ENHANCING RELIABILITY AND SECURITY IN QUANTUM KEY DISTRIBUTION: OPTIMIZING ERROR CORRECTION TECHNIQUES FOR BB84 PROTOCOL

A PROJECT REPORT

Submitted by

PRIYASAHAANA M

DURGA K

MOHAMED AFRI

COURSE CODE: CS6611

COURSE TITLE: CREATIVE AND INNOVATIVE PROJECT

DEPARTMENT OF COMPUTER TECHNOLOGY

ANNA UNIVERSITY, MIT CAMPUS

CHENNAI – 600044

MAY 2024

DEPARTMENT OF COMPUTER TECHNOLOGY

ANNA UNIVERSITY, MIT CAMPUS

CHENNAI – 600044

BONAFIDE CERTIFICATE

Certified that this project report "**Enhancing Reliability And Security in Quantum Key Distribution: Optimizing Error Correction Techniques for BB84 Protocol**" is work of **Priyasahaana M [2021503037], Durga K [2021503015], Mohamed Afri [2021503029]** in the CS6611 - Creative and Innovative Project Laboratory course during the period January 2024 to May 2024.

SIGNATURE

Dr. T. Sudhakar

SUPERVISOR

Assistant Professor

Department of Computer Technology

Anna University, MIT Campus

Chrompet – 600044.

SIGNATURE

Dr. K. Kottilingam

COURSE IN-CHARGE

Assistant Professor

Department of Computer Technology

Anna University, MIT Campus

Chrompet – 600044.

ACKNOWLEDGEMENT

We take this humble opportunity to thank **Dr. K. Ravichandran**, Dean, MIT Campus, Anna University, and **Dr. P. Jayashree**, Professor & Head, Department of Computer Technology, MIT Campus, Anna University for providing all the lab facilities in pursuit of this project.

Undertaking this project has helped us learn a lot, and we would like to express our sincere gratitude towards our Project Guide **Dr. T. Sudhakar**, Assistant Professor, Department of Computer Technology, MIT, Anna University, whose kind guidance, and proper directions helped us in shaping this project perfectly.

We acknowledge the feedback of panel members **Dr. S. Muthurajkumar**, Associate Professor, Department of Computer Technology, MIT, Anna University, **Dr. R. Kathiroli**, Assistant Professor (Sl. Grade), Department of Computer Technology, MIT, Anna University, and **Dr. K. Kottilingam,** Assistant Professor, Department of Computer Technology, MIT, Anna University, in reviewing our work, and encouraging us to successfully implement our project.

We thank all the teaching and non-teaching members of the Department of Computer Technology, MIT, Anna University, seniors, juniors, and friends whose appreciable help, either directly or indirectly helped in the smooth completion of the Creative and Innovative Project in a limited time frame.

Priyasahaana M [2021503037]

Durga K [2021503015]

Mohamed Afri [2021503029]

ABSTRACT

For telecommunications networks, Quantum Key Distribution (QKD) protocols— notably, BB84, developed in 1984 by Charles Bennett and Gilles Brassard—offer strong cryptographic security. However, noise and defective channels can limit their effectiveness, emphasizing the crucial role of error correction algorithms in ensuring reliable key generation.

In this work, we utilize the most recent techniques to model scenarios intended to lower noise and improve the security of key distribution protocols. Our work focuses on investigating the effects of advanced error-correcting methods on QKD systems' reliability in challenging environments.

Our goal is to enhance the overall performance of QKD systems by evaluating the efficacy and efficiency of these techniques, which will enable a smooth integration of these systems into actual secure communication networks. The results of this research will help strengthen data security in the telecoms industry and open the door for QKD to be widely used as a cornerstone of secure communication infrastructure.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

S.No	ABBREVIATIONS	WORD
1.	QKD	Quantum Key Distribution
2.	QEC	Quantum Error Correction
3.	AQEC	Asymmetric Quantum Error Correction
4.	QPQ	Quantum Private Query
5.	QBER	Quantum Bit Error Rate
6.	LDPC	Low Density Parity Check
7.	DC	Data Compression
8.	EC	Error Correction
9.	PA	Privacy Amplification
10.	POVM	Positive Operator Valued Measures
11.	NISQ	Noisy Intermediate Scale Quantum
12.	QRAM	Quantum Random Access Memory
13.	SDK	Software Development Kit

CHAPTER 1

INTRODUCTION

This chapter delves into optimizing Quantum Key Distribution (QKD) protocols like BB84, acknowledging the impact of noise and channel defects. By employing cutting-edge error correction techniques, we aim to enhance the reliability of QKD systems, paving the way for their seamless integration into secure telecommunication networks, thus fortifying data security in the industry.

1.1 CLASSICAL CRYPTOGRAPHY AND ITS LIMITATIONS

Using intricate mathematical techniques to jumble communications and make them unintelligible to anybody lacking the decryption key, classical cryptography has been the mainstay of secure communication for many years. Due to the computationally costly nature of these techniques, it would take an inordinately long time for an attacker to break the code using the resources that are now accessible. Nevertheless, this strategy has a basic flaw, it is predicated on the notion that the present constraints on processing power will not change.

The vulnerabilities of traditional encryption techniques are growing as a result of advances in computing technology, especially the emergence of powerful computers with parallel processing capabilities. As processing power increases, methods like as brute-force attacks—in which an attacker systematically tries every potential decryption key—become more practical. Because of this, it is now necessary to investigate more reliable security solutions that do not rely exclusively on computational complexity [16].

1.2 THE RISE OF QUANTUM COMPUTING AND ITS IMPACT ON SECURITY

The fundamental basis of classical cryptography is seriously threatened by the advent of quantum computing. Quantum computers achieve exponentially higher processing power compared to classical computers by taking advantage of the concepts of quantum mechanics, such as entanglement (a phenomenon where two quantum particles become linked, sharing the same fate regardless of distance) and superposition (the ability of a quantum system to exist in multiple states simultaneously).

For example, the popular public-key encryption technique known as the RSA algorithm, which depends on the difficulty of factoring huge numbers, is especially vulnerable to quantum assaults. These big numbers can be factored effectively by Shor's algorithm, a theoretical quantum computer process, which negates the need for RSA encryption [17]. The fact that this flaw affects a large number of other traditional encryption techniques emphasizes how critically we need a paradigm change to secure communication in the quantum age.

1.3 QUANTUM CRYPTOGRAPHY

Quantum cryptography offers a revolutionary approach to information security, addressing the limitations of classical methods in the face of quantum computing. It makes use of the special qualities of quantum mechanics to ensure information-theoretic security, which is a degree of security that is based on the principles of physics itself and can be shown to be unbreakable. Quantum cryptography enables secure communication by taking use of the basic rules of quantum physics, such as

the no-cloning theorem, which asserts that it is impossible to precisely replicate an unknown quantum state. This is in contrast to conventional encryption, which depends on the difficulty of breaking the code. The significance of quantum cryptography is that any effort to intercept the conversation throws off the quantum state, warning the people involved of a possible security breach. Because of its built-in security, quantum cryptography provides a reliable option for secure communication in an era where traditional encryption techniques are seriously threatened by quantum computers.

1.4 THE BB84 PROTOCOL: A PIONEERING APPROACH

Charles Bennett and Gilles Brassard developed the BB84 protocol in 1984. It is a fundamental quantum key distribution (QKD) system. By distributing a secret key that can be used to encrypt and decode communications, it uses quantum physics to create a secure communication channel between two participants, usually identified as Alice and Bob. The two main components of the protocol are a classical channel for information exchange and a quantum channel for sending quantum states.

Using the quantum channel, Alice sends quantum bits (qubits), which are the quantum counterpart of classical bits. These quantum bits are encoded in photons' (light particles') polarization state. Alice may, for instance, utilize two different polarization states to represent 0 and 1. The significance, though, is in superposition; she may concurrently encode the qubit in both states up until a measurement is taken.

Bob receives the qubits via the quantum channel, but he is unaware of the bit values that each polarization state corresponds to. To create a shared secret key, Bob

and Alice must discuss their measurements and come to an understanding on a common framework for interpreting the qubits through open communication via a classical channel (such as a standard phone conversation). They can also identify any eavesdroppers (eve) who could attempt to intercept the qubits thanks to this transmission.

Based on the no-cloning theorem, the BB84 protocol is secure. Eve will unavoidably collapse the superposition and change the qubits' state if she attempts to listen in by measuring the qubits while they are in route. By comparing their measurement data, Alice and Bob may identify these changes and eliminate any keys that they believe to be compromised. This makes sure that only Alice and Bob have access to the secret key, allowing them to converse safely.

1.5 EVOLUTION OF QKD PROTOCOLS

Since the BB84 protocol proved successful, scientists have been actively investigating QKD developments, which has resulted in the creation of more effective and adaptable protocols. Compared to the four states of the BB84, the B92 protocol, for example, showed that safe key generation may be achieved using only two basis states for encoding the qubits, making implementation simpler.

