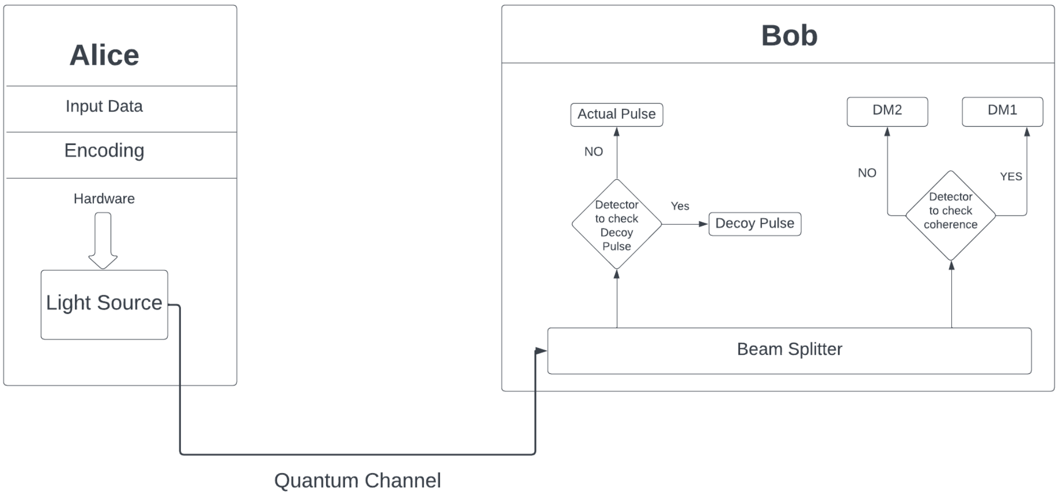


Figure 3.6: Flowchart Representation of COW Protocol Simulation: The image illustrates the process flow in a COW protocol simulator, mapping out the key components and decision paths from Alice's input data encoding to Bob's final pulse detection and processing.

Algorithm 1 Simulation of the Coherent One-Way (COW) Protocol

```
Input: total_rounds, bits_per_round, quantum_channel_properties, noise_models
Output: final_key, average_QBER, success_rate

Initialize simulation environment with quantum channels
Pair adjacent nodes with COW protocols

bit_sequence ← Generate random sequence of bits_per_round length
weak_coherent_pulses ← Encode bit_sequence into weak coherent pulses
decoy_states ← Prepare decoy states

for round = 1 to total_rounds do
    Transmit weak_coherent_pulses and decoy_states through quantum_channel
    Apply noise_models
    received_sequence ← Measure at receiver (Bob's setup)
    Perform classical post-processing for key_reconciliation
    QBER ← Compute Quantum Bit Error Rate
    final_key ← Conduct privacy amplification
    Record QBER for this round
end

average_QBER ← Compute average QBER over all rounds
success_rate ← Determine success rate based on QBER and key_reconciliation results
return final_key, average_QBER, success_rate
```

Variable Descriptions

total_rounds Number of iterations for the QKD process.

bits_per_round Bits encoded and sent in each round.

quantum_channel_properties Features of the quantum channel like loss, delay, etc.

noise_models Types of noise affecting the quantum channel.

final_key Secure key generated after the simulation.

average_QBER Average Quantum Bit Error Rate over all rounds.

success_rate Overall success rate of the QKD process.

3.4 Implementing Three-stage Protocol

The Three-Stage Quantum Key Distribution (QKD) simulation signifies a transition from conventional physical detection techniques to a focus on the cryptographic reliability of quantum communication. Contrary to traditional methods that rely on physical detection mechanisms at the receiver's end, this simulation places a higher emphasis on the cryptographic security of the transmitted quantum bits (qubits). The core of this approach revolves around the creation of quantum states, specifically superposition states, which are crucial for producing secure quantum keys.

These states serve as the foundation for the secure communication channel, persisting throughout the subsequent phases of the QKD process. The transmission takes place through a simulated quantum channel that is specifically created to imitate real-life situations, such as noise and signal loss. The accuracy of the simulation heavily relies on the fidelity of the channel and the ability of the quantum states to withstand different conditions. This methodology enables a thorough assessment of the quantum information transfer process, closely matching real-world quantum communication scenarios.

The simulation effectively utilizes a mathematical technique by using the transpose of unitary matrices for decoding, which eliminates the requirement for advanced quantum state detection hardware. This approach not only streamlines the simulation, but also focuses on the cryptographic operations required to handle and safeguard the quantum keys during the transmission process.

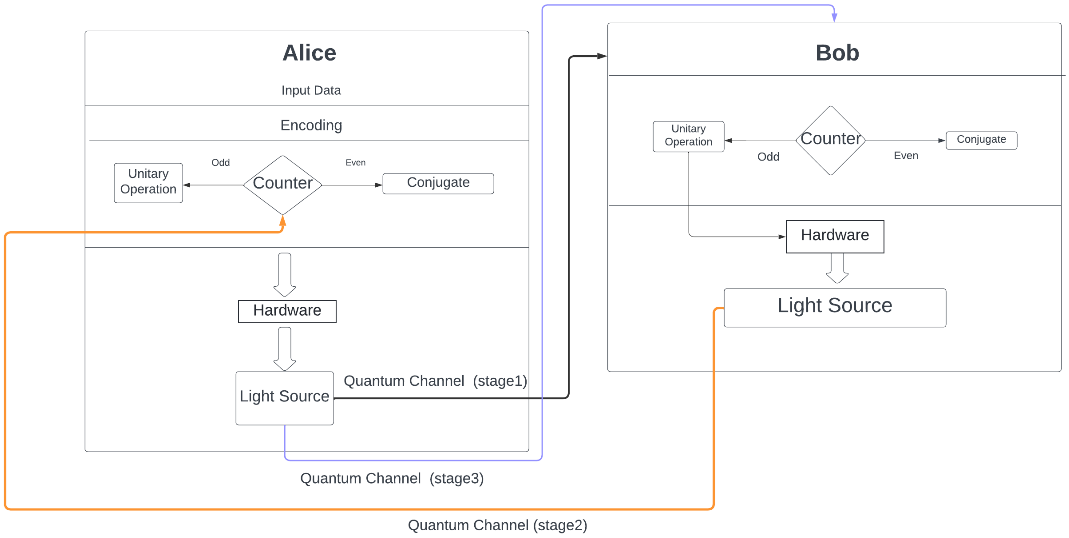


Figure 3.7: The image illustrates a three-stage quantum communication sequence where Alice prepares a quantum state through encoding and unitary operations, which is then transmitted to Bob via a quantum channel. Bob receives the state, applies his own set of unitary operations, and the process may include counter operations and conjugation, indicative of a quantum key distribution (QKD) or similar protocol.

Fig(3.7) shows a schematic design of three-stage protocol using SeQUeNCe simulator.

The simulation provides a detailed examination of the Three-Stage QKD protocol's capacity to maintain secure quantum communication by exploring cryptographic operations. The efficiency [34, 42] of the process, especially in key sifting and distillation through traditional channels, as well as its cryptographic strength, is thoroughly analyzed. The primary objective of the simulation is to assess the efficacy of the protocol in protecting the integrity of transmitted data from potential security breaches. This will provide insights into the reliability and significance of the Three-Stage QKD in actual quantum communication networks.

Algorithm 2 Three-Stage QKD Protocol

```
Input: num_rounds: Total number of rounds in the simulation,
bits_per_round: Number of quantum bits transmitted per round
Output: Final secure key, average QBER, and overall success rate
Initialize Alice and Bob
Create the Unitary Operations $U_A$, $U_B$
Alice generates random quantum bits
for each round in num_rounds do
    /* Stage 1: Alice to Bob */
    Alice applies unitary operation $U_A$ to quantum bits
    Transmit the encoded quantum bits to Bob
    Bob receives quantum bits, measures them to generate part of the key
    /* Stage 2: Bob to Alice */
    Bob applies unitary operation $U_B$ to measured bits and sends them back to Alice
    Alice receives, measures, and applies the conjugate transpose of $U_B$ for decoding
    /* Stage 3: Alice to Bob */
    Alice finalizes the key bits, applies the conjugate transpose of $U_A$, and sends to Bob
    Bob receives the final quantum bits to complete the key
    /* Post-processing */
    Alice and Bob perform classical post-processing for key reconciliation and privacy amplification
    Calculate QBER for the round
end
Compute the average QBER and overall success rate
return final secure key, average QBER, and success rate
```

Variable Descriptions

num_rounds Total number of rounds in the simulation, representing the complete cycles of the QKD process to average out the results for accuracy.

bits_per_round The quantity of quantum bits (qubits) transmitted in each round, determining the size of the quantum key exchanged in one iteration of the process.

U_A Unitary operation applied by Alice to encode the quantum bits, essential for the initial stage of quantum state transformation.

U_B Unitary operation applied by Bob for the second stage of the process, used to manipulate measured quantum bits before sending them back to Alice.

Alice The initiator in the QKD protocol who generates, encodes, and sends the quantum bits to Bob.

Bob The recipient who measures the incoming quantum bits, decodes them, and completes the secure quantum key establishment.

QBER Quantum Bit Error Rate calculated after each round to assess the error levels in the quantum transmission, indicative of the communication's security and integrity.

final_key The secure quantum key established at the end of the simulation, resulting from the successful execution of the QKD process.

average_QBER The mean of the QBER values calculated across all rounds, providing an overall measure of the error rates and thus the efficiency and security of the QKD protocol.

success_rate The proportion of successful key transmissions, reflecting the overall effectiveness of the QKD process across all simulation rounds.

Both simulations were conducted within a networked environment, with nodes representing the sender and receiver in the QKD process. This setup allowed us to simulate not only the quantum communication aspects but also the necessary classical communication for coordinating between the parties involved, such as during the key sifting and reconciliation phases. Through these simulations, we were able to analyze the performance of the COW and Three-Stage protocols under various conditions, assessing their robustness, reliability, and security. The detailed simulation process included monitoring of key metrics like QBER, success rate, and the efficacy of decoy and entanglement strategies, providing comprehensive insights into the operational capabilities and limitations of these quantum key distribution methodologies.

To summarize, this chapter provides a detailed explanation of the complex procedure of simulating quantum networks, with a specific emphasis on implementing Quantum Key Distribution (QKD) protocols in simulated environments. This chapter describes the utilization of the SeQUeNCe simulator, a tool for simulating quantum communication networks, to analyze the effectiveness and dependability of various network structures in different situations. The simulations offer valuable insights into the practical difficulties of incorporating QKD protocols, such as the Coherent One-Way Protocol and the Three-Stage Protocol, into a quantum network. The chapter highlights the crucial significance of simulation in comprehending the behavior of quantum networks and improving the protocols for practical applications.

Chapter 4

Results

This chapter examines the implementation of the project.

4.1 Data Processing

The data processing section primarily concerns itself with the various stages of preparing and simulating the quantum key distribution (QKD) network. The preprocessing phase includes the creation of adjacency matrices according to the specified network topology, calculation of the shortest paths between nodes, and the deletion of specific file contents to ensure a pristine state for each simulation run.

The simulation parameters are established to configure the quantum channels and nodes according to the network topology. The parameters encompass the specified timeline and seed to ensure reproducibility, the attenuation values for the channels, and the conditions required for simulating quantum repeaters. Furthermore, the QKD simulation specifies the precise number of rounds and the number of bits per round. Upon finishing the simulation rounds, a network diagram is produced to visually represent the network and pinpoint the nodes that have quantum repeaters.

A comprehensive description of the preprocessing steps and simulation parameters can be found in Table 4.1.

4.1.1 Pre-processing and Simulation Parameters

In this project, pre-processing refers to the preparation of the simulation environment to accurately represent the network topology and the conditions in which the QKD protocols function. This preparation is essential to ensure that the simulation results are valid and accurately represent real-world scenarios.

The primary stages in the preprocessing phase comprise:

1. **Configuration of the topology:** The network topology, such as grid, ring, star, or torus, is determined and an adjacency matrix is created. The matrix displays physical links between nodes in the network, which is essential in determining the routes that quantum signals will follow.

2. **Path Calculation:** The shortest paths between nodes are computed using a breadth-first search algorithm (BFS) to the adjacency matrix. This step is essential to determine the most effective paths for quantum communication and to simulate the functioning of quantum repeaters in the network.

3. **File Clearance:** Simulation result files are reset at the start of each simulation run to ensure that the data collected is exclusive to the current simulation and unaffected by previous runs.

The preprocessing steps establish the foundation for the following simulation runs, guaranteeing that the network is faithfully depicted and prepared for the execution of QKD protocols.

The simulation parameters, which determine the exact circumstances and configurations of the simulation, are outlined in the table below. The parameters include the attributes of the quantum channel, the quantity of rounds and bits per round for the QKD procedure, and the physical properties of the network, such as distance and attenuation.

Pre-processing Parameters	**Detail**
Adjacency Matrix	Generated based on topology (Grid, Ring, Star, Torus)
Path Calculation	Shortest path computed using BFS
File Clearance	Clears output files before the simulation starts
Timeline & Seed	Timeline with 1×10^{12} resolution, seeded for reproducibility
Attenuation Values	Defined as [0.1, 0.15, 0.5] for simulations
Quantum Channels	Configured with distance, attenuation, and optionally as quantum repeaters
Node Setup	Nodes created and configured according to network topology
Simulation Dynamics	Includes rounds and bits per round for the QKD simulation
Diagram Generation	Network diagram created post-simulation to visualize the network and quantum repeaters

Table 4.1: Overview of Preprocessing Steps and Simulation Parameters

4.1.2 Post-processing and Noise Removal

Large-scale simulations, like those with 1000 rounds, presented significant challenges for the simulator because it is an event-driven model. The main problem was the prolonged execution time, with simulations lasting for one to two days, resulting in significant memory usage. Consequently, the simulator would often experience a state of stuck state and end prematurely. To address these issues and guarantee reasonable simulation durations, the number of iterations was decreased to 100.

However, the decision to decrease the number of rounds in order to reduce execution time and memory usage has led to a new challenge: an amplified impact of noise and variance on the simulation results. To tackle this issue, post-processing methods, specifically the Savitzky-Golay filter, were employed to refine the data and minimize interference caused by noise.

The Savitzky–Golay filter [52], a digital filter, is used to enhance the signal-to-noise ratio while minimizing signal distortion. The process involves using linear least squares to fit low-degree polynomials to subsets of adjacent data points. When used on the simulation data, this filter maintains the important characteristics of the signal, such as the highest and lowest points and the width, which are necessary for accurately representing and analyzing the performance of the quantum key distribution network.

We have implemented a Python code for post-processing which applies the Savitzky–Golay filter to 'average_sifting_percentage' and 'average_key_rate' columns of the data. The filter uses a window size of 5 and a polynomial order of 2. The process of smoothing decreases the rapid changes in the data and enhances the visibility of the fundamental patterns. In addition, a moving average is calculated to further enhance the smoothness of the data and reduce the impact of anomalies and interference.

The post-processing phase guarantees that the data generated will be a polished and dependable representation of the simulation's results. This enables a more precise and significant analysis of the network's performance under different circumstances.

