Comparative Study of the Quantum Communication Protocol in Noisy Environment

A Dissertation Submitted

in Partial Fulfilment of the Requirements

for the Degree of

BACHELOR OF SCIENCE

in

Department of Computer Science

by

Sawan Bhattacharyya

(Registration No.: A01-1112-117-005-2019,
Roll No. : 2022161226)

Under the Supervision of

Amlan Chakrabarti

Ramakrishna Mission
Vivekananda Centenary College, Rahara

to

DEPARTMENT OF COMPUTER SCIENCE
RAMAKRISHNA MISSION VIVEKANANDA
CENTENARY COLLEGE
KOLKATA - 700 118, INDIA

June,2022

Dedicated to Ma, Baba, Didi, GM Sir, and Raja da

DECLARATION

I, **Sawan Bhattacharyya (Registration No: A01-1112-117-005-2019, Roll No: 2022161226)**, hereby declare that, this report entitled **Comparative Study of the Quantum Communication Protocol in Noisy Environment** submitted to Ramakrishna Mission Vivekananda Centenary College, Kolkata towards partial requirement of **Bachelor of Science** in **Computer Science** is an original work carried out by me under the supervision of Amlan Chakrabarti, A.K. Choudhury School of IT, University of Calcutta and has not formed the basis for the award of any degree or diploma, in this or any other institution or university. I have sincerely tried to uphold the academic ethics and honesty. Whenever an external information or statement or result is used then, that have been duly acknowledged and cited.

Kolkata - 700 118 **Sawan Bhattacharyya**

June 2022

CERTIFICATE

This is to certify that the work contained in this project report entitled **Comparative Study of the Quantum Communication Protocol in Noisy Enviornment** submitted by **Sawan Bhattacharyya** (**Registration No: A01-1112-117-005-2019, Roll No: 2022161226**) to Ramakrishna Mission Vivekananda Centenary College, Kolkata towards the partial requirement of **Bachelor of Science** in **Computer Science** has been carried out by him under my supervision and that it has not been submitted elsewhere for the award of any degree.

Kolkata - 700 106

Amlan Chakrabarti

June 2022

Dissertation Supervisor

External Examiner

ACKNOWLEDGEMENT

I want to extend a heartfelt obligation toward all the personages without whom the completion of the project was not possible. I express my profound gratitude and deep regard to my supervisor Amlan Chakrabarti, A.K. Choudhury School of IT, the University of Calcutta for his guidance, valuable feedback, and constant encouragement throughout the project. His valuable suggestions were of immense help. His never-ending enthusiasm to listen to my crazy ideas and adding his insightful suggestion, subsequently convinced me to think about the problem from an entirely different perspective. I sincerely acknowledge his constant support and guidance during the project.

I am equally grateful to Anindita Banerjee, CDAC, and Ajanta Das, Amity University for their immense support and guidance all through the project work. Anindita was always available for discussion which subsequently had improved toward the completion of my thesis.

I am immensely grateful to Mr. Debdeep Mitra of the University of Calcutta whose energetic nature and motivational words had kept me alive all through my work. I am highly grateful to Mr. Amit Saha, University of Calcutta whose energetic behavior had kept me up. I also highly acknowledge the help of Mr. Turbasu Chatterjee who help me a lot in coding. I am also grateful to the IBM Quantum Experience team for allowing me to do this project and providing all the required facilities and tools.

I express my sincere gratitude to Mr.Gautam Mahapatra, Asutosh College whose constant guidance, motivation, and care had given me the final boost toward the completion of this thesis.

I also want to express my deepest respect and love to all my dearest friends and seniors specially Rejoy, Arpan, Reja, Alapan, and Sreyan whose constant support and love had kept me alive from the inside, and who had stood with me in all the aspects either its bad or good since past three years.

Finally, I want to dedicate this thesis to my father, mother, and elder sister whose unconditional love and care had always inspired me. I want to express my deep gratitude and respect to my ideal Rajdeep Mukherjee who had planted the seed of being a researcher, more importantly a curious student. One who had appeared to me as a mentor and inspired me to choose this path. I might not have thought ever to choose to build my career in Computer Science if Rajdeep had not been there.