Beyond manipulating basic states, scientists have explored the intriguing subject of entanglement. A fundamental concept in quantum physics, entanglement explains the situation in which two qubits, separated by physical distance, become entangled and share the same destiny. Exciting opportunities for secure communication across long distances are presented by this relationship. Entangled qubits have been used in protocols that distribute keys. Alice and Bob share pre-established entangled

pairings in such protocols. Alice then extracts her qubits from the pair that is entangled and sends them to Bob. Even though they live far away, they may create a shared secret key by measuring their qubits. Because any effort to listen in on Eve's message will unavoidably disrupt the entanglement and notify Alice and Bob, the security rests on this fact. The security relies on the fact that any attempt to eavesdrop on the transmission (by Eve) would inevitably disturb the entanglement, alerting Alice and Bob to a potential security breach.

1.6 OBJECTIVES

- To develop and optimize error correction techniques tailored for the BB84 protocol in Quantum Key Distribution.
- To enhance the reliability of key generation in quantum channels by applying advanced error reduction methods like Entanglement Purification (creating tightly entangled pairs, entanglement swapping etc) to minimize noise in simulated environments.

The topics discussed above provide the essential background knowledge required to understand the concept behind this project. With the objectives clearly defined, the following chapters provide details on how the objectives are achieved.

1.7 ORGANIZATION OF THE PROJECT REPORT

CHAPTER 2 provides a thorough review of literature focusing on the BB84 protocol, QKD, and QEC in quantum communication, highlighting advancements and challenges in enhancing security and reliability.

CHAPTER 3 explains proposed QKD techniques, emphasizing error correction and reconciliation modules to ensure the reliability and integrity of quantum communication systems.

CHAPTER 4 covers AQEC implementation, encoding patterns, and experimental setups.

CHAPTER 5 shows the results and analysis of the implemented asymmetric error correction method.

CHAPTER 6 concludes by emphasizing the importance of QEC algorithms in enhancing the reliability of QKD protocols, suggesting future research directions to further improve QKD systems' security and integration into telecommunication networks.

CHAPTER 7 presents a concise list of references, encompassing recent studies on quantum key distribution, error correction methods, and advancements in quantum communication technologies.

CHAPTER 2

LITERATURE SURVEY

This chapter presents a comprehensive overview of contemporary research on quantum communication, with a particular emphasis on advancements and obstacles related to the BB84 protocol, QKD, and QEC, underscoring efforts to bolster security and dependability.

2.1 RELATED TO BB84 PROTOCOL

The significance of eavesdropping detection in ensuring the security of the BB84 protocol for practical applications was covered by Lee et al., in [1]. An effort at eavesdropping can be made on the BB84 protocol, a quantum mechanically secure communication mechanism. To identify the interruptions brought about by the eavesdropper's activity, this research focuses on eavesdropping detection techniques during the BB84 protocol. It examines how listening in on the BB84 protocol affects the quantum bit error rate (QBER).

Based on the BB84 protocol, Jia et al., in [2] suggest a new safe key distribution mechanism for quantum communication (QKD). In contrast to conventional BB84, the approach makes use of CSS error-correcting codes. These codes are modified for the quantum world by taking advantage of their innate error-correcting capabilities, which were originally intended for classical data. By strengthening the BB84 protocol's capacity to identify and fix transmission faults, this method promotes more secure and dependable key distribution.

2.2 RELATED TO QUANTUM KEY DISTRIBUTION

A safe and effective QKD protocol with error correction is proposed by Mummadi et al., in [3]. Conventional QKD is susceptible to eavesdropping because of transmission faults. Their method uses asymmetric quantum error correction (AQEC) in conjunction with entanglement purification to minimize these errors. The entangled qubits used for key distribution are cleaned up by entanglement purification, whereas AQEC fixes mistakes without forcing the sender to resend data. Large error rate reduction is demonstrated in simulations, which makes eavesdropping more difficult and allows for longer, more effective quantum keys.

Amer et al. explore the useful applications of quantum key distribution (QKD), a secure communication technique, in [4]. Different error correction strategies that are used to protect the quantum information is being conveyed. It goes into detail on the various encoding techniques used in QKD, including as phase, time-bin, and polarization encoding.

Information reconciliation is a critical phase in quantum key distribution (QKD), which is covered by Kiktenko et al., in [5]. This step makes sure that everyone has the same copy of the secret key. In this research, a novel interactive protocol utilizing polar codes for information reconciliation is proposed. These codes provide effective error correction features. The security and effectiveness of QKD are improved by the novel protocol, which enables both parties to reconcile their keys without disclosing any information about the actual key.

Information reconciliation is a critical phase in quantum key distribution (QKD), which is covered by Kiktenko et al., in [6]. The step introduced makes sure

that everyone has the same copy of the secret key. In this research, a novel interactive protocol utilizing polar codes for information reconciliation is proposed. These codes provide effective error correction features. The security and effectiveness of QKD are improved by this novel protocol, which enables both parties to reconcile their keys without disclosing any information about the actual key.

Oulouda et al., in [7] present a novel method for Quantum Key Distribution (QKD). The technique encodes the data onto a single-photon added-subtracted squeezed coherent state using a single X gate, followed by S and U operations. This is not the case with conventional QKD techniques, which rely on phase shifters and Hadamard gates. In comparison with current methods, the authors assert that their approach offers enhanced security and efficiency.

2.3 RELATED TO ERROR CORRECTION

The findings of the research [8] completely rewrite the three essential algorithms: data compression (DC), error correction (EC), and privacy amplification (PA). It is demonstrated that all three become very similar when they have access to "quantum side information." These algorithms work with classical data traditionally. It works in quantum information in addition to the classical data, which enables the algorithms to accomplish their objectives in a unique way. This equivalency allows for a new definition of PA security in terms of "purified distance" and incorporates quantum information to expand the possibilities of data compression and error correction.

In Quantum Private Query (QPQ), a method for obtaining data from a database while maintaining the confidentiality of the query itself, Wei et al. tackle a significant obstacle in [9]. The problem of errors caused during transmission in noisy

situations is addressed. The approach offers a useful upper bound on acceptable error rates, guaranteeing, even in the presence of noise, the privacy of the user (the query itself stays secret) and the security of the database (information stays concealed).

Using Low-Density Parity-Check (LDPC) codes, Bilash et al., present a unique error correction technique for Quantum Key Distribution (QKD) systems in [10]. The goal of this approach is to lower the quantum information transmission error rate, which is essential for guaranteeing safe communication in QKD. The LDPC code contributes to more dependable and secure key distribution by assisting in the detection and correction of potential transmission faults across quantum channels.

i-QER, a technique to lower errors in quantum circuits without the need for more quantum resources, is presented by Basu et al., in [11]. The method starts by forecasting possible circuit faults. By clever design, the circuit is divided into smaller sub-circuits if the expected error is greater than a threshold. The output of the original circuit is then recreated by combining the results of running these sub-circuits on a quantum computer.

An in-depth discussion of quantum secret sharing—a method for safely transferring confidential data between several parties—is provided by Basak et al., in [12]. A particular kind of quantum entanglement called the GHZ state in the study is employed. IBM's Quantum Experience (Qiskit) tools to implement the whole protocol, including error-correcting techniques are used.

Swathi et al., [13] introduced a new method for asymmetric quantum error correction (AQEC). Unlike traditional AQEC which uses Hadamard and phase shift

gates, their approach utilizes a single X gate followed by S and U operations for encoding a single logical qubit onto five physical qubits. This method aims to improve the efficiency of the encoding circuit. The paper explores how to measure errors using Positive Operator Valued Measures (POVMs) and details how to create a density matrix to represent the probabilities of various outcomes.

W.C. Lindsey in [14] investigates the use of noisy quantum channels for the transmission of classical information. An alternative encoding technique that uses phase shift gates and Hadamard gates instead of the conventional one is introduced. On the initial qubit, S and U operations are performed after a single X gate. This method seeks to encode the data while shielding it from noise-induced phase changes. To illustrate the probability of various outcomes in the noisy channel, the study describes how to generate a density matrix and investigates the use of Positive Operator Valued Measures (POVMs) for measuring mistakes.

Shahriar et al., in [15] suggested a way to enhance Shor's quantum error correction circuits. Usually, Shor's approach employs intricate circuits to rectify errors. To address this, the authors modify the current circuits to include quantum adders. By simplifying the circuits, these adders may increase their efficiency and facilitate their implementation on actual quantum computers.

2.4 SUMMARY

The related works were surveyed, and the limitations were identified to propose an organized work for our research, as described in the following elaborative headings.

CHAPTER 3

PROPOSED WORK

This chapter describes suggested QKD methods, putting special emphasis on modules for error correction and reconciliation to guarantee the integrity and dependability of quantum communication systems.