4.2 Coherent One Way (COW) Protocol

In this section, we will delve into the results concerning the simulation of the Coherent-One-Way protocol modeled over SeQUeNCe. We simulate several distances between Alice and Bob nodes and calculate key-rates and Quantum Bit Error Rate (QBER) over these distances.

Fig(4.1) shows the results for COW protocol and this explains that if there is an increase in the distance, then the QBER will be high. For a standard attenuation rate of 0.15 dB/km, the quantum bit error rate (QBER) remains consistently low over a significant distance. It only experiences a slight increase when the distance exceeds 100 km. The low Quantum Bit Error Rate (QBER) observed under standard attenuation conditions indicates successful error management, ensuring the preservation of quantum coherence over extended distances. On the other hand, when the attenuation rate is

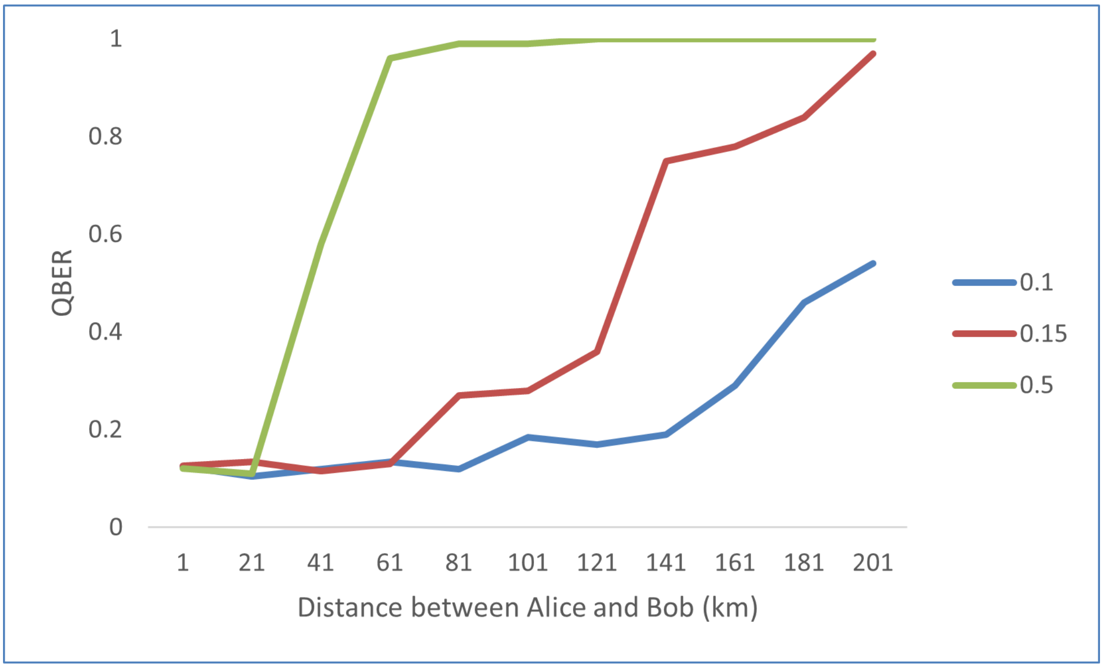


Figure 4.1: This figure shows the QBER over increasing distance between the Alice and Bob nodes for Coherent one way (COW) protocol.

increased to 0.5 dB/km, the QBER initially remains low but then rapidly increases after approximately 60 km. The substantial rise in QBER (Quantum Bit Error Rate) with increased attenuation rates clearly demonstrates a notable increase in QBER which emphasises on the higher loss.

Fig(4.2) shows the results for the COW protocol with different attenuation rates and the higher the attenuation, the lower the key rate. The initial key rate of 0.15 dB/km is relatively high and remains at an acceptable level for approximately 100 km, gradually declining afterwards. The behavior demonstrates the COW protocol's ability to efficiently generate quantum keys over long distances, even when faced with typical levels of signal loss. On the other hand, the key rate, which is measured at 0.5 dB/km, decreases at a much faster pace, reaching almost zero after 60 km. The sharp decline in key rates is in line with the higher QBER, indicating that greater attenuation results in less efficient key generation due to a more significant weakening of the signal.

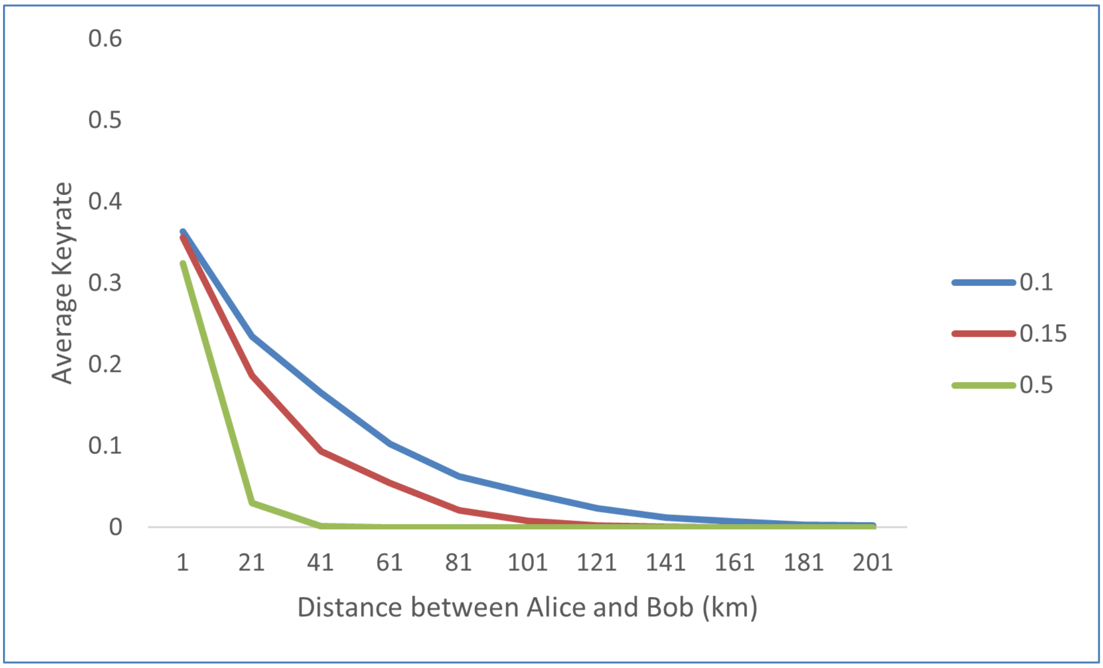


Figure 4.2: This figure shows the key rate over increasing distance between the Alice and Bob nodes for Coherent one way (COW) protocol.

4.2.1 Coherent One-Way Protocol with Quantum Repeater Nodes

In this section, we introduce quantum repeaters in an attempt to increase the distance of the stable transmission. We use two types of repeaters for this, *ideal repeaters* and *non-ideal repeaters.* [1]

Fig(4.3 and 4.4) illustrates the Quantum Bit Error Rate (QBER) performance in the Coherent One-Way (COW) protocol by comparing ideal and non-ideal quantum repeaters at different levels of attenuation (0.15 dB/km and 0.5 dB/km), provides important insights into the effectiveness of the system over different distances. When using ideal repeaters, the system is able to maintain a considerably reduced QBER over greater distances. This effect is particularly evident at the lower attenuation level of 0.15 dB/km, where the QBER remains consistently low even beyond a distance of

[1] In the context of this paper, ideal repeaters provide no extra noise to the system and qubits also avoid facing any attenuation errors when passing through this repeater nodes. Whereas, non-ideal repeaters acts like every other node in the system, and only benefit is the no attenuation loss to the qubits passing through.

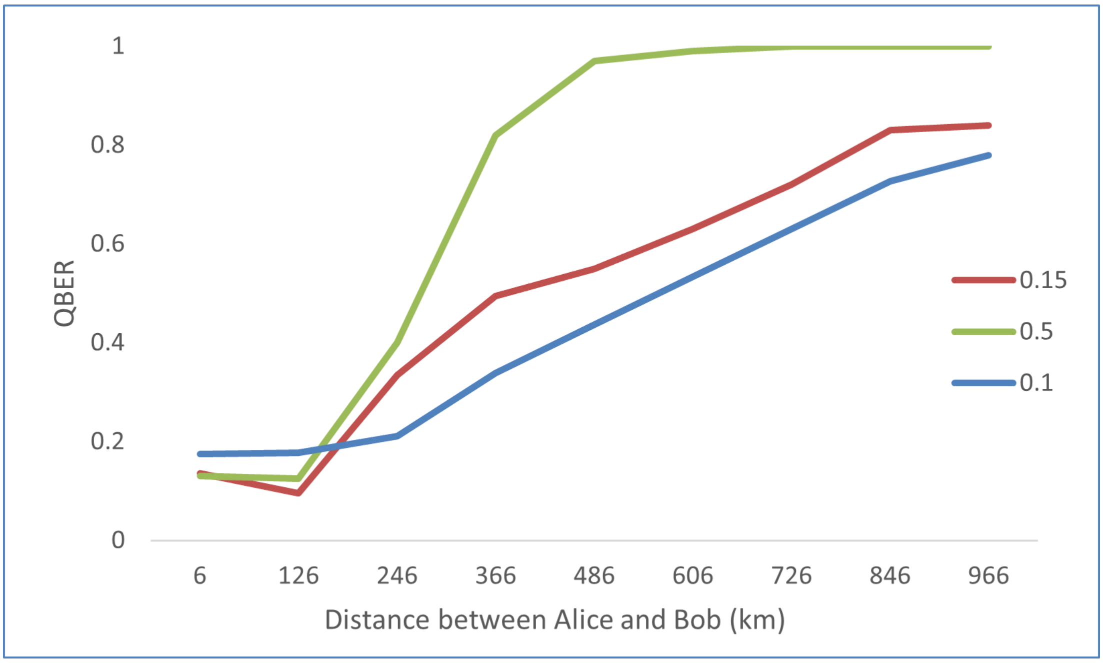


Figure 4.3: This figures shows the QBER over increasing distance between the Alice and Bob nodes for Coherent one way (COW) protocol under the presence of Non-ideal Quantum Repeater nodes.

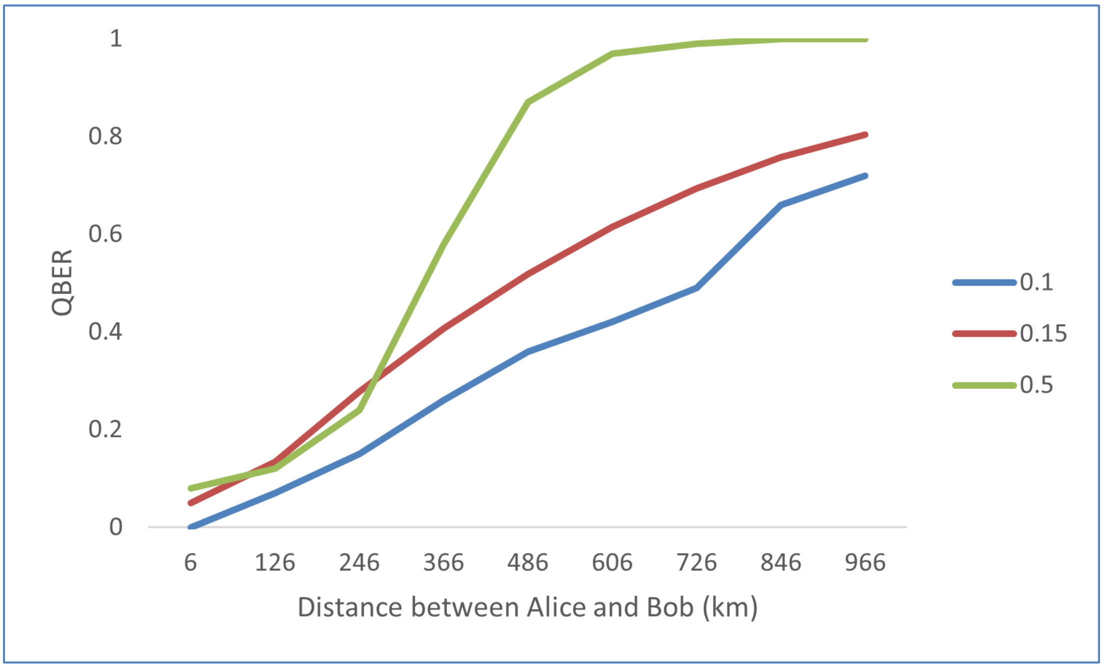


Figure 4.4: This figures shows the QBER over increasing distance between the Alice and Bob nodes for Coherent one way (COW) protocol under the presence of Ideal Quantum Repeater nodes.

600 km. However, when the attenuation reaches 0.5 dB/km, ideal repeaters start to exhibit limitations, resulting in an earlier and noticeable increase in QBER. Despite this, they still manage to maintain lower rates compared to non-ideal quantum repeaters. Non-Ideal quantum repeaters demonstrate a quick increase in QBER (Quantum Bit Error Rate) at both levels of attenuation. This effect is more noticeable at an attenuation level of 0.5 dB/km, where the QBER sharply rises after only 200 km. This emphasizes the importance of implementing repeaters at a strategic position resulting in reduced attenuation using which we can achieve effective long-distance quantum communication.

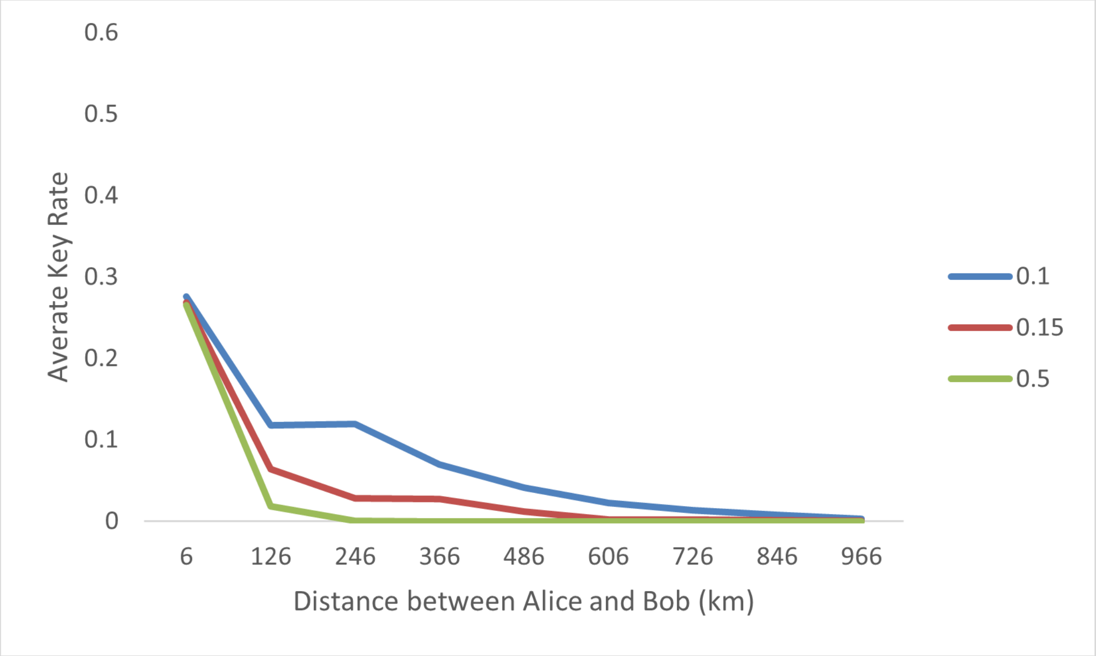


Figure 4.5: This figures shows the key-rates over increasing distance between the Alice and Bob nodes for Coherent one way (COW) protocol under the presence of Non-ideal Quantum Repeater nodes.