Kolkata - 700 118 **Sawan Bhattacharyya**

June,2022

ABSTRACT

Communication at present is rooted deeply in the concept of bits of zeros and ones which originated from Shannon's Theory of Information. Everything in today's digital world from advanced notebooks, to mobile phones, tablets, smartwatches, and laptops are all entrenched in classical communication techniques of zeros and ones. The security in this classical era is perfectly attained by harnessing the properties of primes, exploiting them through the mathematical structures of fields, and groups, or by using topological structures. The most popular and widely used classical cryptosystem, RSA (Rivest, Shamir, Adleman) is based on the mathematical hardness of prime factorization of the product of two large prime by any of the present classical processors. But the advancement in technology particularly in Quantum Information provides a threat to the present communication protocols. It motivates the researchers to move to new technologies that are fundamentally more secure through the principle of Quantum Mechanics. The search for Quantum Communication guarded by Quantum Cryptographic Protocols provides uncompromised security. Such protocols rely upon Qubits, quantum analogous to Bits for data transmissions. These qubits are quite sensible and thus any attempt to measure them by attackers left them to be disturbed and detectable by the legitimate users. But the Quantum Communication Protocols are prone to noise, being too much sensible their states are easily damaged by external factors. Besides the circuit noises Bit and Phase flipping there are other categories of noise. Depolarization, Amplitude Damping, Decoherence, Thermal Relaxation, and Phase Damping are obstacles to achieving long-distance communication. The dissertation focuses on the comparative study of Quantum Communication Protocols in a noisy environment and concludes with the robustness of protocols concerning different classes of noise.

Keywords: Quantum Communication, Quantum Entanglement, Quantum Superposition, Decoherence, Dephasing, Quantum Teleportation

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Communication in the modern world can be traced back to the 18th century when electricity came into the field and proved to be a promising candidate. From Communicating using Morse Code on telegraph lines to digital communication in modern-day computers and the internet, security had always been an indispensable part. In the digital communication binary data, bits that could either be 0 or 1 but not both are transferred from senders to receivers. These bits travel either through free space or through cables. These bits are physically realized through the variation in some physical quantity commonly voltage; they are transferred in cables in the same way as electricity gets transferred in a metallic wire. The noise that arises in the case of our classical communication is all sort of the interaction of electrical signals with the environment. Quantum Communication on the other hand is administered by the laws of Quantum Mechanics transfer data or more precisely Quantum states. These Quantum states are mathematically represented by the concepts of qubits (quantum bits). These qubits are governed by the law of Quantum Mechanics, Quantum Super-

position, Quantum Entanglement, and the particular no-cloning theorem. The last one i.e., no-cloning theorem is of particular interest because it satisfies the unconditional security of many of our Quantum Communication Protocols. The Quantum states cannot be copied and any attempt to do so would let a trace upon the measured qubit [6]. The trace is accounted for by a change in probability distribution which in turn let the measurement be detected, making the quantum communication inherently private. The qubit is also governed by the strange phenomenon of quantum entanglement where two distant qubits are correlated in such a way that measuring one qubit would be exposed the state of the second qubit. Entanglement is supported by the no-cloning theorem, making it impossible for the third party to copy the state of the qubit into its local qubits and entangled it with the other two. The qubits also show the phenomenon of quantum superposition which let the states of a number of qubits in a mixed form and individual states cannot be known unless being measured. In Quantum Computing, the data could be in a superposition of 0 and 1 states in addition to our 0 or 1 state. The superposition of states can be expressed as a mixture of the various state with their own probability of being measured. These qubits are physically realized by some entity that is governed by the principle of quantum mechanics such as a photon, trapped ion, superconducting loop, and much more. Quantum information is supposed to be encoded in matter qubits in our future generation of a quantum computer and photonic qubits are sent through the channel. The main reason is that photonic qubits are difficult to store and are prone to environmental loss of information. Qubits though having the potential of unconditional security lags behind classical bits by the factors of noise. Qubits are extremely fragile and are prone to a number of errors, the most common being decoherence. The main two categories of the quantum channel are free space channel and fiber optics cable. The reason for using these two as our quantum communica-

tion channel is that decoherence occurs within the limit of 20-30 km of atmosphere leaving much of free space with negligible loss while environmental factors are not significant inside the fiber optics for free space and optical fiber respectively. The technology will work in synergy with classical communication to overcome the limitation poses by traditional communication technology. The main limitation posed by our classical counterpart is its security which is unconditionally served by the quantum counterpart. The problem of key distribution in the classical domain is purposefully served by Quantum Key Distribution protocols, a prime candidate of Quantum Communication Protocols and our main area of focus in this dissertation [13].