3.1 INTRODUCTION

One approach for secure communication is Quantum Key Distribution. It is predicated on the ideas of superposition and entanglement in quantum mechanics. Information in the quantum world is expressed in terms of qubits. A qubit may be thought of as a superposition of several qubits that possess several states simultaneously. The value will be lost into any state based on the greatest likelihood once it has been measured. Assuming a two level quantum system with a pure quantum state of $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, where the amplitudes of states $|0\rangle$ and $|1\rangle$ are represented by α and β. One unique characteristic of the quantum states is Entanglement, where it is impossible to measure two or more quantum states independently although they are formed with comparable features.

The main component of quantum cryptography is QKD. Comparing quantum cryptography to traditional cryptography reveals differences. The single channel utilized in classical cryptography for key sharing between sender and recipient is the classical channel. However, information is shared between classical and quantum channels in quantum cryptography.

In Figure 3.1, the technique of distributing a quantum key which is created by quantum particles between two parties over a quantum channel known as Quantum Key Distribution is illustrated.

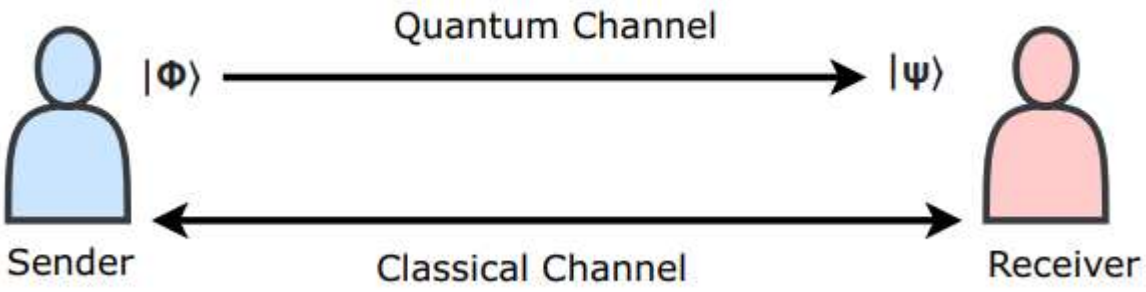

Figure 3.1 Quantum Key Distribution

The quantum states with a polarization basis are generated by the transmitter and communicated to the recipient, as seen in the above image. A polarization basis is used by the receiver to measure the quantum states that the transmitter sent. The measured quantum states coincide with the sender's quantum states if the recipient employs the same basis. These complementary quantum states are regarded as the key that may be used to further procedures.

There is also a chance that someone else may be able to view the data once the key has been supplied. However, in the quantum theory, every attempt to examine or quantify the quantum state will cause disturbances to its true state.

As a result, we used the same foundation to identify the causes of mismatched keys as follows:

- The presence of an eavesdropper or third party.
- The presence of noise.

The exchange of another key will begin the conversation again if the key cannot be matched because of the presence of a third party. Sometimes, despite the noise, the communicating parties interpret it as a third party's presence and discard the message in favor of sharing the updated key. Due to the inherent noise of quantum particles, the error rate in the current generation of Noisy Intermediate Scale Quantum (NISQ) Systems is significant. By adding bits or causing phase flips, noise causes mistakes that alter the real quantum state and deteriorate.

3.2 MODULES

Entangled pairs are crucial for safe data transfer in QKD. So the entanglement of qubits is generated. Therefore, in order to prevent further mistakes, the entangled pairs employed in QKD processes must be maximally entangled. To separate the maximally entangled couples, entanglement purification techniques are therefore necessary. On encoding the information the entangled qubits, noise can be introduced. Quantum error correction methods must be used to identify and fix problems caused by the noise inherent in qubits.

We then suggested a QKD methodology that included Asymmetric Quantum Error Correction (AQEC) and an Entanglement Purification technique. We are suggesting three key processes to lower the error rate and improve QKD efficiency. They are as follows:

1. Entanglement Module
2. Key generation and Transmission Module
3. Reconciliation Module

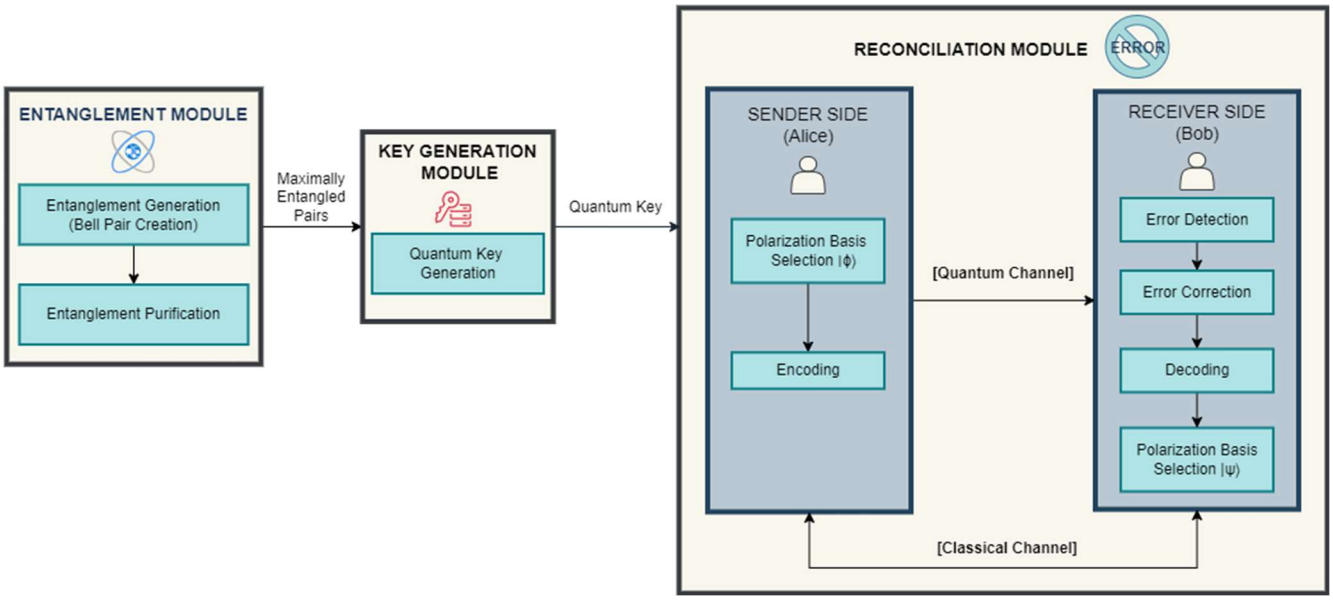

Figure 3.2 Optimization of Error Detection and Correction in QKD

3.2.1 ENTANGLEMENT MODULE:

1. Entanglement Generation:

Entanglement, a phenomenon unmatched in the classical world, is at the core of quantum communication. The Entanglement Generation Module is essential to the coordination of this event. Its objective is the process of producing entangled qubit pairs, which are the essential components of secure communication protocols such as Quantum Key Distribution (QKD).

Consider these qubits as the bits, or the 0s and 1s of classical information, of the quantum world. Qubits, on the other hand, can exist in a superposition of both states concurrently, in contrast to bits, which can only exist in one state at a time (0 or 1). Entanglement, a spooky connection in which two qubits become linked and share the same fate regardless of their physical separation, is made possible by this "quantum weirdness". Imagine flipping a coin; regardless of how far apart they are,

if one is headed, the other will always be tails. Comparable, but at the quantum level, is entanglement.

The module uses a toolbox of quantum gates, including the Hadamard gate, to accomplish this entanglement. With the help of this gate, a qubit can explore both possibilities in superposition before being collapsed into a single state by a measurement. Another important actor is the CNOT gate, which controls an operation on two qubits. The CNOT gate contributes to the complicated entanglement fabric by allowing one qubit to be altered in response to the state of another.

2. Superposition to Entanglement:

Expanding on the idea of superposition that the Hadamard gate first offered, the Entanglement Generation Module uses the CNOT gate's capabilities to produce entangled pairs. Consider Alice and Bob as two people that wish to communicate securely. Using the Hadamard gate, the module first generates qubits in a superposition state. Imagine these qubits as coins that are indecisive between heads and tails, whirling in mid-air.

Then the CNOT gate enters the picture, performing this quantum dance like a master. It uses the state of one qubit (the control) as a basis for controlling the state of another qubit (the target). This links the qubits' destinies and enables the module to control them in a certain way. The target qubit is adjusted such that it lands on tails if the control qubit touches heads. The qubits are now entangled and share a common destiny as a result of this association.

The quality of the initial qubits and the accuracy of the quantum gates are critical to the process's success. Not-so-perfect entanglement can result from even little flaws. The module doesn't end there, though. Entanglement purification is the following step that makes sure the best entangled pairs are utilized for secure communication.

3. Entanglement Purification:

The Entanglement Purification Module wouldn't want to utilize poor quality entangled pairs for communication. The module uses a range of methods to achieve purification. The act of discarding is one such method. The module may determine whether entangled couples have lower correlations by comparing their behaviors. These pairings are then eliminated, leaving just the pairs that are most entangled that is, the most appropriate for communication.

Entanglement switching is an additional method, a more advanced one. In this instance, the module makes use of the strength of already-entangled pairs to enhance the entanglement of other pairs.