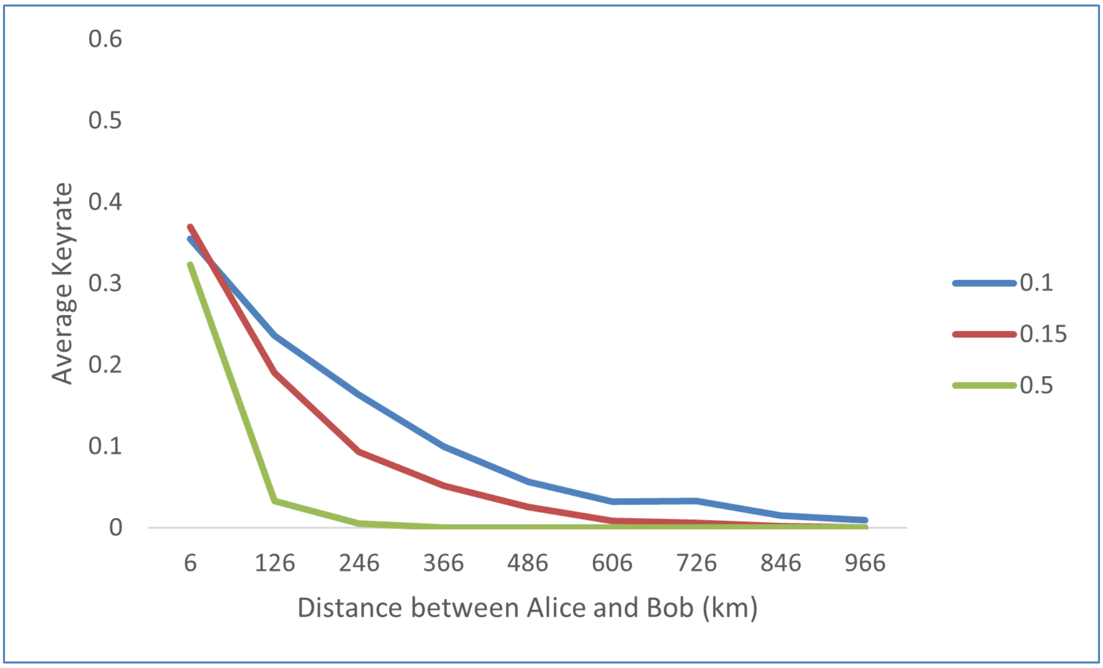


Figure 4.6: This figures shows the key-rates over increasing distance between the Alice and Bob nodes for Coherent one way (COW) protocol under the presence of Ideal Quantum Repeater nodes.

Fig(4.5, 4.6) shows varying key rate performance based on different repeater conditions (ideal vs. non-ideal) and attenuation levels (0.15 dB/km and 0.5 dB/km), resulting in distinct outcomes. When using ideal repeaters, the graph shows a greater and more consistent key rate over different distances, even when there is a higher level of attenuation at 0.5 dB/km. The effects of attenuation are effectively reduced, resulting in a gradual decrease in the key rate. This ensures that the key rate remains at a feasible level even over long distances. This emphasizes the effectiveness of ideal repeaters in maintaining the integrity and efficiency of quantum key distribution. Conversely, the non-ideal repeaters demonstrates a more significant decrease in key rates, especially at the higher level of attenuation of 0.5 dB/km. Here, the rate of change decreases significantly after the initial distances and levels off at a lower rate much earlier. The rapid decline in performance suggests that non-ideal repeaters have a limited ability to mitigate the keys being tampered or altered or lost over increased distance.

4.3 Three-stage Protocol

In this section, we will delve into the results concerning the simulation of the three-stage protocol modeled over SeQUeNCe. We simulate several distances between Alice and Bob nodes and calculate key-rates and Quantum Bit Error Rate (QBER) over these distances.

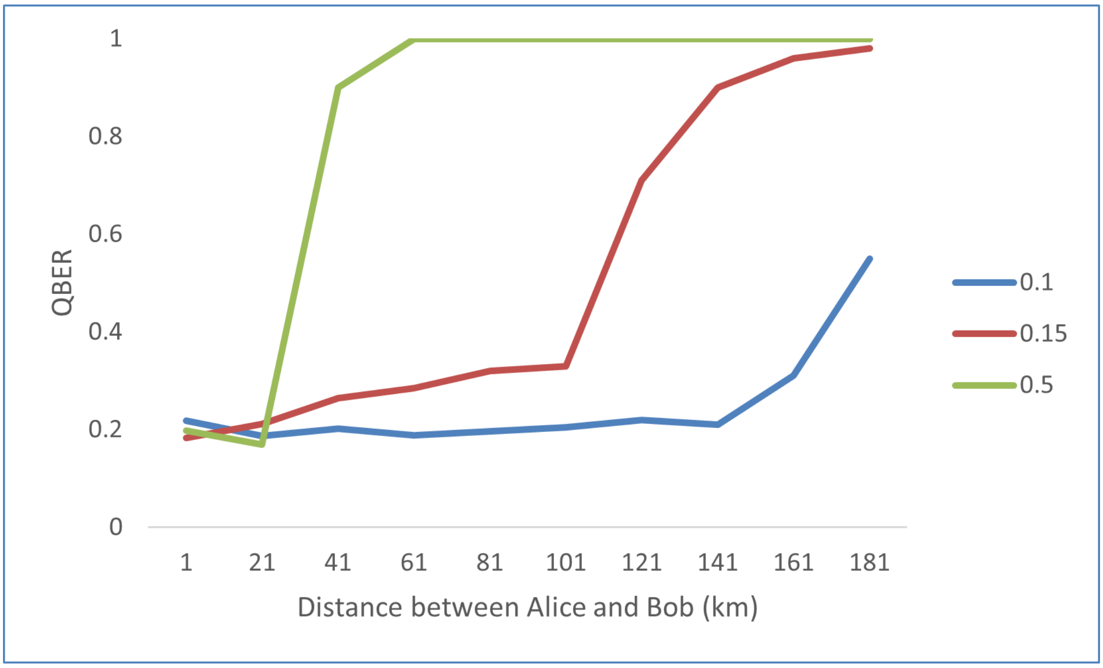


Figure 4.7: This graph displays the QBER across varying distances for attenuation levels of 0.1, 0.15, and 0.5 dB/km, highlighting the effects of attenuation on error rates in quantum key distribution for 3 stage over a P2P network.

Fig(4.7) shows the results for p2p connection for three stage protocol. The QBER graph depicts, the attenuation level of 0.15 dB/km, the error rates for the QBER are still manageable even over long distances. This indicates that the 3-stage protocol's design has a strong capacity for correcting errors. The protocol's effectiveness in maintaining lower error rates confirms the high level of performance, thus improving the security of quantum communications. Nevertheless, when the attenuation rate reaches 0.5 dB/km, the QBER experiences a substantial increase, highlighting the protocol's susceptibility to greater optical losses. These losses further increase error rates and reduce the feasibility of long-range quantum communication.

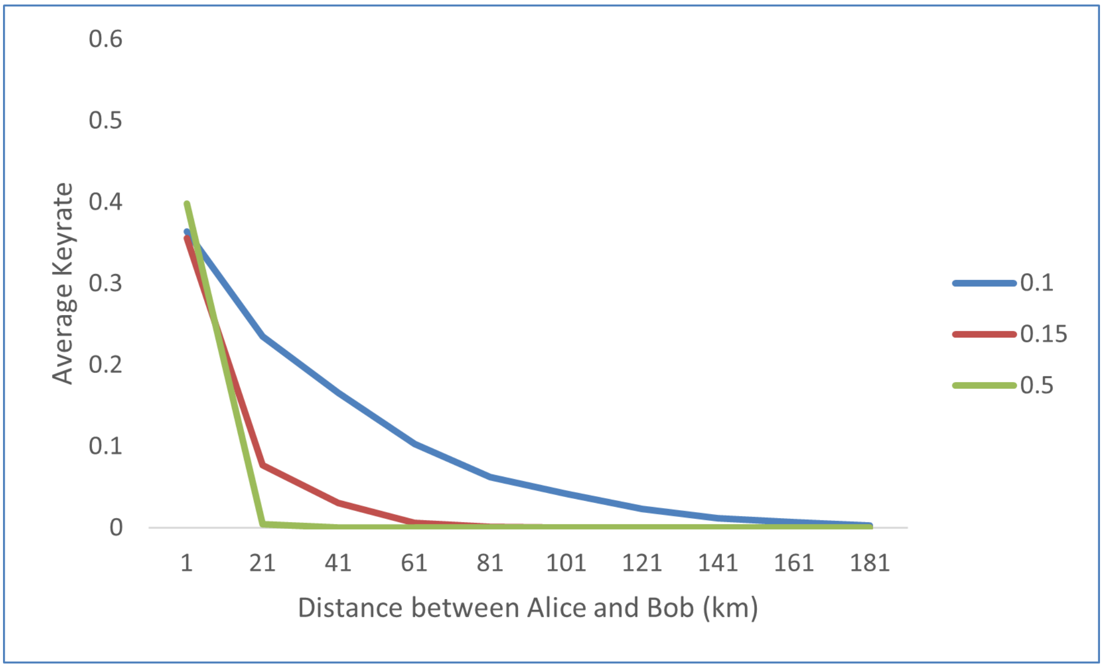


Figure 4.8: Graph illustrating the decline in Average Key Rate with increasing distance for different attenuation values in a quantum key distribution system for 3 stage over a P2P network.

Fig(4.8) graph illustrating the performance of the key rate under the 3-stage protocol shows a significant reliance on the levels of attenuation. With a gradual decrease of 0.15 dB/km, the key rate diminishes, enabling a sustainable exchange of keys over longer distances. This is essential for the practical implementation of quantum cryptography. This demonstrates the effectiveness of the protocol in preserving quantum key distribution despite inherent losses in the system. On the other hand, when the attenuation is 0.5 dB/km, the key rate decreases significantly, suggesting that the system has a limited operational range under higher attenuation. The significant decrease in value highlights the need to reduce fiber losses in quantum networks in order to enhance the efficiency of key rate and achieve the highest level of communication security and range.

4.3.1 Three-stage with Quantum Repeater Nodes

In this section, we introduce quantum repeaters in an attempt to increase the distance of the stable transmission. We use two types of repeaters for this, *ideal repeaters* and *non-ideal repeaters.* [2]

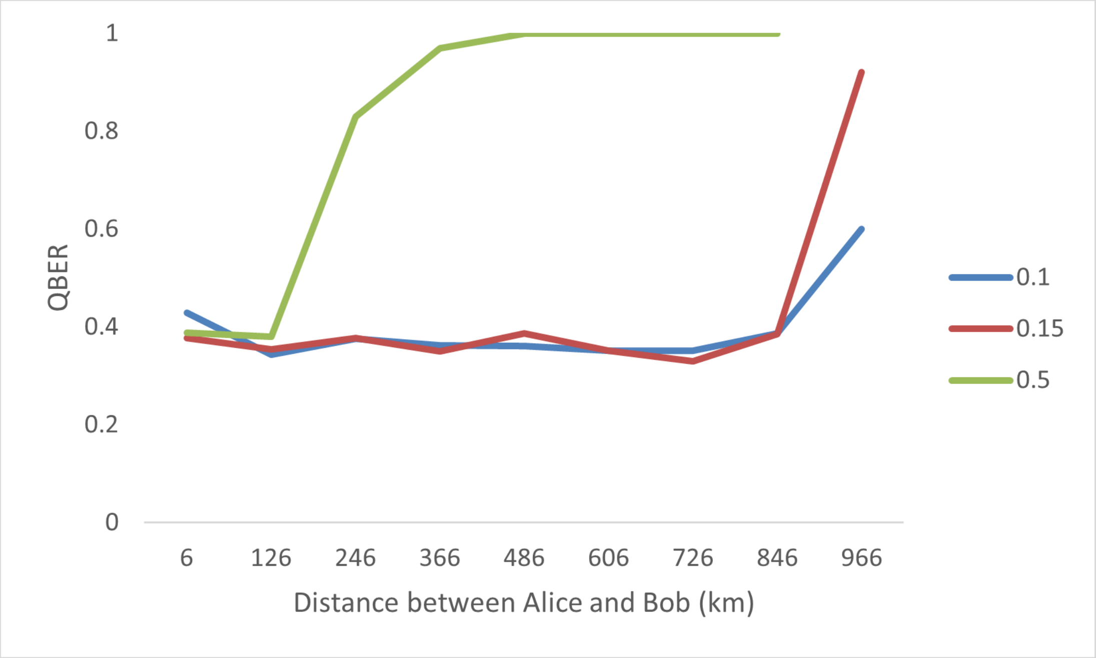


Figure 4.9: This figure shows the QBER over increasing distance between the Alice and Bob nodes for the three-stage protocol under the presence of Non-ideal Quantum Repeater nodes.

[2] In the context of this paper, ideal repeaters provide no extra noise to the system and qubits also avoid facing any attenuation errors when passing through these repeater nodes. Whereas, non-ideal repeaters acts like every other node in the system, and only benefit is the no attenuation loss to the qubits passing through.

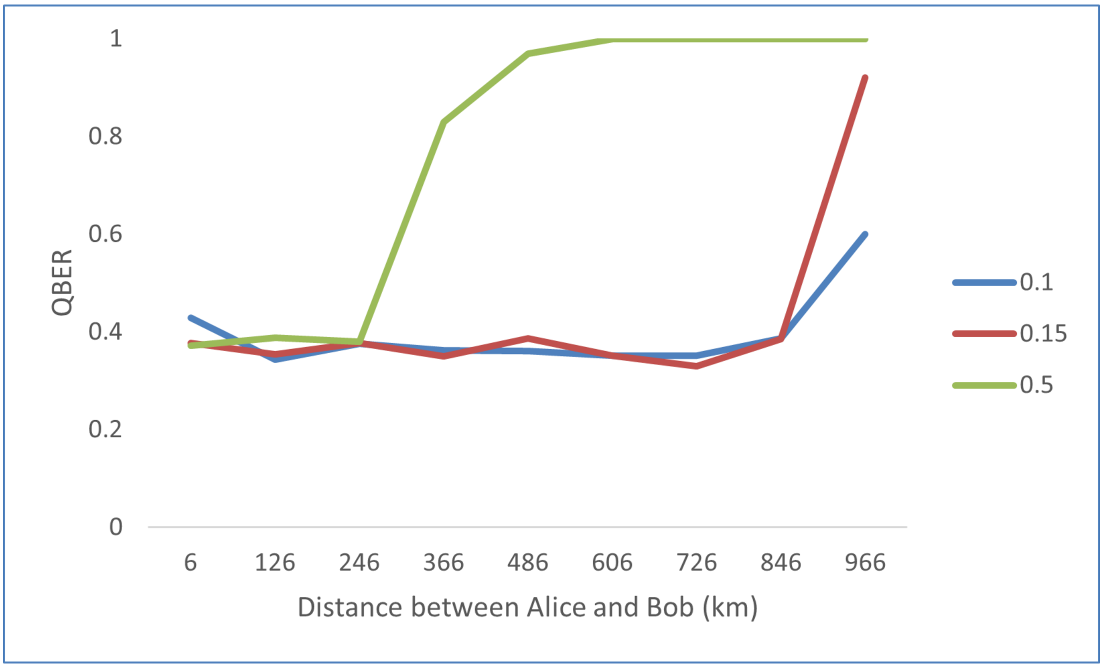


Figure 4.10: This figure shows the QBER over increasing distance between the Alice and Bob nodes for three-stage protocol under the presence of ideal Quantum Repeater nodes.