1.1 Quantum Communication

Quantum Communication in the simplest term can be explained as the art of transferring quantum state from one place to other. Quantum information is encoded into qubits the unit of information in quantum information science. There are several ways to realize quantum communication in terms of the number of qubits required to encode one unit of information.

1. **One qubit:** The sender encodes the bit she wants to communicate with the receiver into one qubit and sends it.

2. **Two qubits:** There is a central source distributing entangled pair of qubits, one in the pair belongs to the sender and the other to the receiver.

3. **Three qubits:** The sender takes the help of an entangled pair of qubits, one belonging to him or her and the other to the receiver. The sender also uses one

extra qubit to prepare it in the state he or she wanted to transfer and perform the measurement in his or her part, the receiver, in turn, performs the operation in his or her part of the entangled pair depending upon the measurement result from the sender [12]. The information is teleported from the sender's ancillary qubit to the receiver part in the entangled pair.

4. **Four qubits:** The sender teleports the entangled pair also called entanglement swapping. Entanglement swapping is the key ingredient in the functionality of quantum repeater needed for long-distance quantum communication.

1.2 Quantum Communication Protocols

Quantum Communication protocols can be classified into the following classes based on the application and technique used [7].

- **Quantum Key distribution:** Cryptographic key distribution between sender and receiver.
- **Quantum authentication:** Verifies the identity of the sender and the integrity of the message transmit.
- **Quantum Oblivious transfer:** Sender sends much potential information to the receiver but is not aware of the content of the transmission. It finds many potential applications in secure computation, bit commitment, remote coin-flipping, and digital contract signing.

- **Quantum Teleportation protocols:** A somewhat different form of the protocol where the sender teleports quantum information to the receiver irrespective of the distance using entangled state [10].

Now in this thesis, Quantum Key Distribution had been focused on and studied which can further be classified into the following form

- **Prepare and Measure Protocols:** Sender prepares the quantum states which he or she wants to transfer according to the classical information and on the other hand receiver measures the received quantum state to obtain the information. Example BB84, B92, SARG04.
- **Entanglement Based Protocol:** Sender and receiver both depend on some central source or some third party to transmit the entangled pair-a part of which belongs to the sender and the other to the receiver. Example Ekert E91.

1.3 Quantum Noise Models

Quantum Communication even though provides unconditional security but lags behind classical communication in providing long-distance error-free transmission of information. Qubits are extremely fragile and prone to various noise and errors [11]. Noise that can arise in our communication protocols can be classified into two classes [2].

1.3.1 Circuit Noise

Circuit noise is a class of noise that arises in our quantum circuit due to defects in our circuits and hardware. Circuit noise can be further classified into two classes:

1. **Bit Flip:** Bit flip is an error where the qubits computational state flip from 1 to 0 and vice versa.
2. **Phase Flip:** Phase flip error affects the phase of the qubit. In essence, this error is equivalent to a Z-gate.

1.3.2 Channel Noise

Channel noise is a category of noise that arises in our channel and affect the qubits. Channel noise can be further classified into the following classes.

1. **Depolarization:** The polarize state of our photonic qubit depolarizes and consequently the encoded information is lost.
2. **Amplitude Damping:** The amplitude damping error is a quantum channel error that models physical processes such as spontaneous emission.
3. **Phase Damping:** Interaction with the environment can lead to loss of quantum information changes without any changes in qubit excitations.
4. **Amplitude-Phase Damping:** Combines the effect of phase and amplitude damping.