Entangled pairs are represented with Bell states. In a 2-level quantum system, there are total four possible bell states that can be generated which are represented as follows:

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle) \quad (1)$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle) \quad (2)$$

After simplifying the equations for each entangled quantum state, the equations will be modified as follows:

$$|00\rangle = \frac{1}{\sqrt{2}} (|\Psi^+\rangle + |\Psi^-\rangle) \quad (3)$$

$$|01\rangle = \frac{1}{\sqrt{2}} (|\emptyset^+\rangle + |\emptyset^-\rangle) \quad (4)$$

$$|11\rangle = \frac{1}{\sqrt{2}} (|\Psi^+\rangle - |\Psi^-\rangle) \quad (5)$$

$$|10\rangle = \frac{1}{\sqrt{2}} (|\emptyset^+\rangle - |\emptyset^-\rangle) \quad (6)$$

The entanglement is produced by using CNOT and Hadamard gates. We must cleanse the entanglement once it has been generated. Next, entangled qubits will undergo the entanglement switching process. One unique characteristic of entanglement is entanglement switching, wherein the two quantum systems, which do not directly interact, become entangled. i.e., qubits that have never before interacted can get entangled. This technique is primarily used to separate the maximally entangled pairs and send data over larger distances without breaking the qubits' entanglement.

3.2.2 KEY GENERATION AND TRANSMISSION MODULE

The sheer nature of quantum communication channels creates a huge challenge: noise, even in the absence of eavesdroppers. The noise can disturb the sensitive quantum states of the qubits, leading to mistakes such as "phase flips" (where the qubit's internal rotation inadvertently shifts from 0 to 1) and "bit flips"

(where 0 becomes 1 or vice versa). These mistakes may compromise the produced key's confidentiality.

This problem is handled by the Key Generation Module via a procedure known as Error Rectification. This entails adding so-called Ancilla qubits, extra qubits to the transmission process. Through meticulous manipulation of these Ancilla qubits in conjunction with the data qubits, the module can identify and, in some situations, even rectify mistakes caused by noise. Error-correcting methods can have some limits, though. They frequently call for more qubits and intricate processes, which might slow down communication.

- **Entangled Qubit Sharing: Strengthening Sender-Receiver Bonds**

Secure quantum communication relies on producing and exchanging maximally entangled pairs of qubits, which is started by entanglement purification techniques. Through the process of separating strongly quantum entangled pairs from less entangled pairs, these techniques ensure the production of qubit pairs with extremely interconnected states. These maximally entangled qubits are then sent over dedicated quantum channels between the transmitter, usually called Alice, and the receiver, usually called Bob.

The basis for quantum key distribution protocols is the sharing of entangled qubits, which makes it easier to generate secret keys that are essential for encrypted communication. The security of the communication channel is ensured by the intrinsic entanglement between qubits, any unauthorized attempt to intercept the transmission would disrupt the entanglement, promptly alerting Alice and Bob to potential intrusion attempts.

- **The Importance of Entangled Qubit Exchange**

In addition to providing a secure channel, the entanglement-based quantum communication paradigm highlights the importance of quantum physics in contemporary encryption. Quantum communication methods leverage the non-local correlations present in quantum states through the creation and sharing of maximally entangled qubits, opening up new possibilities for safe information transfer. These protocols provide a strong foundation for encrypting sensitive data while reducing the hazards associated with traditional eavesdropping methods. By utilizing the concepts of quantum entanglement. A new era of cryptography and information security is thus being directed by the synergy of entanglement purification, qubit sharing, and quantum key distribution, which together provide a strong foundation for developing secure communication paradigms in the quantum theory.

3.2.3 RECONCILIATION MODULE:

- **ENCODING**

In quantum communication, encoding prevents unwanted access by transforming data into forms that are unintelligible. This assures safe transmission. Reliability is increased by incorporating error detection and repair algorithms, which are essential for overcoming noise and errors in quantum channels. Data integrity is preserved by smooth processing inside the quantum framework that is ensured by compatibility with quantum processes. Additionally, by efficiently expressing information, encoding minimizes resource usage, a critical factor in resource-constrained quantum systems. Overall, encoding plays a critical role in maintaining the security and effectiveness of quantum communication by protecting quantum data, guaranteeing dependability, preserving compatibility with quantum activities, and optimizing resource use. To encode the quantum information S, U, and CNOT

operations are performed on input data. After performing S and Unitary operations on input data, the possibility of phase flip will be reduced. After that, the CNOT operations will be performed on input data to encode it.

- **S Gate:** (Ref : [Nielsen and Chuang, Quantum Computation and Quantum Information, ISBN 978-0-521-63503-5])

The Phase gate (or S gate) is a single-qubit operation defined by

$$s = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{7}$$

The S gate is also known as the phase gate or the Z-90 gate, because it represents a 90-degree rotation around the z-axis. It's crucial for adjusting phase and mitigating errors in quantum communication.

- **U Gate:** (Ref : [Nielsen and Chuang, Quantum Computation and Quantum Information, ISBN 978-0-521-63503-5])

The U gate, often called the "arbitrary single-qubit phase gate," introduces a phase shift to a qubit's quantum state by a specified angle and is represented by:

$$U(\theta) = \begin{pmatrix} e^{i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} \tag{8}$$

Here, ɵ represents the angle of the phase shift applied by the gate. The U gate is a fundamental component in quantum computing and communication, allowing precise control over the phase of qubit states, essential for various quantum algorithms and protocols.

- **Encoded Information:** After performing S and U operations on the quantum state, the CNOT gate will be applied to convert a single logical qubit into multiple physical qubits using the given formula

$$\text{Encoded Information} \quad \emptyset_E = \sum_i \text{CNOT}\ (|q_i\rangle, |q_{i+1}\rangle) \tag{9}$$

Here $(|q_i\rangle, |q_{i+1}\rangle)$, represents the Quantum states. After encoding the information, it will be transmitted to the receiver through the depolarization quantum channel.

- **ERROR DETECTION**

During transmission via the quantum channel, errors may emerge due to external noise or interference. Through the utilization of additional qubits referred to as Ancilla qubits, the error detection module detects these issues. To identify errors in the sent quantum information, techniques such as CNOT gates and measurement operations are employed.

This problem is taken on by the Error Detection Module, a crucial part of Key Generation. It makes use of extra qubits, or Ancilla qubits, to act as sentinels along the path taken by the data qubits. Through meticulous manipulation of these Ancilla qubits in conjunction with the data qubits, the module is able to identify discrepancies that may indicate possible mistakes. Imagine that every communication (data qubit) Alice sends is entwined with a crimson thread (the Ancilla qubit). The red thread would probably be disrupted by any outside interference that messes with the message, letting Alice know there's an issue. To expose any discrepancies in the Ancilla qubits' states, the module uses exact measurement operations on them. CNOT gates also function as conditional switches.

A CNOT gate may be used to modify the data qubit in a certain way, which may expose the type of the error, based on the state of the Ancilla qubit, which may indicate a possible error. Through a methodical examination of the Ancilla qubits' behavior and judicious use of these methodologies, the Error Detection Module is for spotting possible mistakes in the quantum data that is being broadcasted.

- **ERROR CORRECTION**

The Reconciliation Module within Quantum Key Distribution (QKD) plays a critical role in establishing secure communication. Error correction, within this module, is an essential process for guaranteeing the integrity of the transmitted quantum information.

- **The Challenge of Noise:** QKD depends on the transmission of quantum information contained on qubits, as opposed to classical communication. The qubits are prone to mistakes in transmission because of noise in the surrounding environment and imperfection in the channel. Bit flips, in which a qubit's state changes from 0 to 1, and phase flips, in which the qubit's internal rotation inadvertently shifts, are two examples of these faults.
- **The Importance of Error Correction:** If these mistakes are not fixed, the confidentiality of the encoded data may be jeopardized. The security of the connection might be compromised by even a single mistake that goes unnoticed.
- **The Role of Error Correction:** The Error Correction Module acts as a safeguard against these errors. It employs various techniques to identify and rectify the errors introduced during transmission. This process often involves applying specific quantum gates (like X, Z, or combinations) to the qubits based on the identified error patterns.

- **DECODING:**

Bob, the recipient, uses the decoding procedure after Alice, the sender, uses certain quantum gates to encode the message onto entangled qubits. In essence, Alice's encoding processes are reversed by this procedure. Through a carefully selected series of comparable gates (CNOT gates, S gates, and Unitary operations), Bob deciphers the secret message concealed in the qubits' quantum states.

3.3 SUMMARY

The above discussed chapter provided a detailed overview of QKD methods, emphasizing error correction and reconciliation modules to ensure the integrity and reliability of quantum communication systems. It discusses key processes such as entanglement generation, key generation and transmission, and reconciliation, highlighting their roles in mitigating errors and ensuring secure communication.

CHAPTER 4

IMPLEMENTATION

This chapter delves into the implementation of AQEC, detailing encoding patterns and experimental setups. It explores the intricacies of AQEC in enhancing error correction in quantum communication systems, providing insights into its practical application and experimental validation.