Fig(4.9), Fig(4.10) graphs illustrate the Quantum Bit Error Rate (QBER) for the 3-stage protocol in both ideal and non-ideal quantum repeater scenarios. These graphs clearly show the significant impact of repeater quality at different levels of attenuation, specifically 0.15 dB/km and 0.5 dB/km. The non-ideal quantum repeaters graph illustrates that the quantum bit error rate (QBER) remains relatively low for shorter distances, but increases significantly as the distance increases, especially at an attenuation level of 0.5 dB/km. This indicates that non-ideal repeaters have limited capability to fully correct errors over longer distances. In contrast, the ideal repeater, consistently exhibits a significantly lower QBER at all distances. This demonstrates the remarkable ability of ideal repeaters to fully restore quantum states and reduce errors, even when faced with higher levels of attenuation. The significant difference between the two scenarios emphasizes the crucial importance of advanced repeater technologies in prolonging the effectiveness and dependability of long-distance quantum communications within the 3-stage protocol

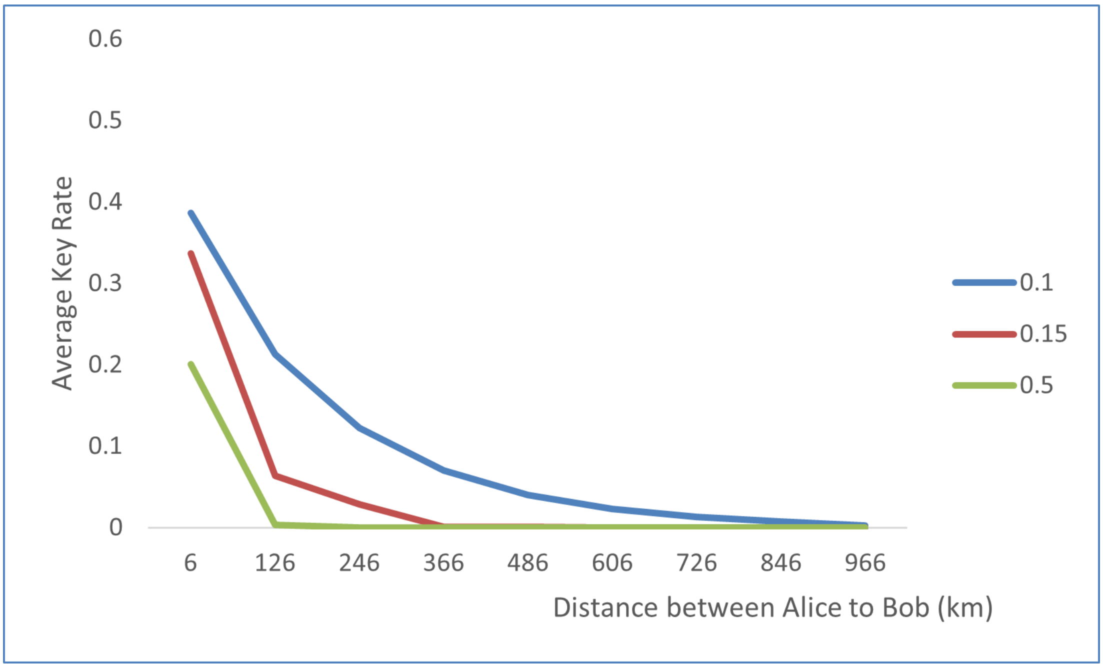


Figure 4.11: This figures shows the key-rates over increasing distance between the Alice and Bob nodes for three-stage protocol under the presence of Non-ideal Quantum Repeater nodes.

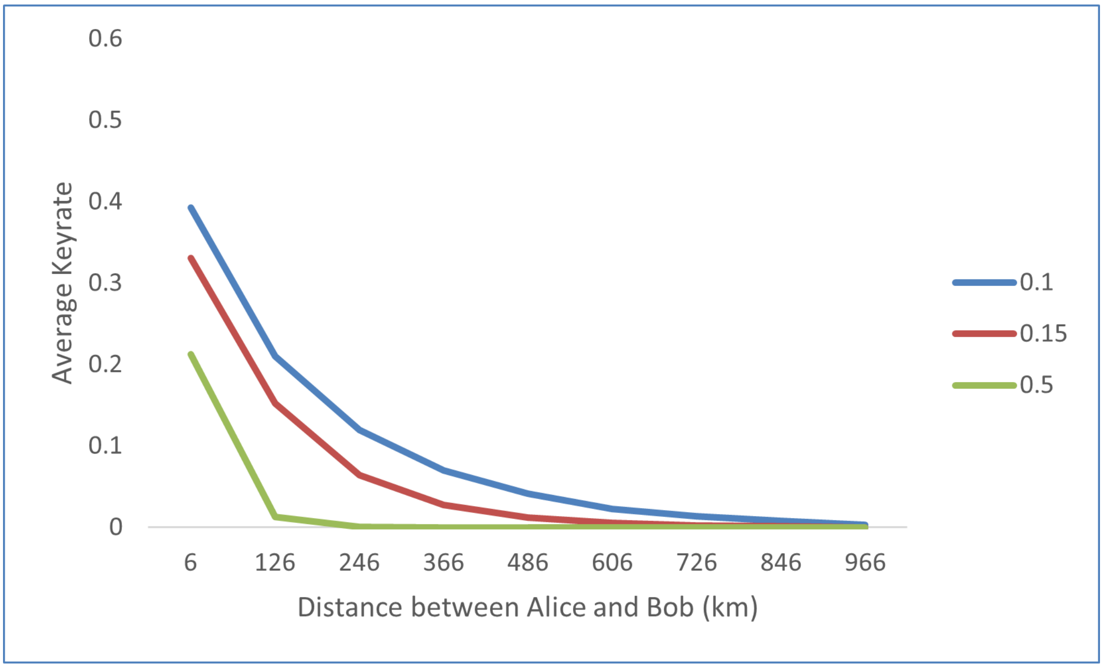


Figure 4.12: This figures shows the key-rates over increasing distance between the Alice and Bob nodes for three-stage protocol under the presence of ideal Quantum Repeater nodes.

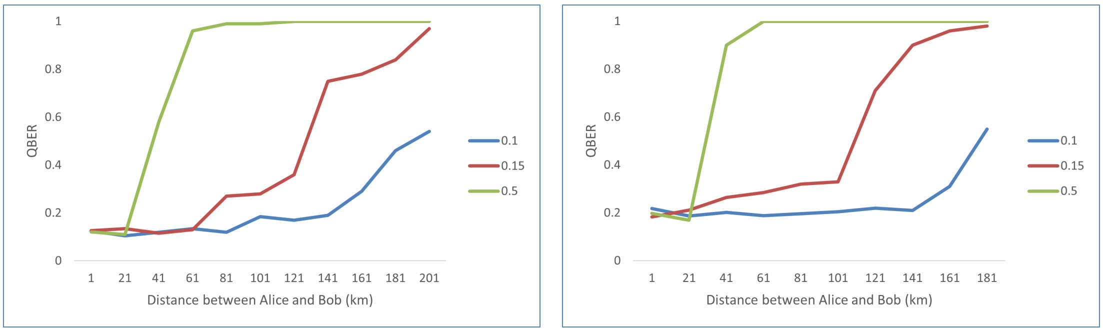
Fig(4.11), Fig(4.12) illustrate the key rate at which data is transmitted in a 3-stage quantum communication protocol, comparing the performance of ideal and non-ideal quantum repeaters. Specifically, analyze the impact of attenuation levels of 0.15 dB/km and 0.5 dB/km. The ideal repeater graph illustrates for a quantum repeater, where the key rate remains consistently high at all distances and even exhibits a gradual decrease at higher levels of attenuation (0.5 dB/km). This suggests that ideal repeaters successfully prevent the qubits being lost or tampered over the network, thus preserving a higher rate of data transmission over greater distances. This is crucial for the reliability and security of quantum communication networks. Conversely, non-ideal repeaters demonstrates a faster decline in key rates at both levels of attenuation, especially at 0.5 dB/km. The steeper decline is due to the limited ability of non-ideal repeaters to compensate for the loss and errors caused by noises. This leads to significantly lower key rates, which undermines the effectiveness and reliability of quantum key distribution as the distance increases.

4.4 Comparison of the Protocols

This section provides a comparative analysis [32] of the performance disparities between the Coherent One-Way (COW) protocol and the Three-Stage protocol in a quantum key distribution (QKD) network. This analysis is based on graphical data and considers different noise conditions. These graphical analyses provide a data-driven perspective on the performance of each protocol in terms of key rate and quantum bit error rate (QBER) as a function of distance, considering various levels of attenuation.

4.4.1 QBER Analysis

P2P analysis on COW and Three-stage



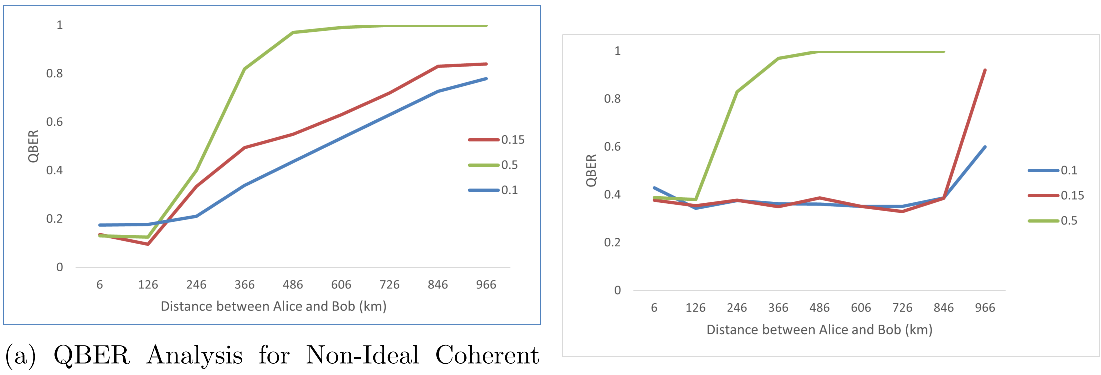
(a) QBER Performance of Coherent One-Way (COW) Protocol demonstrating superior long-distance performance with consistently lower QBER across a range of distances and attenuation levels (0.1, 0.15, and 0.5 dB/km), showcasing its effectiveness for reliable quantum communications.

(b) QBER Performance in a 3-Stage Protocol illustrates the Quantum Bit Error Rate (QBER) for a 3-stage protocol across different attenuation levels (0.1, 0.15, and 0.5 dB/km), highlighting the rapid increase in QBER at greater distances, particularly under higher attenuation conditions.

Figure 4.13: Comparative Analysis of Quantum Bit Error Rates (QBER) across P2P transmission

Fig (4.13a, 4.13b) shows significant differences in their effectiveness for peer-to-peer quantum communications. The 3-stage protocol effectively maintains a low Quantum Bit Error Rate (QBER) at shorter distances, demonstrating satisfactory performance at both levels of attenuation. However, when the distance is extended, particularly with a higher attenuation rate of 0.5 dB/km, the quantum bit error rate (QBER) increases rapidly. This indicates that the protocol has limitations in effectively managing error rates over long distances. Unlike the 3-stage protocol, the COW protocol maintains a lower QBER at short distances and also performs much better at longer ranges. Despite an extremely noisy condition of 0.5 dB/km, COW exhibits a relatively lower QBER, highlighting its superior ability to handle errors and maintain communication integrity over longer distances.

Non-ideal QR analysis on COW and Three-stage



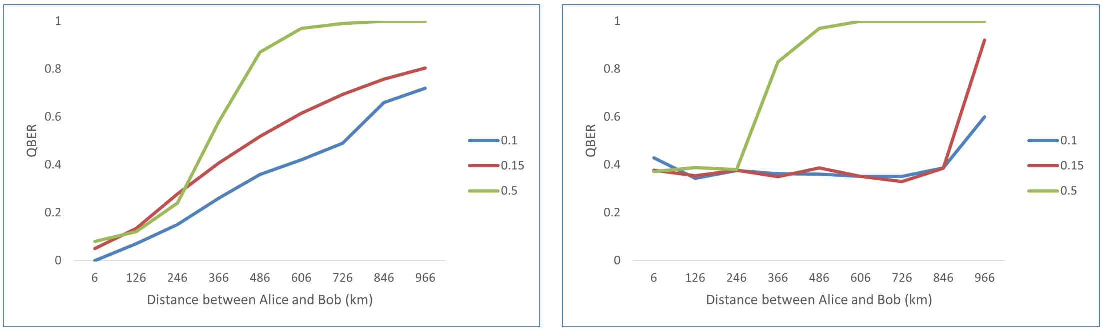
(a) QBER Analysis for Non-Ideal Coherent One-Way (COW) Protocol: Displaying QBER for the COW protocol in non-ideal conditions at attenuation levels of 0.1, 0.15, and 0.5 dB/km. The graph showcases the COW protocol's effective error management, maintaining lower QBER over a broader range of distances and under various attenuation levels, emphasizing its suitability for extended quantum communication networks.

(b) QBER Analysis for Non-Ideal 3-Stage Protocol illustrates the Quantum Bit Error Rate (QBER) across different attenuation levels (0.1, 0.15, and 0.5 dB/km) for a non-ideal 3-stage protocol. It highlights the protocol's rapid increase in QBER with extended distances, especially under higher attenuation, pointing out its limitations in long-range quantum communications.