5. **Thermal Decoherence and Dephasing:** There are two aspects of noise in this error, the first one is thermal decoherence over time that occurs in the form of excitation and deexcitation and the second is the dephasing of the qubits over time [6].

1.4 Objective

The main objective of this dissertation is to study the effects of these categories of noise on Quantum Key Distribution protocols by categorizing these noise into main three noisy quantum channels.

1. **Depolarizing Channel**
2. **State Preparation and Measurement (SPAM) Channel**
3. **Thermal Decoherence and Dephasing Channel**

Further, the aim of this thesis is to calculate the secure key generation rate for the QKD protocols.

1.5 Organization

The dissertation had organized into chapters.

The first chapter, "Introduction" gives a breif overview of Quantum Communication,it various protocols and the noise models that had been studied.

The second chapter "Theory of Quantum Communication" which deal with the theoretical background of the Quantum Key Distribution mathematical formulation of the secure key generation rate. It also introduces the three noise channels that had been studied in the dissertation. It also discusses the fundamentals of quantum computing.

The third chapter, "Methodology" species the algorithm studied and the tool used for the purpose. It specifies the various packages and modules that had been used in the study.

The fourth chapter, "Result" specifies the probability distribution for the three types of noise channels. It also specifies the experimental result for the outcomes of the bits and the secure key generation rate for the three noisy channels.

The fifth chapter, "Discussion and Conclusion" analysis the result and draw a conclusion based on the experimental result.

The sixth chapter, "Challenges and Future Work" describe the challenges that had been arises in the research with a future direction.

Chapter 2

Theory of Quantum Communication

The concept of computation is as old as the history of science itself. Philosophers, mathematicians, physicists, and engineers were too much concerned with the issue of computation. The development of computers contributed by the work of Babbage, Neuman and others once again ignited the concern with the issue of computation. The first remarkable progress in this field was brought by Alan Turing who is widely regarded as the father of artificial intelligence and theoretical computer science. Turing in the year 1936 provided an edge toward the mathematical formulation of the computation by introducing the concept of the Turing Machine [8]. Turing Machine is a mathematical model of computation which takes both numbers and symbols as input rather than numbers as proposed by John Von Neuman. Subsequent development in the field was put forward by the formulation of the Church Turing thesis. The thesis claim that any real-world computational process can be translated into

an equivalent Turing machine.
With the rapid development in the field of computer science, a modified version of the thesis came into the stage. The modified church Turing thesis claim that any reasonable computational process can be efficiently solved by a probabilistic Turing machine. The main differences in this modified church Turing thesis are

- The simulation was required to be efficient
- The computational model of Turing was replaced by a probabilistic Turing machine.
- The term reasonable computational process also included analog computation along with digital computation.

Church Turing's thesis is not a mathematical statement hence there doesn't exist any rigorous proof for the thesis. It had been considered as an axiom and widely used by computer scientists as validation of the computational problems.[8]However with the development in the field of quantum computational models need for the validation of the thesis is felt widely.

2.1 Fundamentals

2.1.1 Quantum Mechanics

The protocols of quantum communication and the model of quantum computation are governed by the laws of quantum mechanics. Quantum mechanics describe a

system by specifying a vector space-Hilbert space. The following six postulates describe a discrete system.

1. At a fixed time t_0, the state of a physical system is defined by specifying a normalized vector in the state space $\mathcal{V}$. The standard notation is the Dirac notation as $|\psi(t_0)\rangle$.

2. Every measurable physical quantity $\mathcal{A}$ is described4ed by a linear operator A called as observable acting in $\mathcal{V}$.

3. The only possible result of the measurement of the physical quantity $\mathcal{A}$ is one of the eigenvalues of the corresponding observable A.