4.1 ASYMMETRIC QUANTUM ERROR CORRECTION

An asymmetric error correction algorithm is a technique used in quantum key distribution (QKD) that is intended to rectify mistakes that arise when quantum bits (qubits) are being sent between participants in the key distribution process. Asymmetric error correction techniques consider the special properties of quantum communication channels and the quantum structure of the information being sent, in contrast to conventional symmetric error correction algorithms that handle mistakes equally regardless of where they come from.

4.1.1 Quantum Error Detection: Due to their intrinsic fragility, quantum systems are prone to mistakes caused by a variety of elements, including poor measuring instruments, noise, and de-coherence. Quantum error detection techniques are utilized by asymmetric error correction algorithms to discover mistakes that may have arisen during qubit transmission. Usually, this detection procedure needs to measure the qubits that have been received and contrasting the findings with the predictions made from the transmitted quantum states.

4.1.2 Syndrome Generation: Asymmetric error correction algorithms, upon detecting mistakes, produce error syndromes, which contain information on the

kinds and locations of errors that have transpired. This stage is essential for figuring out the remedial measures required to return the transferred qubits to their initial states.

4.1.3 Asymmetric Error Quantum Correction: Asymmetric Quantum Error Correction (AQEC) algorithms take advantage of the special qualities of quantum states to apply customized correction operations based on the particular error syndromes observed. This is in contrast to symmetric error correction, which usually needs applying identical operations to correct errors. Quantum gates or quantum error-correcting codes that aim to minimize the introduction of new mistakes while reversing the impact of identified faults are applied during these corrective procedures.

4.1.4 Efficiency of Error Correction: The goal of Asymmetric Quantum Error Correction (AQEC) algorithms is to minimize the resources needed for mistake correction while simultaneously achieving high levels of efficiency. This needs selecting corrective procedures optimally taking into account the capabilities of the quantum hardware utilized for error correction in addition to the location and severity of defects.

4.2 ENCODING PATTERNS

Quantum computers have the potential to solve certain problems faster than classical computers. However, loading data into a quantum computer is not trivial. To load the data, it must be encoded in quantum bits (qubits).

Multiple data encodings are feasible because qubits may represent the data in a variety of ways. The data itself and the selected encoding have an impact on how

long the loading process takes to complete. In the worst situation, loading takes a very long time. This is important because speed-up-promising quantum algorithms presume that data loading may be completed in logarithmic or linear time. We provide three popular encodings as patterns to highlight abstract knowledge about encodings and the implications of selecting a certain data encoding. Patterns, particularly in intricate fields like quantum computing, can help make this new technology and its vast potential understandable to consumers from a variety of backgrounds. They especially make it easier for software developers to create quantum applications. This section explains the pattern format and our approach to pattern collection.

A presentation of the patterns that follow is next, with an overview displayed in Figure. 4.1

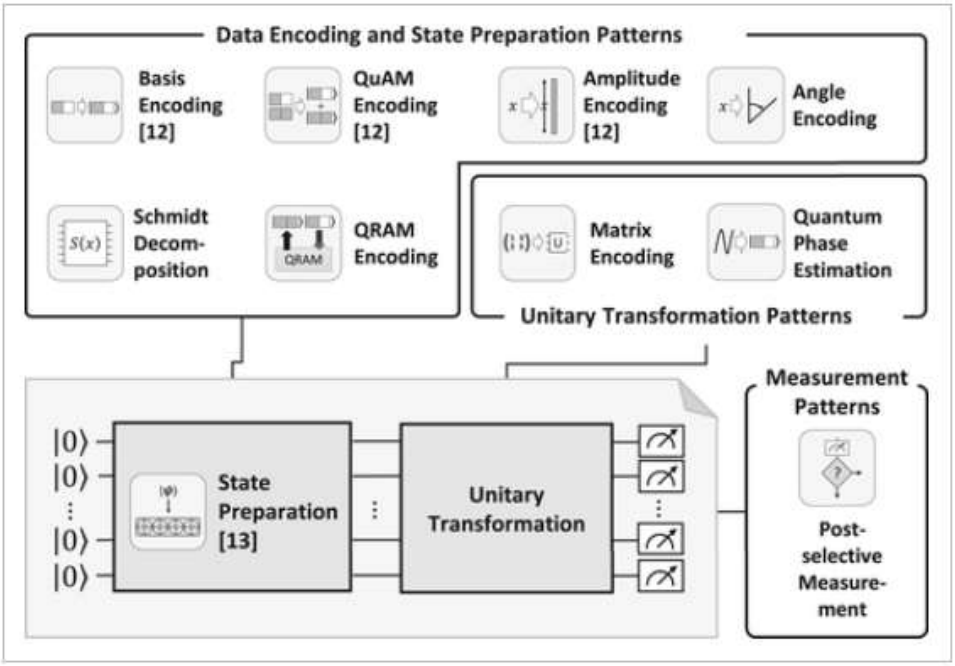

Figure 4.1 Encoding patterns

Table 4.1 represents the comparison of data encoding patterns.

ENCODING PATTERN	ENCODING	REQ. QUBITS
BASIS ENCODING	$x_i \approx \sum_i^m = -k^{b_i 2^i} \rightarrow \lvert b_m \ldots b_k \rangle$	$l = k + m$ per data-point
ANGLE ENCODING	$x_i \rightarrow \cos(x_i) \lvert 0 \rangle + \mathrm{Sin}(x_i) \lvert 1 \rangle$	1 per data-point
QuAM ENCODING	$\mathrm{X} \rightarrow \sum_{i=0}^{n-1} \frac{1}{\sqrt{n}} \lvert x_i \rangle$	l
QRAM ENCODING	$\mathrm{X} \rightarrow \sum_{i=0}^{n-1} \frac{1}{\sqrt{n}} \lvert i \rangle \lvert x_i \rangle$	$[\log n\,] + l$
AMPLITUDE ENCODING	$\mathrm{X} \rightarrow \sum_{i=0}^{n-1} x_i \lvert i \rangle$	$[\log n]$

For the Quantum Random Access Memory (QRAM) Encoding, we assume that all *n* data points are loaded. Table 4.1 gives an overview of the data encoding patterns presented in this work as well as previous encoding patterns. While the encodings of the first two patterns define how a single numerical data point x is encoded, the three other patterns describe how a set X of n data points can be represented.

As a result, before introducing the patterns of Angle Encoding and QRAM Encoding, we go into further depth about this pattern. We do not include the forces for data encoding patterns in the explanations of angle and QRAM encoding as we have already stated above. A numerical data point's Basis Encoding begins with an approximation of its value based on its binary representation. The |bm…b−k state

then encodes the resultant bitstring, bm…b−k. As a result, a single qubit represents each bit in its bitstring. For this reason, Basis Encoding is inefficient in terms of the quantity of qubits needed. QuAM Encoding, in contrast, takes advantage of superposition to encode a collection of data points in a qubit register that has the same length.

Random access memory in quantum for encoding to represent the same data, [log n] more qubits are required. The data representation in Amplitude Encoding is even more compact, using just [log n] qubits. The final three encodings in Table 4.1 cannot, however, be realized efficiently for every given data collection; that is, in a constant or logarithmic number of parallel processes. Angle encoding and Basis encoding can be realized in constant time (one single simultaneous operation), but they are not efficient in terms of the number of qubits required. The associated patterns provide more information on the encodings described in Table 4.1 as well as their implications.

4.3 EXPERIMENTAL SETUP:

4.3.1 TOOLS REQUIRED

- **Jupyter Notebook:** Jupyter Notebook is a web-based application used to create and share interactive notebook documents, which can contain live code, text, data visualizations, videos and other computational outputs. Created by Project Jupyter, the application is open-source and supports the use of over 40 programming languages, including Python, R and Scala. Jupyter Notebook showcases real-time code results and imagery, and can execute cells in any order.

- **Qiskit :** Qiskit is an open-source software development kit (SDK) for working with quantum computers at the level of circuits, pulses, and algorithms. It provides tools for creating and manipulating quantum programs and running them on prototype quantum devices on IBM Quantum Platform or on simulators on a local computer.

4.3.2 PACKAGES REQUIRED

- **'QiskitRuntimeService' Package :** IBM Quantum backend contact is facilitated via the QiskitRuntimeService class, which is a component of the qiskit_ibm_runtime package. It makes things like finding available backends, sending jobs, and getting results possible. It is an essential component for establishing a connection to actual IBM Quantum hardware to perform quantum circuits. It would play a crucial role in gaining access to and using IBM Quantum resources in a complete program, allowing users to use the computational and experimental capacity of real quantum computers.

- **'backends' Package:** A list of backends that are available and meet specific requirements is retrieved from IBM Quantum using the "backends" function, which is probably implemented within the QiskitRuntimeService class. It is useful for choosing appropriate quantum processors according to hardware specs.