Figure 4.14: Comparative Analysis of Quantum Bit Error Rates (QBER) across non-ideal QR transmission

The comparison of the Quantum Bit Error Rate (QBER) between non-ideal 3-stage 4.14b and Coherent One-Way (COW) protocols 4.14a, specifically at attenuation levels of 0.15 and 0.5 dB/km, demonstrates clear differences in the performance characteristics of quantum communication. The 3-stage protocol graph, which is not ideal, demonstrates that the QBER (Quantum Bit Error Rate) remains relatively low when the distance is shorter. However, as the distance increases, the QBER experiences a rapid increase, particularly when there is a higher attenuation of 0.5 dB/km. This indicates that its effectiveness is limited when used over long distances with significant signal loss. On the other hand, the COW protocol, even in a less than ideal situation, demonstrates a greater ability to consistently maintain a lower QBER (Quantum Bit Error Rate) over a wider range of distances. Significantly, even when the attenuation is increased, the rise in QBER (Quantum Bit Error Rate) occurs more gradually, emphasizing its resilience in managing errors. Hence, the COW protocol is deemed as the superior choice for quantum communications over both short and long distances, especially in situations with higher optical losses.

Ideal QR analysis on COW and Three-stage



(a) Quantum Bit Error Rate (QBER) trends for ideal 3-stage quantum repeaters across varying distances, showing the impact of different attenuation rates (0.1, 0.15, and 0.5).

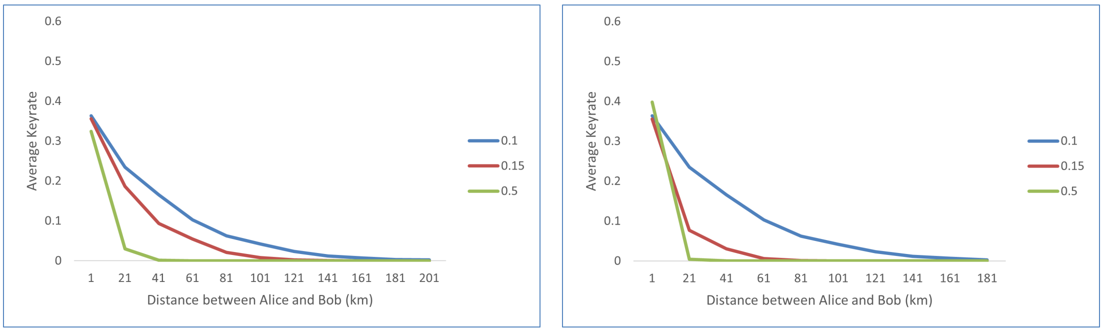
(b) Quantum Bit Error Rate (QBER) performance for ideal Coherent One-Way protocol across multiple distances, illustrating the effects of attenuation levels (0.1, 0.15, and 0.5).

Figure 4.15: Comparative Analysis of Quantum Bit Error Rates (QBER) across ideal QR transmission

The Quantum Bit Error Rate (QBER) trends of the ideal 3-stage 4.15b and Coherent One-Way (COW) 4.15a protocols exhibit significant differences, especially at attenuation levels of 0.15 and 0.5. When considering shorter distances, the 3-stage protocol consistently exhibits a lower QBER (Quantum Bit Error Rate) at all levels of signal attenuation compared to COW, demonstrating its strong performance in minimizing errors even under high levels of attenuation. Nevertheless, as the distance becomes greater, the COW protocol demonstrates a more gradual rise in QBER, especially at the standard attenuation of 0.15, highlighting its superior durability over extended distances. The difference shows the potential of the COW protocol for long-distance quantum communications, where it is important to maintain low error rates. On the other hand, the 3-stage approach is more efficient for shorter distances, where lower attenuation is a significant factor.

4.4.2 Key Rate Performance

P2P analysis on COW and Three-stage



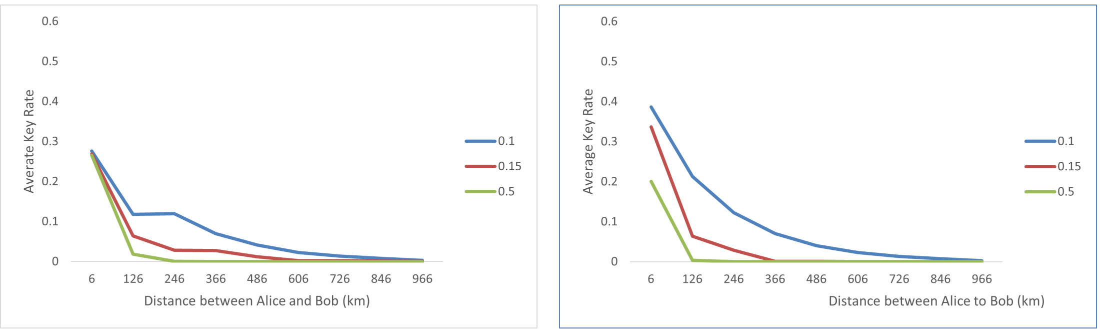
(a) Key Rate Analysis for the COW protocol demonstrates the average key rates for attenuation levels (0.1, 0.15, and 0.5) across various distances, showcasing the protocol's resilience and efficiency in maintaining higher key rates over significant distances.

(b) Key Rate Analysis for the 3-Stage Protocol illustrates the average key rates for the 3-stage protocol with attenuation levels of 0.1, 0.15, and 0.5. The graph highlights the protocol's performance and its capability to sustain viable key rates up to a certain distance.

Figure 4.16: Comparative Analysis of Keyrate across P2P transmission

Upon evaluating the keyrate of the Coherent One-Way 4.16a and the 3-Stage 4.16b protocols at attenuations of 0.15 and 0.5, numerous findings arise regarding their effectiveness at varying distances. With an attenuation of 0.15, the 3-Stage protocol initially provides a greater keyrate at shorter distances (up to 21 km). However, its performance rapidly declines beyond this range, reaching minimal levels at approximately 61 km. On the other hand, the COW protocol initially operates at a lower keyrate when the distance is short, but it undergoes a more gradual decrease, allowing it to maintain its effectiveness up to approximately 121 km with the same level of attenuation. When the attenuation is increased to 0.5, the 3-Stage protocol once again demonstrates its superiority at short distances. However, it experiences a significant decrease in keyrates and approaches 0 at around 61 km. In contrast, the COW protocol, although it has a slower initial speed, demonstrates superior durability by sustaining measurable keyrates over longer distances. The observed trend indicates that the COW protocol outperforms the 3-Stage protocol in long-distance quantum key distribution, especially in environments with higher attenuation, although the latter may be more suitable for shorter distances.

Non-ideal QR analysis on COW and Three-stage



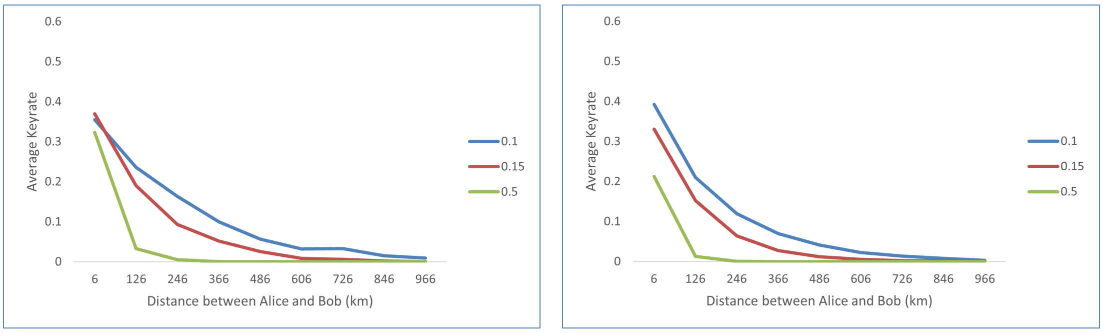
(a) Average Key Rate vs. Distance for Coherent One-Way (COW) Protocol under different attenuations. The lines represent different attenuation levels: 0.1 (blue), 0.15 (red), and 0.5 (green), demonstrating how key rate declines with increasing distance and attenuation.

(b) Average Key Rate vs. Distance for 3-Stage Protocol under different attenuations. the lines represent attenuation levels of 0.1 (blue), 0.15 (red), and 0.5 (green), highlighting the differences in how quickly the key rates decline with increasing distance and higher attenuation.

Figure 4.17: Comparative Analysis of Keyrate across non-ideal QR transmission

The Coherent One-Way (COW) protocol 4.17a and the 3-Stage protocol 4.17b in quantum key distribution systems can be analyzed by comparing their keyrate performance under attenuations of 0.15 and 0.5 at different distances. Regarding the 0.15 attenuation, both protocols initially have similar keyrates at shorter distances. However, the 3-Stage protocol shows a more noticeable decrease as the distance increases, eventually leveling off after 250 km. The COW protocol exhibits a slight advantage in maintaining higher keyrates over longer distances, rendering it more efficient for extended quantum communications in the presence of lower attenuation. With a 0.5 attenuation, the contrast becomes more apparent. Both protocols exhibit a sharp decrease within the first 100 km, but the 3-Stage protocol declines at a faster rate and becomes insignificant beyond this point. On the other hand, the COW protocol, despite having a lower initial keyrate, shows more robustness by maintaining detectable but low keyrates even over longer distances. Based on this analysis, it can be concluded that in situations where there is greater signal loss and longer distances, the COW protocol is more effective than the 3-Stage protocol. The COW protocol provides superior long-term usefulness in difficult transmission conditions.

Ideal QR analysis on COW and Three-stage



(a) Quantum Bit Error Rate (QBER) trends for ideal 3-stage quantum repeaters across varying distances, showing the impact of different attenuation rates (0.1, 0.15, and 0.5).

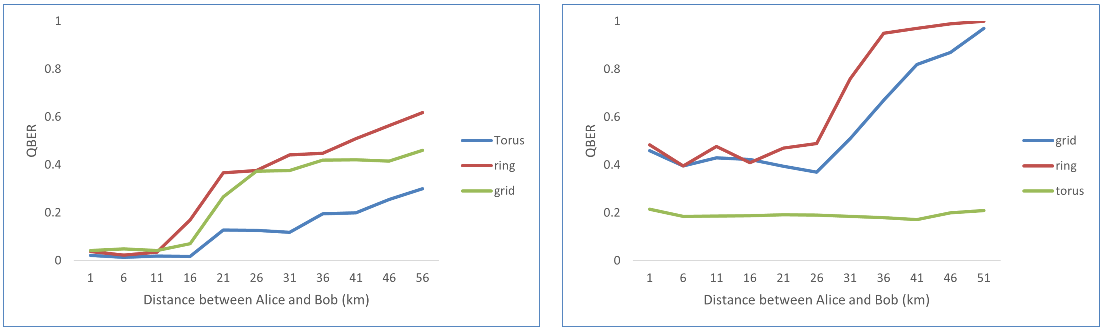
(b) Quantum Bit Error Rate (QBER) performance for ideal Coherent One-Way protocol across multiple distances, illustrating the effects of attenuation levels (0.1, 0.15, and 0.5).

Figure 4.18: Comparative Analysis of Quantum Bit Error Rates (QBER) across ideal QR transmission

The comparative analysis of the Coherent One-Way (COW) protocol4.18a and the 3-Stage protocol4.18b, performed under 0.1, 0.15 and 0.5 attenuations, reveals significant variations in their performances at different distances. The COW protocol exhibits a lower average keyrate at shorter distances compared to 3-stage protocol and shows a more gradual decrease as the distance increases, ultimately outperforming the 3-Stage protocol at longer distances, for the 0.15 attenuation. This demonstrates the enhanced capacity of the COW protocol to maintain efficient quantum key distribution over long distances. However, when faced with a more difficult condition of 0.5 attenuation, both protocols experience notable decreases in keyrate as the distance increases. Nevertheless, the COW protocol manages to maintain a high keyrate for a longer distance compared to the 3-Stage protocol, which reaches almost zero keyrates much earlier. The ability of the COW protocol to remain effective even under high attenuations and over long distances highlights its potential for reliable long-distance quantum communications, especially in situations where maintaining the key integrity is crucial.

4.5 Comparison over Different Topologies

This section provides a detailed comparison of how various network structures impact crucial parameters in quantum communication systems. This analysis is required due to the basic difficulties with quantum key distribution (QKD). This section aims to determine the optimal network topology, such as a ring or a grid, that can provide lower error rates and higher transmission capacities. These factors are crucial to the successful implementation of QKD.



(a) QBER in a COW protocol topology. The torus topology remains stable and low, while the ring and grid experience significant increase.

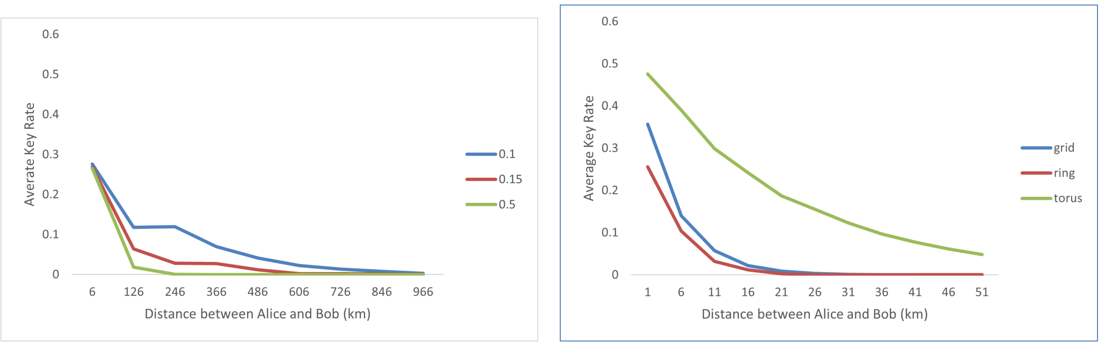
(b) QBER in a 3-stage protocol topology. The graph shows a consistent trend across distances, with a steep rise in QBER values for grid and ring topologies.

Figure 4.19: Comparative Analysis of COW and 3-stage QBER Across Different Topologies

Fig(4.19a) exhibits a clear performance pattern among the three topologies: grid, ring, and torus. At the beginning, all three topologies exhibit low QBER values, which suggests excellent performance over shorter distances. However, as the distance expands, both the grid and ring topologies start to encounter an increase in QBER (Quantum Bit Error Rate) from approximately 16 kilometers onwards, indicating a significant susceptibility to errors caused by distance. In contrast, the torus topology is notable for its stability, as it consistently maintains a low QBER (Quantum Bit Error Rate) across all distances tested. The torus topology's strong performance indicates that it may be better suited for meeting the requirements of the COW protocol. This is likely due to its ability to reduce decoherence and other errors in quantum communication over longer distances.

Fig(4.19b) exhibits that although all three topologies initially have comparable and low QBER values, the grid and ring topologies only experience noteworthy increases in QBER after surpassing a distance of 31 kilometers. The torus topology once again exhibits a gradual and consistent rise in QBER, further confirming its effectiveness in efficiently handling long-distance quantum communications. The graph highlights a crucial feature of the 3-stage protocol's capacity to sustain lower error rates over a greater initial distance compared to the COW protocol.

Fig(4.19) compares the QBER (Quantum Bit Error Rate) between the 3-stage and COW protocols shows an important difference in the initial error rates and how they change as the distance increases. The 3-stage protocol begins with considerably elevated QBER levels, approximately 0.4 for grid and ring topologies, indicating a notable initial vulnerability to errors. On the other hand, the COW protocol demonstrates superior initial error management by starting with almost no QBER in all topologies. As the distance between the protocols increases, the Quantum Bit Error Rate (QBER) in both protocols also increases. However, the COW protocol shows a more consistent and gradual increase, which is particularly noticeable in the torus topology where the QBER remains consistently low. The comparison emphasizes the effectiveness of the COW protocol in maintaining quantum coherence over extended distances, rendering it more appropriate for applications that require low error rates to ensure dependable quantum communication.