4. When a physical quantity $\mathcal{A}$ is measured on a system in state $|\psi(t_0)\rangle$, the probability of obtaining the eigenvalue a_n of the observable A is given by:

$$Pr(a_n) = |\langle u_n|\psi(t_0)\rangle|^2 \tag{2.1}$$

   where $|u_n\rangle$ is the normalized eigenvector of A associated with the eigenvalue a_n $\langle u_n|\psi(t_0)\rangle$ denotes the inner product of the vectors $|u_n\rangle$,$|\psi(t_0)\rangle$. The math above is true when the eigenvalue is nom degenerate. The general case is formulated as:

$$Pr(a_n) = \sum_{i=0}^{g_n} |\langle u_n^i|\psi(t_0)\rangle|^2 \tag{2.2}$$

   where g_n is the degree of degeneration and $|u_n^i\rangle$ is an orthonormal basis of the eigensubspace associated with the eigenvalue a_n.

5. After performing a measurement on the system and getting a result a_n the

system is no longer in its previous state but in a state corresponding to the eigenvalue a_n.

6. The time evolution of the state vector $|\psi(t_0)\rangle$ is governed by the Schrodinger equation:

$$ih\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle \tag{2.3}$$

where *H(t)* is known as Hamiltonian representing the total energy of the system.If this Hamiltonian is independent of time and time is discrete the modified version of the Schrodinger equation:

$$|\psi(t=1)\rangle = U|\psi(t=0)\rangle \tag{2.4}$$

where U is an unitary transformation in $\mathcal{V}$.

Some phenomenal properties of quantum mechanics are discussed next:

1. **Quantum Superposition:** Quantum superposition is a fundamental principle of quantum mechanics, it states that any two quantum states can be added or superimposed and the results would be another valid quantum state. A pure qubits state is a coherent superposition of the basic state. This means that a single qubit can be described by a linear combination of $|0\rangle$ and $|1\rangle$

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.5}$$

where α and β are probability amplitude and in general both are the complex number.According to born rule, probability of $|0\rangle$ with value 0 is $|\alpha|^2$ and the

probability with outcome $|1\rangle$ with value 1 is $|\beta|^2$.Because the absolute square of the amplitude equate to probability it must be true that

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.6}$$

Note that the qubit superposition state does not have a value between 0 and 1 rather there is a probability of $|\alpha|^2$ that it attains a 0 state and a probability of $|\beta|^2$.In other words, superposition means that there is no way, even in principle, to tell which of the two possible states forming the superposition state pertains.

2. **Quantum Entanglement:** Quantum entanglement is a physical process that occurs when a pair or group of particles is generated or interacts in such a way that the quantum state of each particle of the pair cannot describe independently of the state of other in the pair [8]. The simplest systems to display quantum entanglement is the system of two qubits, two entangled qubits

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \tag{2.7}$$

in these states of equal superposition, there are equal possibilities of measuring either the product state with $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$ as $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{}$, i.e., there is no way to tell that whether the first qubit has the value of 0 or 1 and same with the case of second qubit.

3. **Heisenberg Uncertainty principle:** Heisenberg uncertainty principle is the fundamental law that governed the security of most quantum communication protocols. The principle state that the more precisely the position of some particle is determined, the less precisely its momentum can be predicted from initial conditions, and vice versa. Mathematically the principle can be formulated as:

$$\Delta x \Delta p \geq \frac{h}{4\pi} \tag{2.8}$$

In the above formulation, x and p represent the position and momentum respectively. The more precisely the value of the position is determined the less precise the momentum and vice versa in order to satisfy the inequality.

2.1.2 Bits and Qubits

In quantum computing or quantum communication, the information is encoded in qubits the quantum analogous to classical bits used in classical communication. Quantum bits are a two-state system representing binary 0 and 1. Qubits show the unique property of quantum superposition and quantum entanglement. Due to the superposition property, they can exhibit quantum mechanical coherence properties [3]. Because of this, although all classical information protocols can be implemented with qubits, there are quantum information protocols that cannot be implemented using classical bits. One example is quantum key distribution, which is a method of sharing unconditionally secure secret keys between legitimate users as described earlier in the context.

A qubit lives in a two-dimensional quantum system, which means that its Hilbert space is spanned by two basis states (refer Figure 2.1).