- **'QuantumCircuit' Package:** It is used to instantiate a quantum circuit. It also allots classical bits, which will be employed to measure the states of the qubits. The foundation for implementing and experimenting with quantum algorithms inside the Qiskit framework is provided by this class, which allows to construct and modify quantum operations, gates, and measurements.

- **‘transpile’ Package:** This function is in charge of converting a quantum circuit into a format that can be used on a certain backend. In order to improve circuit speed and execution efficiency, it makes changes and improvements to the circuit. Some of these include breaking down complicated gates into smaller ones that the target backend can handle, modifying gate sequences for gate-set compatibility, and implementing further optimizations.

- **‘assemble’ Package:** This function is in charge of further optimizing a transpiled quantum circuit for use on a particular backend. Tasks like resource allocation, gate scheduling, and gate sequence optimization may be included to optimize the compiled circuit's efficiency and performance on the intended hardware.

- **‘Aer’ Package:** Quantum circuits may be simulated using the "Aer" class, which is imported from the qiskit_aer package. It offers a framework for modeling the actions of a quantum computer, to run and examine the outcomes of quantum algorithms in a safe setting.

  The "Aer" simulator is used to run the quantum circuit on a simulated quantum environment rather than actual hardware. When testing, debugging, and developing quantum algorithms without the limits of hardware quantum computers, this is very helpful.

- **‘QuantumRegister’ Package:** The Quantum Registers package in Qiskit provides functionality to create and manipulate quantum registers, which are collections of qubits used to store quantum information. Quantum registers store

quantum information manipulated by quantum algorithms, facilitating operations like quantum gates acting on multiple qubits simultaneously.

4.4 ENTANGLEMENT GENERATION AND PURIFICATION

Entanglement is a special phenomenon seen in the field of quantum mechanics, in which two or more qubits become entangled. Despite their physical distance from one another, their properties are linked. To create entanglement between qubits, quantum gates like Hadamard and CNOT gates are frequently utilized and to separate maximally entangled couples from less entangled ones, the entanglement purification is done. Entanglement swapping is one of the techniques in entanglement purification to raise the quality of entangled qubits.

ALGORITHM FOR ENTANGLEMENT

Input: Two Entangled Pairs

Output: Maximally Entangled Pair

1: Initialize the size of Quantum register q[] and Classical register c[] as 4.

2: Perform Hadamard operation on q[0] and q[3]

3: Perform cx operation on q[0] & q[1], q[0] & q[2], q[0] & q[3]

4: Observe the correlation between entangled pairs by performing Bell State Measurement

5: Perform cx operation on q[0],q[3]

6: Perform Hadamard operation on q[0] and q[3]

7: Perform cx operation on q[0],q[3], on q[0],q[2] then on q[0],q[1]

8: Store the output in Classical registers

9: Measure the information stored in the Classical register

4.5 ENCODING

Following the acquisition of maximally entangled pairs, the encoding part is in charge of encoding quantum information to these pairs on the Sender (Alice) side. To be ready for transmission, qubits undergo operations including the S gate, unitary operations, and CNOT gates. Encoding guarantees the security of the quantum data while it is being sent via the quantum channel. In encoding process, additional redundancy will be added in advance to handle the noise with extra qubits and quantum operations. After encoding the information, it will be transmitted through the quantum channel and if any error occurs then that will be measured using syndrome measurement with bounding function.

ALGORITHM FOR ENCODING

Input: Maximally Entangled Pairs

Output: Encoded Quantum Information $|\varphi\rangle$

1: Initialize the number of qubits n as 5

2: Initialize Quantum register q and Classical register c with size 5

3: Apply NOT operation on initial qubit

4: Apply S and U operations along with X,Y and Z axis

5: for i = 0 to n − 2 do

6: Perform CNOT operation on q[i] & q[i+1]

7: end for

8: for i = 0 to n − 1 do

9: Store the information from the quantum register to the Classical register

10: end for

11: Measure the information stored in the classical register

4.6 ERROR DETECTION AND CORRECTION

In classical error correction, syndrome measurement is used to find which error occurred on which input state based on that we can apply the same error to correct it. Similarly in quantum error correction, the syndrome measurement is used to retrieve the error information like which pauli error(X, Y, or Z) has occurred and on which physical qubit. Based on this information, the same pauli operator will be applied to the corrupted qubit to revert the error effect.

After encoding the data, if any syndrome has occurred while transmitting the information can be measured and corrected with the help of the bounding function and CNOT operations. The combination of ancilla qubits is used to detect the error on exactly which qubit it has occurred and then the operations are performed to correct it.

Interference or noise from the surroundings might cause errors to arise during transmission across the quantum channel. By utilizing extra qubits known as Ancilla qubits, the error detection module finds these problems. To find faults in the conveyed quantum information, methods like measurement operations and CNOT gates are used.

In order to guarantee the integrity of the quantum information conveyed, detected mistakes must be fixed. Based on the identified error patterns, the error correction module corrects faults by applying the proper quantum gates (X, Z, or their combination).Fixing mistakes contributes to the quantum communication system's continued dependability.

ALGORITHM FOR ERROR DETECTION AND CORRECTION

Input: Encoded Quantum Information transmitted through quantum channel $|\varphi\rangle$

Output: Encoded information along with the syndrome measurement $|A\rangle$ and $|\varphi\rangle$

1: Initialize number of qubits n as 8

2: Initialize Quantum register q, Classical register c with size 5

3: Initialize Ancilla Register a with size 3

4: q[0] ← Z

5: q[0]&q[5] ← Controlled NOT operation

6: q[1]&q[6] ← Controlled NOT operation

7: q[2]&q[5] ← Controlled NOT operation

8: q[2]&q[6] ← Controlled NOT operation

9: q[3]&q[7] ← Controlled NOT operation

10: q[4]&q[5] ← Controlled NOT operation

11: q[4]&q[7] ← Controlled NOT operation

12: for i = 0 to n/3 do

13: Store the information from quantum register to Ancilla register

14: end for

15: Measure the information stored in ancilla register

16: Initialize Ar with the combination of ancilla qubits

17: if Ar = 0 then

18: Append Z gate on initial qubit

19: end if

20: for i = 0 to n do

21: Store the information from Quantum register to Classical register

22: end for

23: Measure the information stored in classical register

4.7 DECODING

The decoding part on Receiver (Bob) side retrieves the original quantum information by reversing the encoding process when errors have been fixed. To decode the acquired quantum information back into its original form, certain operations are applied, including CNOT gates, S gates, and Unitary operations. By decoding, the sent quantum information is ensured to be accurately interpreted by the receiver.

ALGORITHM FOR DECODING

Input: Encoded information along with the syndrome measurement | A⟩ and |φ⟩

Output: The original information that has been shared initially |φ⟩

1: Initialize the number of qubits n as 5

2: Initialize Quantum register q, Classical register c with size 5

3: for i = n − 1 to 0 do

4: Perform CNOT operation on q[i] & q[i-1]

5: end for

6: q[0] ← Unitary operation

7: q[0] ← S

8: for i = 0 to n − 1 do

9: Store the information from the Quantum register to the Classical register

10: end for

11: Measure the information stored in the Classical register

CHAPTER 5

RESULTS AND ANALYSIS

The proposed asymmetric error correction method is used to transmit the single logical qubit information using 5-physical qubits and 3-ancilla qubits. The overall algorithm of AQEC contains the encoding, error detection and correction, and decoding operations.

The implemented modules are tested for various qubits, and the results have been documented.

- Entanglement between qubits is generated and purified for error management purposes.
- After the entanglement of qubits, the Quantum Key is generated by encoding the quantum information into those qubits whose results are illustrated in Figure 5.1.
- Once the Encoded Quantum Information is transmitted via the Quantum Channel from the sender side, the noise mitigated in the Quantum Information needs to be detected and corrected which was done by the Asymmetric Quantum Error Correction (AQEC) algorithm which uses extra qubits called Ancilla qubits, and measured qubits are illustrated in Figure 5.2.
- After performing the AQEC algorithm, the encoded and error–corrected information needs to be decoded to get the desired qubits on the receiver side and the decoded qubits information is illustrated in Figure 5.3.