(a) QBER in a COW protocol topology. The torus topology remains stable and low, while the ring and grid experience significant increase.

(b) QBER in a 3-stage protocol topology. The graph shows a consistent trend across distances, with a steep rise in QBER values for grid and ring topologies.

Figure 4.20: Comparative Analysis of Quantum Bit Error Rates (QBER) Across Different Topologies

Fig(4.20a) illustrates the average key rates for various topologies utilizing the Coherent One-Way (COW) protocol. At the beginning, all three topologies (torus, ring, and grid) exhibit high key rates, suggesting effective quantum key distribution (QKD) over short distances. As the distance between Alice and Bob increases, all topologies exhibit a decrease in key rates. However, the torus topology demonstrates the slowest decline, thereby maintaining a higher key rate over longer distances. These findings indicate that the COW protocol, especially when implemented with the torus topology, is able to maintain a higher level of efficient quantum communication as the distance between parties involved increases.

Fig(4.20b) illustrates the key rates according to the Three-Stage protocol, revealing that the initial key rates are significantly higher compared to the COW protocol for all topologies. Once again, the torus demonstrates its superior effectiveness, although its initial advantage diminishes more rapidly when compared to its performance in the COW protocol. With increasing distance, both the grid and ring topologies experience a substantial decrease in key rate, demonstrating an even greater reduction compared to the gradual decrease observed in the COW protocol.

Fig(4.20) shows that the Three-Stage protocol has higher initial key rates. However, the decline in key rates is more significant and faster, especially for the grid and ring topologies. This suggests that the protocol may be less effective in maintaining key rate integrity over longer distances. In contrast, the COW protocol exhibits a more consistent and controlled decrease in key rates, making it a more suitable option for long-range applications that require a stable and reliable key rate. In both protocols, the torus topology consistently outperforms other topologies by maintaining higher key rates for longer periods.

4.6 A Brief Summary of the Results

To summarize, a comprehensive comparison is conducted between the Coherent One-Way (COW) and Three-Stage protocols in quantum key distribution, focusing on their individual performances under various distances and attenuation scenarios. At shorter distances, the Three-Stage protocol exhibits superior key rates and marginally improved error management (QBER), indicating its efficacy in nearby, less attenuated settings. However, when the distance is extended, the COW protocol demonstrates superior long-range abilities. It effectively handles a slow decrease in key rates and sustains a lower QBER compared to the Three-Stage protocol. This indicates that the COW protocol is robust in extended quantum communications, particularly in situations with higher attenuation. The COW protocol is well-suited for situations where dependable long-range communication is essential, due to its capacity to maintain keyrate integrity and security over extended distances. On the other hand, the Three-Stage protocol, while initially efficient, encounters substantial difficulties in sustaining performance over longer distances and in the presence of severe attenuations. This results in a more rapid decline in both the rate at which encryption keys are generated and the level of security provided. Therefore, although the Three-Stage protocol may be favored for short-distance applications that demand a high initial keyrate and low QBER, the COW protocol is the more feasible choice for long-distance quantum communications.

Chapter 5

Future Works

This section describes the progress and additional exploration of the thesis. Within the realm of quantum communication, future works include a wide range of objectives that aim to enhance the effectiveness, confidentiality [38], and expanding the research several of quantum technology.

5.1 Multi-Photon Implementation

Multi-photon quantum key distribution (QKD) can improve the efficiency and reliability of quantum communication systems by utilizing the characteristics of multiphoton states to address problems associated with the loss of photons and decoherence. These issues are commonly encountered in single-photon QKD systems. Multi-photon systems exhibit enhanced resistance against specific forms of eavesdropping attacks, such as beam-splitting, due to the distribution of quantum information across multiple photons. This distribution renders it hard for an eavesdropper to acquire comprehensive information without being detected.

Moreover, multiphoton quantum key distribution (QKD) has the capacity to significantly enhance the rate at which cryptographic keys are generated. The reason for this is the capacity of multiphoton states to transmit more of information per quantum state in comparison to single-photon systems. Moreover, the utilization of multiphoton states has the potential to enhance the reliability of quantum communication over extended distances, thus addressing a significant drawback of existing QKD technologies that are constrained by limited range caused by optical losses.

5.2 Quantum Network with two quantum channels

There are many efficiency and privacy issues related to the designs of various practical quantum networks. We propose the introduction of a second quantum channel that can only be used over a small distance but is of high quality, i.e. it has low noise and it is an *authenticated* channel. We assume that there will not be any attacker reducing the quality of the channel. Consider Fig(5.1), we consider a quantum network consisting of six nodes, the first being Alice and the last being Bob's nodes respectively.

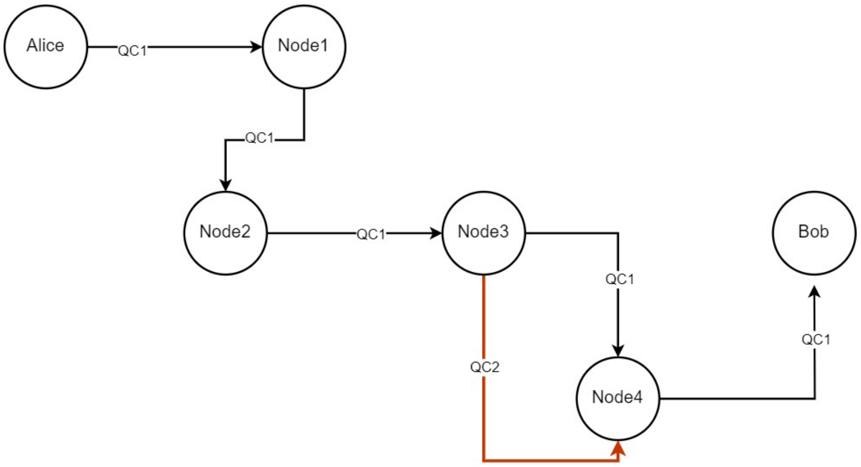


Figure 5.1: A scenario for the use of a second quantum channel in a quantum network

We define the method to determine the introduction of the second quantum channel as follows,

1. We run a QKD protocol over the entire network of six nodes to determine the quantum bit error rate (QBER) for the entire system. We keep repeating the network round measurements and determine the highest bound of the QBER for this network simulation. For further discussion, we will refer to it as global QBER

or Q_{G}.

2. We need to determine the connections between the nodes that have unusually high uncertainty, which may indicate the presence of an attacker or a very highly noisy channel. Both of which will reduce the quality and security of the transmission. To deal with this, we perform a standard QKD run over individual edges, for example, BB84. This will help us identify the QBER for individual edges. We refer to these as Q_1, Q_2, Q_3, and Q_4.

3. We need to define a relative security measurement parameter; we call it relative QBER and mathematically we can define it as

$$Q_{\mathcal{R}} = \frac{\sum\limits_{i=0}^{n} Q_{\mathrm{i}}}{Q_{\mathrm{G}}}, \tag{5.1}$$

   where Q_{i} is the individual QBER for the node edges determined using the standard QKD protocol and Q_{G} is the global QBER for the entire network.

4. Now that we have defined a normalized QBER of each edge with respect to the global QBER. We now define the connection of some nodes with the second quantum channel.

```
for i in range(nodes):
    if Q_i > Q_R:
        connect QC_2 and connect QC_1
    else:
        connect QC_1
```

5. For our example, we see from Fig(5.1) that QBER between node 3 and nodes 4 exceeds the $Q_{\mathcal{R}}$, thus the edge is also connected by the second quantum channel. This second channel is authenticated; however, the bandwidth is lower than the main channel. There can be two approaches to move further,

   - **Store and Send**: All communication will be shifted from the main channel to the secondary channel over this path. However, this node stores the qubits and sends them in smaller packet sizes to accommodate the bandwidth.

- **Error Correction Channel**: This can be used as an error correction channel. A small bit sequence can be shared over both channels and it can be integrated with ongoing sequence to mitigate some errors. This step can be used in the security amplification step of the QKD too.

5.3 3d Topology

The illustrated network topology, Fig(5.2) represents a sophisticated 3D communication model that streamlines data transmission between two interconnected ground networks by leveraging satellite technology[21, 29, 54]. Both Ground Network A and Ground Network B have networks with an interconnected node system, where all nodes within each network are connected to each other, creating a strong intra-network communication framework. In a conventional 2D network topology, transmitting data from Alice in Network A to Bob in Network B would require multiple terrestrial hops. Specifically, the data would travel from Alice to Node 2 in Network A, then to Node 4 in Network B via an established direct ground link, and finally reach Bob.

Nevertheless, the suggested 3D topology utilizes a satellite as a relay in order to enhance and expedite this process. Alice can transmit data directly to the satellite, bypassing the need to go through multiple intermediate nodes. The satellite then promptly forwards the data to Bob, completely avoiding any connections with ground-based nodes. This approach greatly reduces the number of intermediate steps that data must go through, resulting in a decrease in the time it takes for data to travel, a reduction in the likelihood of errors during transmission, and an improvement in the overall efficiency of the network.

The efficient technique of transmitting data through satellites is particularly advantageous in situations that demand quick and dependable communication, such as disaster

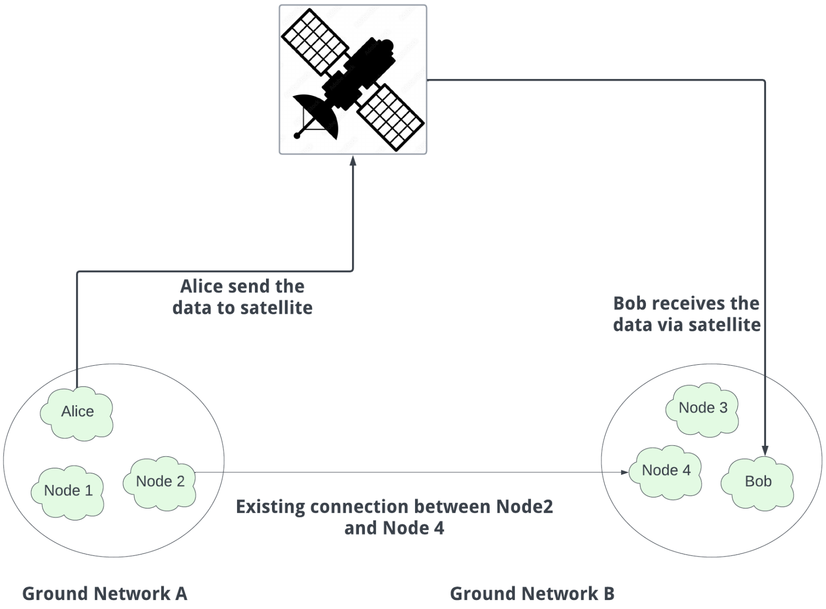

Alice send the data to satellite
Bob receives the data via satellite
Alice
Node 1
Node 2
Node 3
Node 4
Bob
Existing connection between Node2 and Node 4
Ground Network A
Ground Network B

Figure 5.2: Pictorial representation of a sample 3d topology. Assuming Ground Network A is interconnected and so does Ground Network B.

response, global financial transactions, or in remote regions with limited or unreliable ground infrastructure. In addition, the network attains enhanced security by utilizing satellites, as the data transmitted is less susceptible to interception in comparison to multiple ground node transfers. Implementing a 3D topology that integrates satellite technology is a major advancement compared to traditional 2D network models. This solution provides improved resilience, flexibility, and efficiency in managing the growing complexities and requirements of global data communications.

Chapter 6

Conclusion

Overall, the thorough assessment of the Coherent One-Way (COW) and Three-Stage protocols in quantum key distribution (QKD) has greatly enhanced the understanding of secure quantum networks. This study offers a precise illustration of the performance of each protocol under different levels of noise and quantum bit error rate (QBER). It serves as an essential reference for the development of future quantum communication infrastructure.

The COW protocol exhibited exceptional efficiency [34, 42] in consistently maintaining a low QBER (Quantum Bit Error Rate) over different distances, thereby demonstrating its ability to operate effectively in large-scale fiber network environments. This feature renders it especially beneficial for applications that require fast and dependable quantum communication without the necessity of excessively intricate error correction mechanisms. The COW protocol's simplicity and efficiency make it especially appealing in settings where speed and reliability are of utmost importance.

Although the Three-Stage protocol has extensive security features, it was determined to be most efficient for shorter distances within the context of this thesis. Although it incorporates important methods for distributing keys and encrypting data to improve security and protect against various forms of quantum noise and eavesdropping, its efficiency [34, 42] decreases more significantly over longer distances compared to the Coherent One-Way (COW) protocol. The Three-Stage protocol is well-suited for quantum networks that operate over shorter distances and require low Quantum Bit Error Rates (QBER) to be maintained.

Both protocols greatly benefit from simulation tools such as SeQUeNCe, which enable thorough examination of their behavior in different scenarios. This thesis highlights the significance of these tools in the development of quantum communication systems that are both more resilient and efficient.

In making the decision between the COW and Three-Stage protocols, it is crucial to consider the network's specific needs, such as the acceptable levels of QBER, the necessary security measures, and the scale of the network. This thesis not only outlines a strategy for improving the protocols discussed, but also establishes the foundation for future advancements in quantum key distribution and secure quantum communications. Acquiring this knowledge is essential for progressing in the field of quantum cryptography and safeguarding quantum communications from potential risks posed by the development of quantum computing.

Bibliography

[1] Bader A. Alohali et al. "A Survey on Cryptography Key Management Schemes for Smart Grid". In: *Journal of Computer Sciences and Applications* 3.3A (2015), pp. 27–39. DOI: 10.12691/jcsa-3-3A-4. URL: https://researchonline.ljmu.ac.uk/id/eprint/3522/.

[2] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. 1984.

[3] V. Bommanapally, M. Subramaniam, and A. Parakh. "Embedding a Problem Graph into Serious Games for Efficient Traversal Through Game Space". In: *IEEE Frontiers in Education Conference*. College Station, TX, USA, Oct. 2023, pp. 1–5.

[4] D. Bouwmeester et al. "Experimental quantum teleportation". In: *Nature* 390.6660 (1997), pp. 575–579.

[5] H. J. Briegel et al. "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication". In: *Physical Review Letters* 81.26 (1998), pp. 5932–5935.

[6] Joseph Burr, Abhishek Parakh, and Mahadevan Subramaniam. "Evaluating different topologies for multi-photon quantum key distribution". In: *SPIE Defense + Commercial Sensing*. Orlando, FL, Apr. 2022.

[7] Joseph Burr, Abhishek Parakh, and Mahadevan Subramaniam. “Quantum Internet”. In: *ACM Ubiquity* 2022 (Aug. 2022), pp. 1–14. URL: https://dl.acm.org/doi/10.1145/3547493.