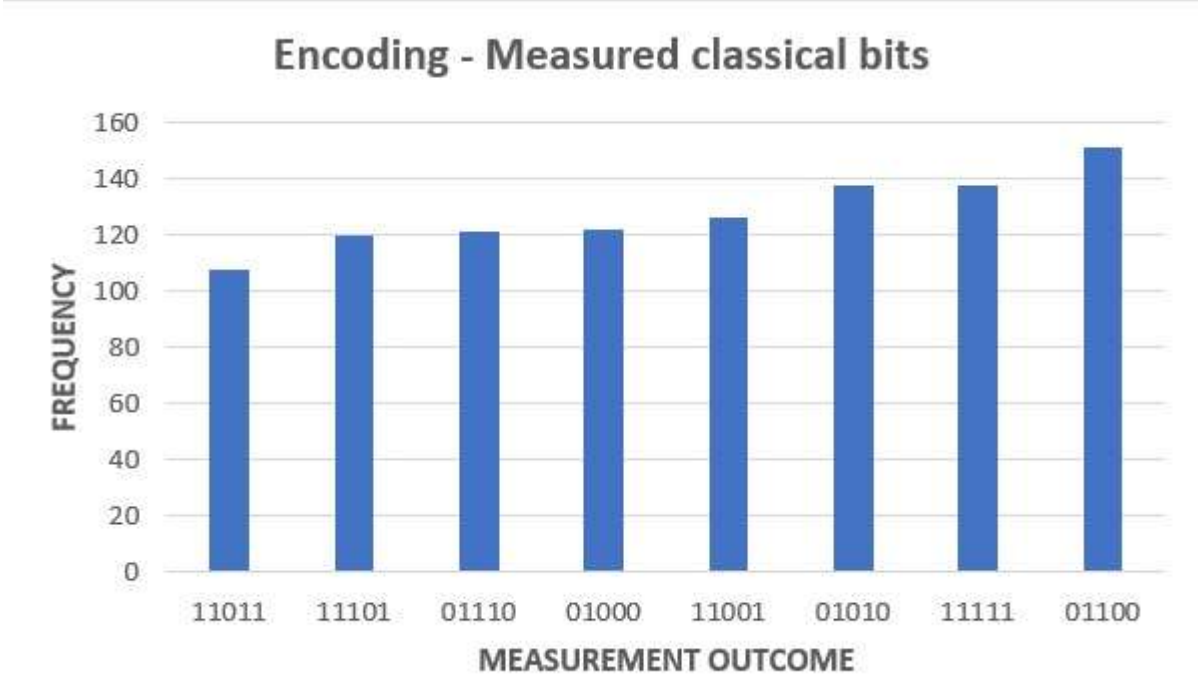

Figure 5.1 Encoded Qubits

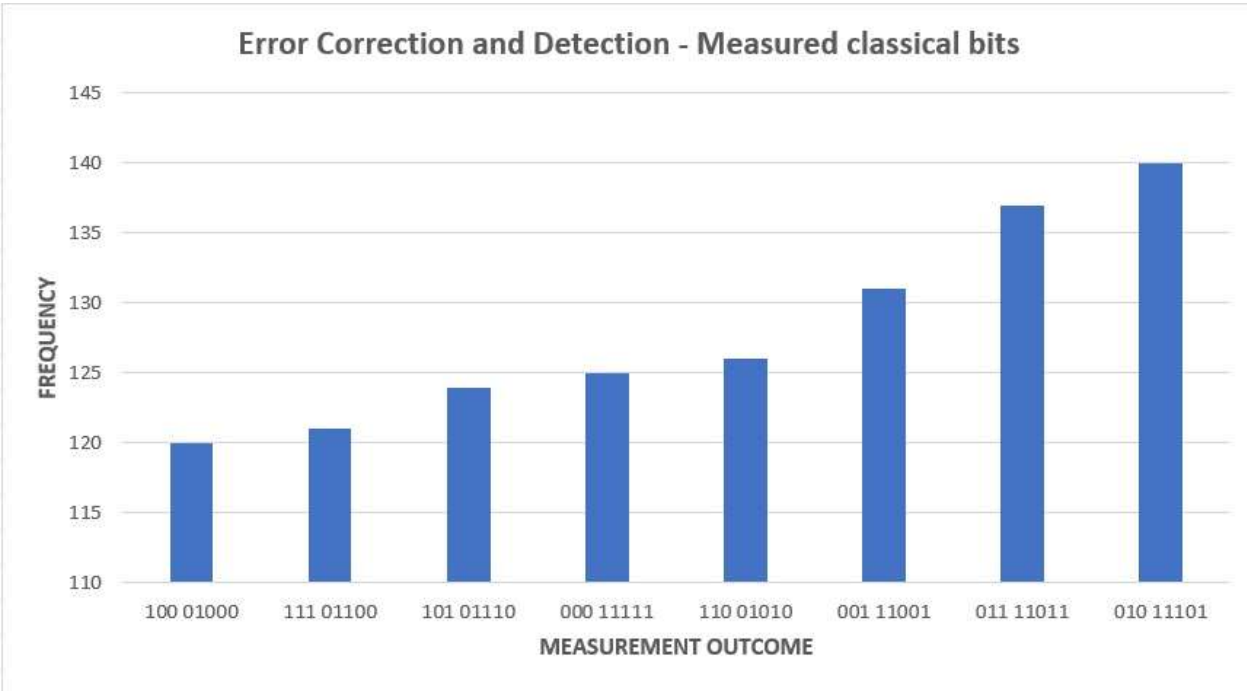

Figure 5.2 Qubits after Error Detection and Correction

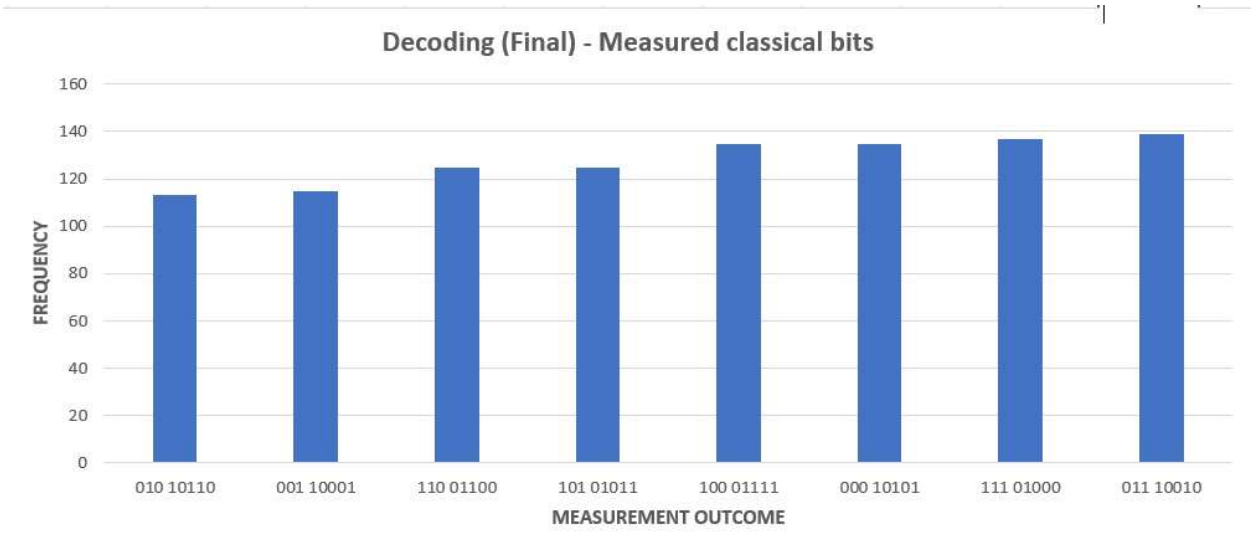

Figure 5.3 Decoded Qubits

Thus, the above-explained operations are done with the qubits. The results of the transmission of qubits with and without the application of the Asymmetric Quantum Error Correction (AQEC) algorithm are compared and the results are tabulated in Table 5.1.

Table 5.1 represents the results after applying AQEC algorithm.

PARAMETERS	WITHOUT AQEC	WITH AQEC
Error Probability	0.1358	0.1113
Success Probability	0.8642	0.8887

From Table 5.1, it is inferred that with the Asymmetric Quantum Error Correction (AQEC) algorithm, the success probability has increased which is illustrated in Figure 5.4 and the error rate has decreased which is illustrated in Figure 5.5.

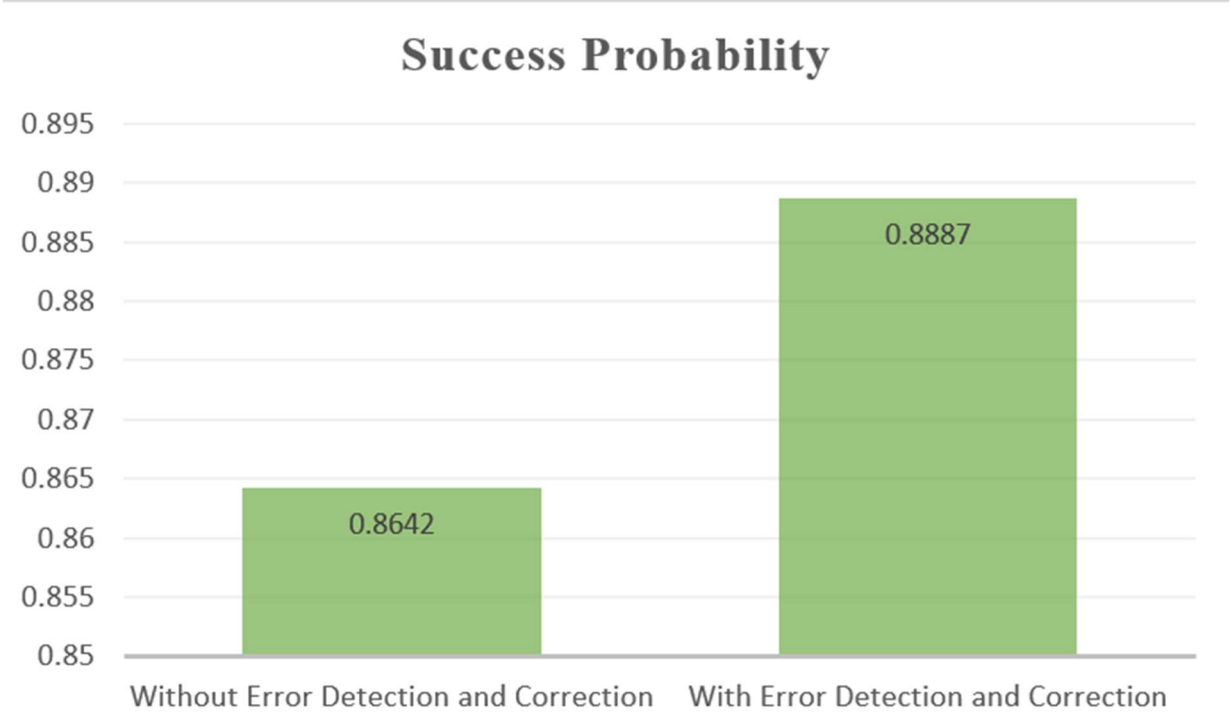

Figure 5.4 Comparison of Success Probabilities

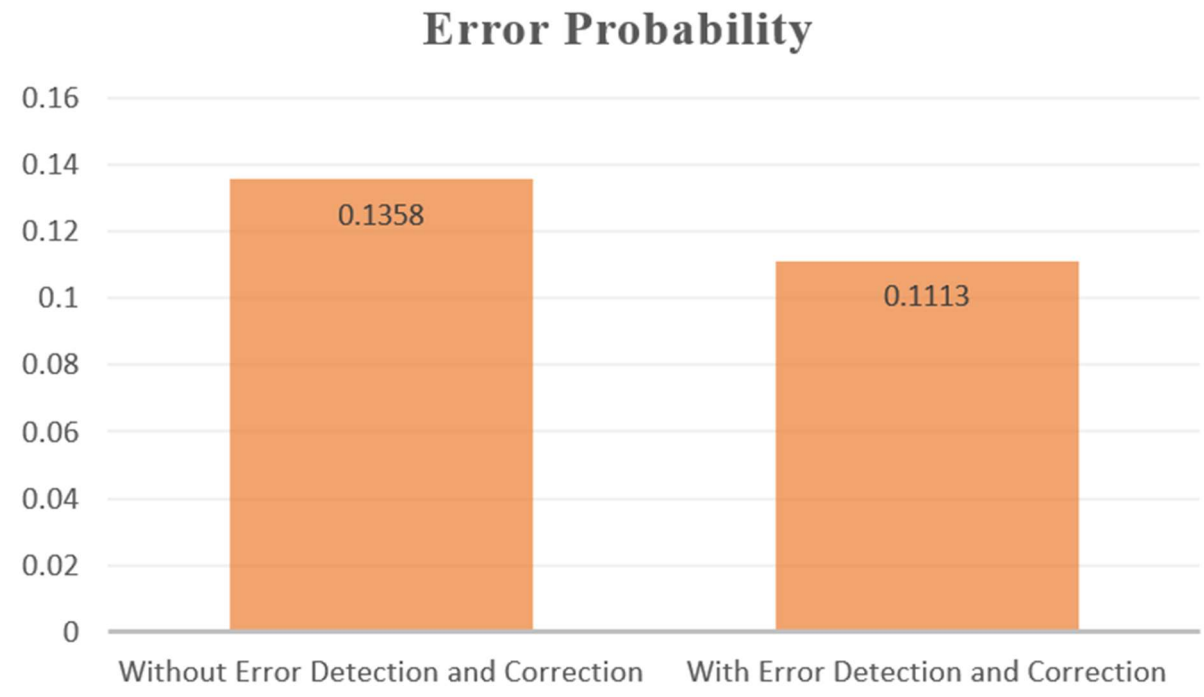

Figure 5.5 Comparison of Error Probabilities

CHAPTER 6

CONCLUSION AND FUTURE WORKS

In conclusion, this study highlights how crucial error correction algorithms are to maintaining the security and dependability of quantum key distribution (QKD) protocols in communications networks. Although QKD systems, like BB84, provide robust cryptographic security, their efficacy can be compromised by noise and malfunctioning channels. This work tries to reduce these issues and improve QKD systems' overall performance by applying sophisticated error-correcting algorithms. We want to assess the effectiveness and efficiency of these strategies in enhancing the dependability of critical distribution protocols using thorough analysis and simulation of demanding scenarios.

To further improve the fields of quantum key distribution and data security in telecommunications networks, future research efforts may concentrate on several important topics. To begin with, further research and development into sophisticated error correction techniques designed especially for QKD systems may result in notable increases in security and dependability. Furthermore, for QKD systems to be widely adopted, it would be imperative to improve and simplify the integration process into real secure communication networks. Additionally, continued research into cutting-edge QKD-compatible authentication and encryption methods may improve the overall security posture of the telecom network. We can improve data security in the telecom sector and set the stage for QKD to become an essential part of secure communication infrastructure by tackling these areas of future study.

CHAPTER 7

REFERENCES

1. C. Lee, I. Sohn and W. Lee, "Eavesdropping Detection in BB84 Quantum Key Distribution Protocols," in IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2689- 2701, Sept. 2022

2. Jia, W., Feng, B., Yu, H. and Bian, Y.. Quantum key distribution protocol based on CSS error correcting codes. In Proceedings of the ACM Turing Celebration Conference-China, pp. 1-8. May, 2019

3. Mummadi, S. and Rudra, B., Practical Demonstration of Quantum Key Distribution Protocol with Error Correction Mechanism. International Journal of Theoretical Physics, vol. 62, no. 4, p.86, 2023

4. F. Gao, "Practical Analysis of Discrete Variable Quantum Key Distribution," IEEE Transactions on Circuits and Systems (ICCS), Chengdu, China, pp. 140-143, 2020

5. E. O. Kiktenko, A. O. Malyshev and A. K. Fedorov, "Blind Information Reconciliation With Polar Codes for Quantum Key Distribution," in IEEE Communications Letters, vol. 25, no. 1, pp. 79-83, Jan. 2021

6. Majumdar, Ritajit, and Susmita Sur-Kolay. "Approximate ternary quantum error correcting code with low circuit cost." 2020 IEEE 50th International Symposium on Multiple-Valued Logic (ISMVL) IEEE, 2020.

7. Oulouda, Youssef, Mohamed El Falaki, and Mohamed Daoud. "Quantum Key Distribution Using a Single-Photon Added–Subtracted Squeezed Coherent State." Journal of Russian Laser Research 44.1 13-24, 2023

8. T. Tsurumaru, "Equivalence of Three Classical Algorithms With Quantum Side Information: Privacy Amplification, Error Correction, and Data Compression," in IEEE Transactions on Information Theory, vol. 68, no. 2, pp. 1016-1031, Feb. 2022

9. C. -Y. Wei, X. -Q. Cai, T. -Y. Wang, S. -J. Qin, F. Gao and Q. -Y. Wen, "Error Tolerance Bound in QKDBased Quantum Private Query," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 3, pp. 517-527, March 2020

10. B. Bilash, B. K. Park, C. Hoon Park and S. -W. Han, "Error-Correction Method Based on LDPC for Quantum Key Distribution Systems," International Journal on Information and Communication Technology Convergence (ICTC), Jeju, Korea, South, pp. 151-153, 2020

11. Basu, S., Saha, A., Chakrabarti, A. and Sur-Kolay, S. i-qer: An intelligent approach towards quantum error reduction. ACM Transactions on Quantum Computing, vol.3, no.4, pp.1-18, 2022

12. Basak, N., Das, N., Paul, G., Nandi, K. and Patel, N.,. Quantum secret sharing protocol using GHZ state: implementation on IBM qiskit. Quantum Information Processing,vol. 22, no. 11, p.393, 2023

13. M. Swathi and B. Rudra, "A Novel Approach for Asymmetric Quantum Error Correction With Syndrome Measurement," in IEEE, vol. 10, pp. 44669-44676, 2022

14. W. C. Lindsey, "Transmission of Classical Information Over Noisy Quantum Channels–A Spectrum Approach," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 3, pp. 427-438, March 2020

15. S. Shahriar and A. B. M. Alim Al Islam, "Extending Shor's Quantum Error Correction Circuits Using Quantum Adders," in IEEE Global Communications, Kuala Lumpur, Malaysia, pp. 1381-1386, 2023

16. Wade Trappe and Lawrence C. Washington, “Introduction to Cryptography with Coding Theory, 2nd Edition”, Prentice-Hall, Inc., USA. 2005

17. Vidick, Thomas, and Stephanie Wehner, “Introduction to Quantum Cryptography”, Cambridge University Press, 2023