[8] L. Cimini. “Analysis and Simulation of a Digital Mobile Channel Using Orthogonal Frequency Division Multiplexing”. In: *IEEE Transactions on Communications* 33.7 (1985), pp. 665–675. DOI: 10.1109/TCOM.1985.1096357.

[9] Sheila Cobourne. *Quantum Key Distribution Protocols and Applications*. MSc Dissertation RHUL-MA-2011-05. Available online: https://d1wqtxts1xzle7.cloudfront.net/58693536/RHUquantum-thesis-libre.pdf. Royal Holloway, University of London, Mar. 2011.

[10] W.J. Dally and C.L. Seitz. “The torus routing chip”. In: *Distributed Computing* (Oct. 1986).

[11] Whitfield Diffie and Martin Hellman. “New directions in cryptography”. In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654.

[12] A. K. Ekert. “Quantum Cryptography Based on Bell’s Theorem”. In: *Physical Review Letters* 67.6 (1991), p. 661.

[13] Nicolas Gisin et al. “Quantum cryptography”. In: *Rev. Mod. Phys.* 74 (1 Mar. 2002), pp. 145–195. DOI: 10.1103/RevModPhys.74.145. URL: https://link.aps.org/doi/10.1103/RevModPhys.74.145.

[14] R. H. Hadfield. “Single-photon detectors for optical quantum information applications”. In: *Nature Photonics* 3.12 (2009), pp. 696–705.

[15] IBM. *Qiskit 0.45 Release Notes*. https://docs.quantum.ibm.com/api/qiskit/release-notes/0.45. Accessed: 2023-10-03. 2023.

[16] Nitin Jha, Abhishek Parakh, and Mahadevan Subramaniam. “Effect of noise and topologies on multi-photon quantum protocols”. In: *Quantum Computing, Communication, and Simulation IV*. Ed. by Philip R. Hemmer and Alan L. Migdall. Vol. 12911. International Society for Optics and Photonics. SPIE, 2024, 129110G. DOI: 10.1117/12.3000586. URL: https://doi.org/10.1117/12.3000586.

[17] Nitin Jha, Abhishek Parakh, and Mahadevan Subramaniam. "Multi-photon 3-Stage QKD for Practical Quantum Networks". In: *Research Square* 1 (2023). DOI: 10.21203/rs.3.rs-3826628/v1.

[18] Richard Jozsa and Noah Linden. "On the role of entanglement in quantum-computational speed-up". In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 459.2036 (2003), pp. 2011–2032.

[19] Subhash Kak. "A Three-Stage Quantum Cryptography Protocol". In: *Foundations of Physics Letters* 19.3 (Apr. 2006), pp. 293–296. ISSN: 1572-9524. DOI: 10.1007/s10702-006-0520-9. URL: http://dx.doi.org/10.1007/s10702-006-0520-9.

[20] H. J. Kimble. "The quantum internet". In: *Nature* 453.7198 (2008), pp. 1023–1030.

[21] Sheng-Kai Liao et al. "Satellite-to-ground quantum key distribution". In: *Nature* 549.7670 (2017), pp. 43–47.

[22] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. "Decoy State Quantum Key Distribution". In: *Physical Review Letters* 94.23 (2005), p. 230504.

[23] N. Lütkenhaus. "Security against individual attacks for realistic quantum key distribution". In: *Physical Review A* 61.5 (2000), p. 052304.

[24] R. Mallipeddi et al. "A Framework for an Intelligent Adaptive Education Platform for Quantum Cybersecurity". In: *IEEE Frontiers in Education Conference*. College Station, TX, USA, Oct. 2023, pp. 1–5.

[25] S. Mishra, K. Thapliyal, A. Parakh, et al. "Quantum anonymous veto: a set of new protocols". In: *EPJ Quantum Technology* 9 (2022), p. 14. DOI: 10.1140/epjqt/s40507-022-00133-2.

[26] Armand Niederberger, Valerio Scarani, and Nicolas Gisin. "Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography". In: *Phys. Rev. A* 71 (4 Apr.

2005), p. 042316. DOI: 10.1103/PhysRevA.71.042316. URL: https://link.aps.org/doi/10.1103/PhysRevA.71.042316.

[27] M. A. Nielsen and I. L. Chuang. "Quantum Computation and Quantum Information". In: (2000).

[28] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[29] Daniel KL Oi et al. "CubeSat quantum communications mission". In: *EPJ Quantum Technology* 4.1 (2017), p. 6. DOI: 10.1140/epjqt/s40507-017-0060-1. URL: https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-017-0060-1.

[30] *Overview of Public Key Cryptography*. Accessed: 2024-04-10. Universidade Lusófona de Humanidades e Tecnologias, n.d. URL: https://netlab.ulusofona.pt/im/teoricas/OverviewPublicKeyCryptography.pdf.

[31] J. W. Pan et al. "Experimental entanglement swapping: Entangling photons that never interacted". In: *Physical Review Letters* 80.18 (1998), p. 3891.

[32] A. Parakh. "A probabilistic quantum key transfer protocol". In: *Security and Communication Networks* 6 (11 2013), pp. 1389–1395.

[33] A. Parakh, P. Chundi, and M. Subramaniam. "An Approach Towards Designing Problem Networks in Serious Games". In: *IEEE Conference on Games*. London, UK, Aug. 2019.

[34] A. Parakh and M. Subramaniam. "Bootstrapped QKD: improving key rate and multiphoton resistance". In: *SPIE Security + Defence: Quantum Technologies and Quantum Information Science*. Berlin, Germany, 2018.

[35] A. Parakh, M. Subramaniam, and P. Chundi. "A Framework for Incorporating Serious Games into Learning Object Repositories through Experiential Learning". In: *HICSS-55*. Jan. 2022.

[36] A. Parakh, M. Subramaniam, and M. Galore. "Galore: A Platform for Experiential Learning". In: *The Journal of the 25th Colloquium for Information Systems Security Education* 2022 (Winter 2022), pp. 62–69.

[37] A. Parakh et al. “A Novel Approach for Embedding and Traversing Problems in Serious Games”. In: *ACM SIGITE Conference on Information Technology Education*. Oct. 2020.

[38] Abhishek Parakh. “Providing variable levels of security in quantum cryptography”. In: *SPIE Conference on Quantum Communications and Quantum Imaging XVI*. San Diego, Aug. 2018.

[39] Abhishek Parakh. “Quantum Teleportation with One Classical Bit”. In: *Nature Scientific Reports* 12 (2022), p. 3392. URL: https://www.nature.com/articles/s41598-022-06853-w.

[40] Abhishek Parakh. “Using fewer qubits to correct errors in three-state QKD protocol”. In: *SPIE Security + Defence: Quantum Technologies and Quantum Information Science*. Berlin, Sept. 2018.

[41] Abhishek Parakh and Mahadevan Subramaniam. “Network routing protocols for multi-photon quantum cryptography”. In: *Proceedings of Quantum Communications and Quantum Imaging XIX*. Vol. 11835. SPIE. Aug. 2021, p. 118350L.

[42] Abhishek Parakh, Pramode Verma, and Mahadevan Subramaniam. “Improving efficiency of quantum key distribution with probabilistic measurement”. In: *International Journal of Security and Networks* 11.1/2 (2016), pp. 37–47.

[43] Abhishek Parakh et al. “Quantum Cryptography Exercise Schedules with Concept Dependencies”. In: *Journal of The Colloquium for Information Systems Security Education* (2020).

[44] M. Peev et al. “The SECOQC quantum key distribution network in Vienna”. In: *New Journal of Physics* 11.7 (2009), p. 075001.

[45] Stefano Pirandola et al. “Advances in Quantum Cryptography”. In: *Advances in Optics and Photonics* 12.4 (2020), pp. 1012–1236.

[46] John Preskill. “Lecture notes for physics 229: Quantum information and computation”. In: *California Institute of Technology* 12 (1998), p. 14.

[47] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. “A method for obtaining digital signatures and public-key cryptosystems”. In: *Communications of the ACM* 21.2 (1978), pp. 120–126.

[48] Nasir Saeed et al. “Point-to-Point Communication in Integrated Satellite-Aerial 6G Networks: State-of-the-Art and Future Challenges”. In: *IEEE Open Journal of the Communications Society* 2 (2021), pp. 1505–1525. DOI: 10.1109/OJCOMS.2021.3093110.

[49] N. Sangouard et al. “Quantum repeaters based on atomic ensembles and linear optics”. In: *Reviews of Modern Physics* 83 (2011).

[50] Soumya Sarkar. *Tensor Networks and Quantum Error-Correcting Codes*. https://www.quantumofgravity.com/blog/wp-content/uploads/2023/03/Soumya-Sarkar-Tensor-Networks-and-Quantum-Error-Correcting-Codes-Aug-21-2021.pdf. 2021.

[51] V. Scarani et al. “The security of practical quantum key distribution”. In: *Reviews of Modern Physics* 81.3 (2009), p. 1301.

[52] Ronald W. Schafer. “What Is a Savitzky-Golay Filter? [Lecture Notes]”. In: *IEEE Signal Processing Magazine* 28.4 (2011), pp. 111–117. DOI: 10.1109/MSP.2011.941097.

[53] Mehrdad S. Sharbaf. “Quantum cryptography: An emerging technology in network security”. In: *2011 IEEE International Conference on Technologies for Homeland Security (HST)*. 2011, pp. 13–19. DOI: 10.1109/THS.2011.6107841.

[54] Srihari Sivasankaran et al. “A CubeSat platform for space based quantum key distribution”. In: *2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*. 2022, pp. 51–56. DOI: 10.1109/ICSOS53063.2022.9749724.

[55] Damien Stucki et al. “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres”. In: *New Journal of Physics* 11.7 (2009), p. 075003.

[56] P. Subramaniam and A. Parakh. “A quantum Diffie-Hellman protocol”. In: *International Journal of Security and Networks* 11.4 (2016), pp. 213–223.

[57] Kishore Thapliyal, Rishi Dutt Sharma, and Anirban Pathak. “Protocols for quantum binary voting”. In: *International Journal of Quantum Information* 15.01 (2017), p. 1750007. DOI: 10.1142/S0219749917500071.

[58] S. Vadla et al. “QUASIM: A Multi-dimensional Quantum Cryptography Game for Cyber Security”. In: *Journal of The Colloquium for Information Systems Security Education* 6 (Spring 2019).

[59] Pramode K. Verma, Mayssaa El Rifai, and Kam Wai Clifford Chan. *Multi-photon Quantum Secure Communication*. Springer, 2018.

[60] W. K. Wootters and W. H. Zurek. “A Single Quantum Cannot be Cloned”. In: *Nature* 299.5886 (1982), pp. 802–803.

[61] X. Wu et al. “SeQUeNCe: a customizable discrete-event simulator of quantum networks”. In: *Quantum Science and Technology* 6.4 (2021), p. 045027.

[62] Xiaoliang Wu et al. *SeQUeNCe: A Customizable Discrete-Event Simulator of Quantum Networks*. 2020. arXiv: 2009.12000 [quant-ph].

[63] Feihu Xu et al. “Secure Quantum Key Distribution with Realistic Devices”. In: *Reviews of Modern Physics* 92.2 (2020), p. 025002.

[64] Noson S. Yanofsky and Mirco A. Mannucci. *Quantum Computing for Computer Scientists*. Cambridge University Press, 2008.

[65] Z. Yuan et al. “Experimental demonstration of a BDCZ quantum repeater node”. In: *Nature* 454 (2008).

[66] Wei Zhang et al. “Quantum Secure Direct Communication with Quantum Memory”. In: *Phys. Rev. Lett.* 118 (22 May 2017), p. 220501. DOI: 10.1103/PhysRevLett.118.220501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.118.220501.

Appendix A

Raw Graphs

Since I have kept the trend-lines for the graphs in chapter 4, I am attaching here the post-processing graphs along with the noise. This can be used to understand the graph output after post-processing and compare it with the graphs in chapter 4. The graphs follow same pattern. All the COW QBER graphs will be attached first (along with the keyrate), followed by 3-stage.

A.1 Github Repos for Code

https://github.com/karthick-git-hub/Sequence

https://github.com/karthick-git-hub/Simulator

A.2 Coherent One-way Protocol

A.2.1 P2P

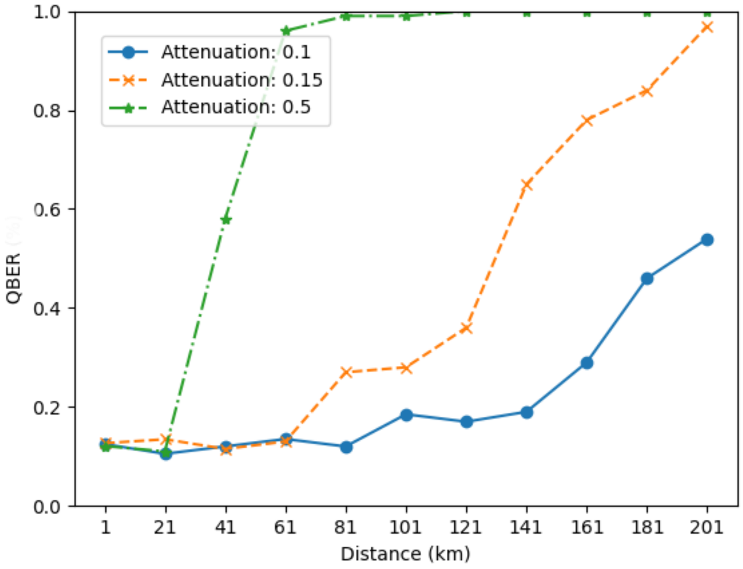


Figure A.1: QBER Graph of COW using P2P by SeQUeNCe simulator.

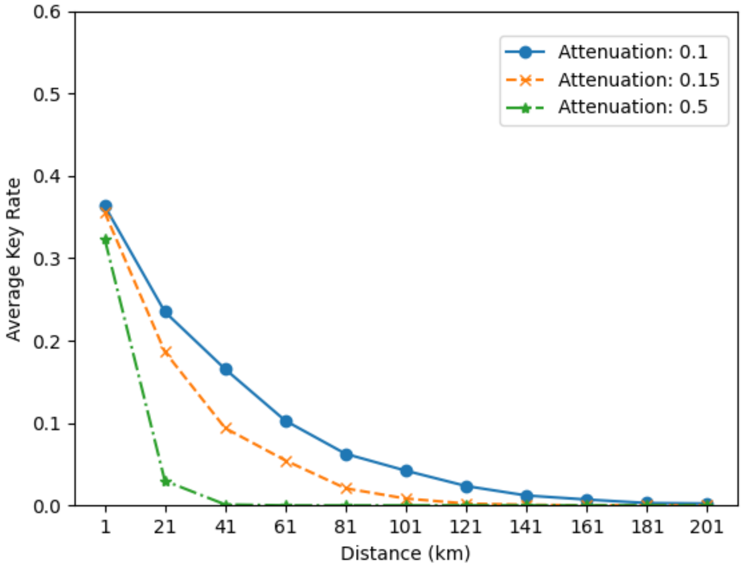


Figure A.2: Keyrate Graph of COW using P2P by SeQUeNCe simulator.

A.2.2 Non-Ideal

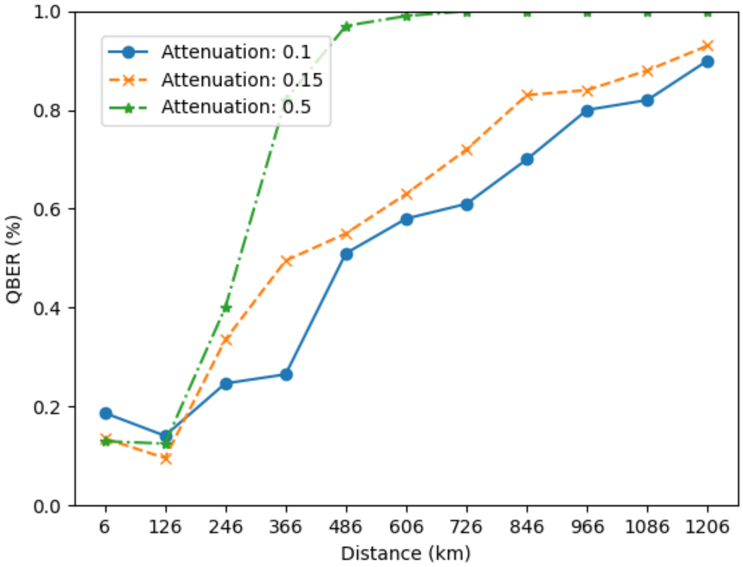


Figure A.3: QBER Graph of COW using non-ideal QR by SeQUeNCe simulator.

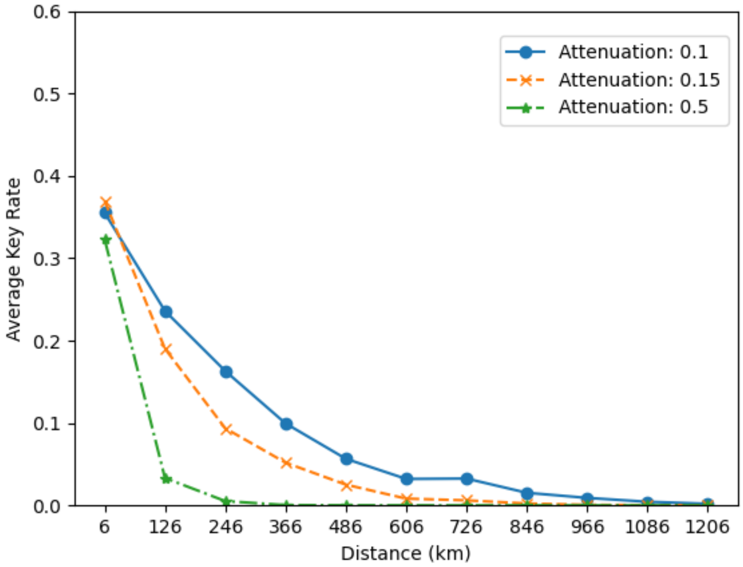


Figure A.4: Keyrate Graph of COW using non-ideal QR by SeQUeNCe simulator.

A.2.3 Ideal

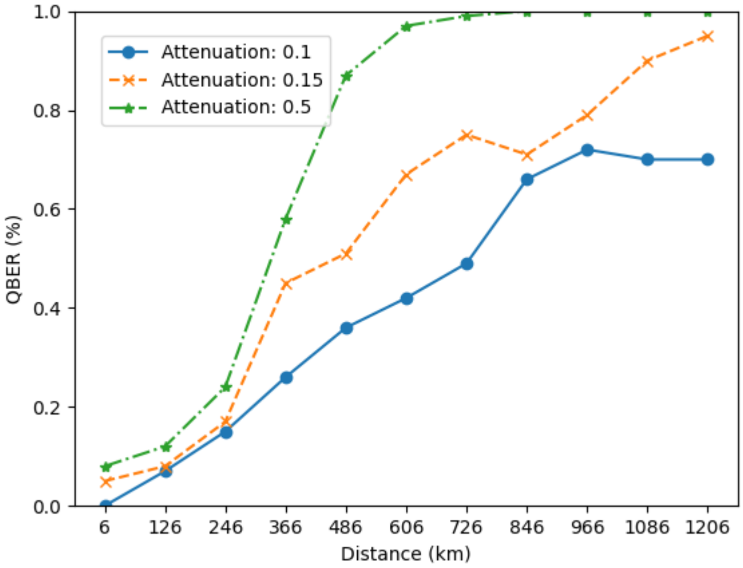


Figure A.5: QBER Graph of COW using Ideal QR by SeQUeNCe simulator.

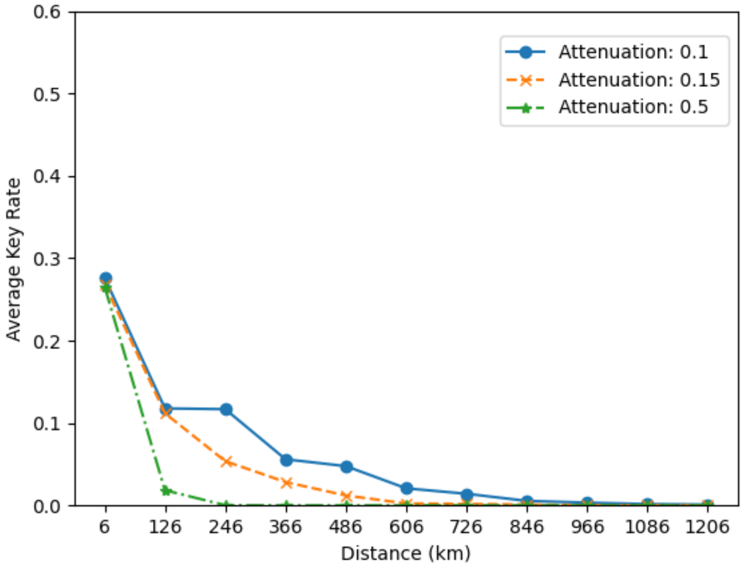


Figure A.6: Keyrate Graph of COW using Ideal QR by SeQUeNCe simulator.

A.3 Three-Stage Protocol

A.3.1 P2P

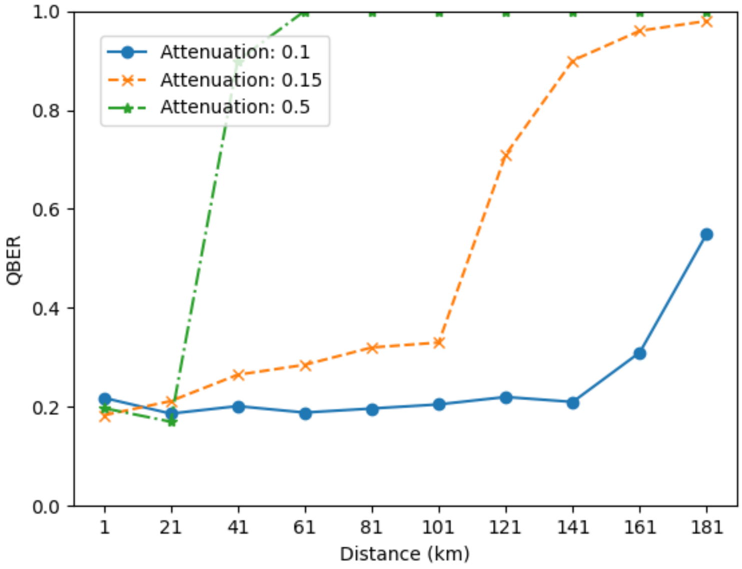


Figure A.7: QBER Graph of 3-stage using P2P by SeQUeNCe simulator.

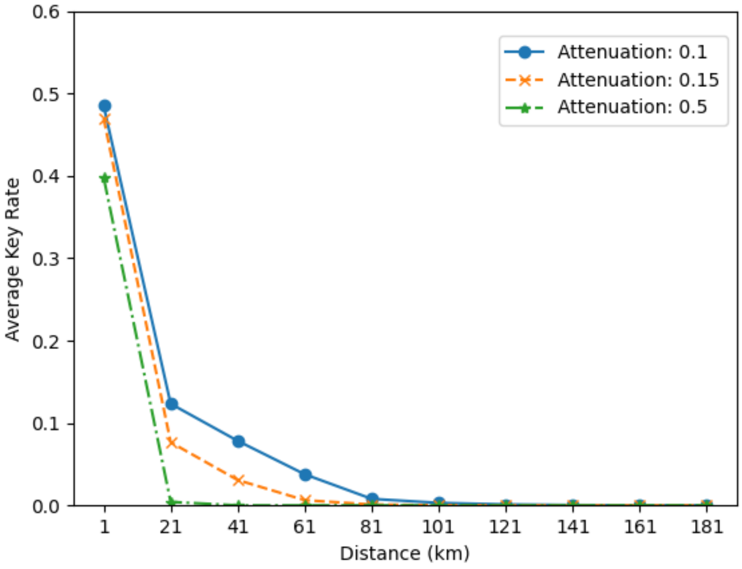


Figure A.8: Keyrate Graph of 3-stage using P2P by SeQUeNCe simulator.

A.3.2 Non-Ideal

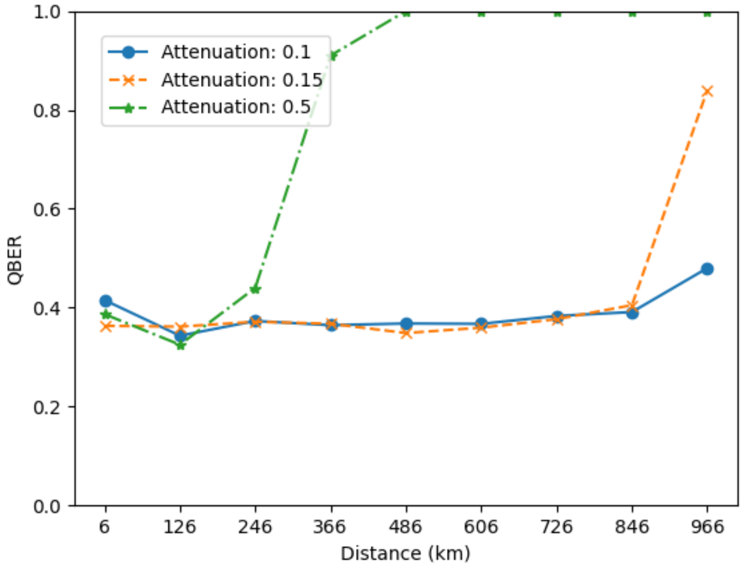


Figure A.9: QBER Graph of 3-stage using non-ideal QR by SeQUeNCe simulator.

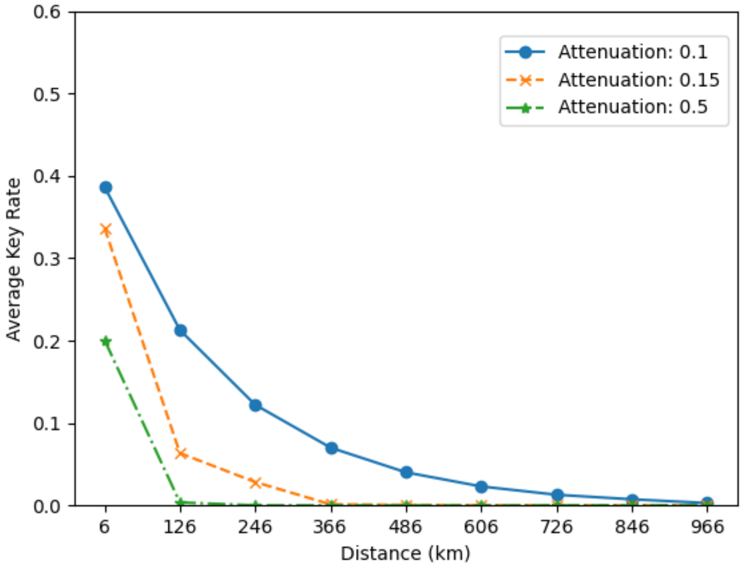


Figure A.10: Keyrate Graph of 3-stage using non-ideal QR by SeQUeNCe simulator.

A.3.3 Ideal

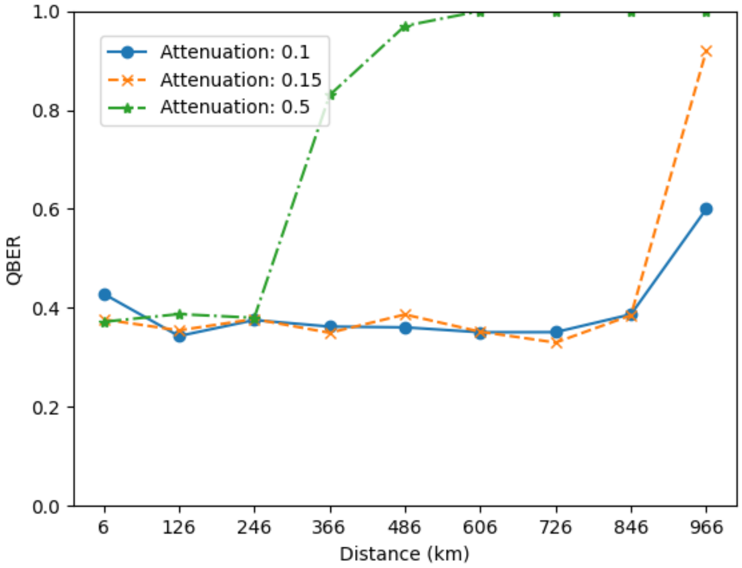


Figure A.11: QBER Graph of 3-stage using Ideal QR by SeQUeNCe simulator.

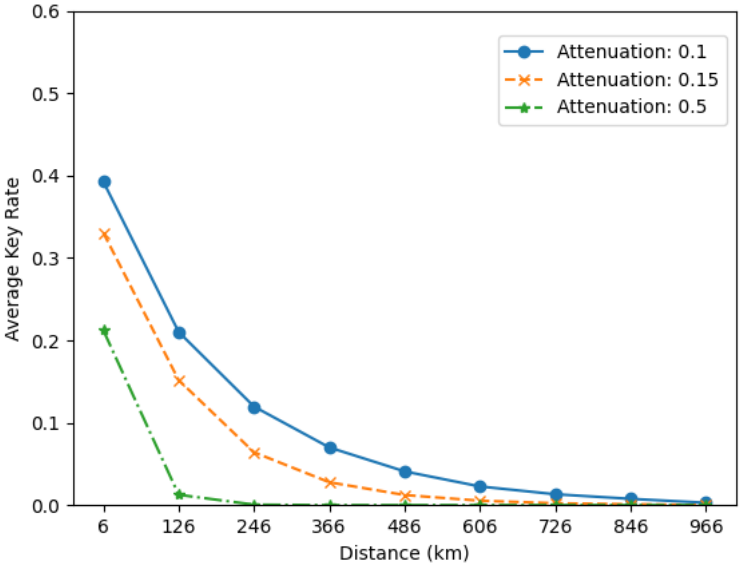


Figure A.12: Keyrate Graph of 3-stage using Ideal QR by SeQUeNCe simulator.