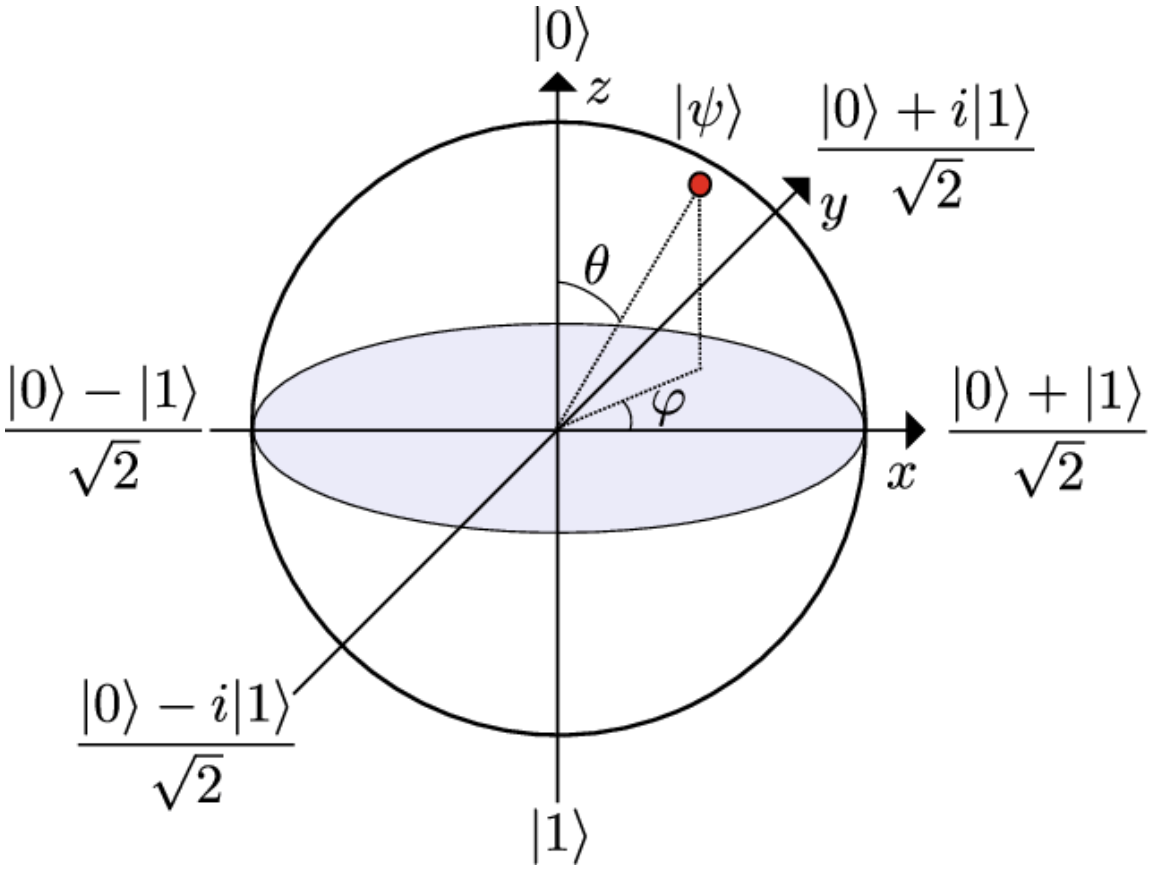

Figure 2.1: Representation of Qubit in three dimensional Bloch Sphere where z axis denotes the computational basis,x axis denotes superpositions of computational basis and y axis denotes superpositions of computational basis in argand plane

The two orthogonal states of the system are denoted as $|0\rangle$ and $|1\rangle$, form a complete basis for the Hilbert space of the qubit. This basis is referred to as the computational basis [12]. Any other basis can be expressed by linear combinations of the computational basis.

All states of the qubit can be expressed on the computational basis as:

$$|\psi_{qubit}\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle \tag{2.9}$$

The angles θ and ϕ are two independent degrees of freedom and they define a point on the unit sphere in a three-dimensional space. Thus, we can visualize the state of a qubit as a vector pointing from the origin to the unit sphere, as shown in This sphere is referred to as the Bloch sphere.

In order for a qubit to be useful, we must be able to perform three fundamental operations on it: prepare it in a well-defined state, apply controlled unitary operations on it, and be able to measure it. Physical systems that are suitable as qubits in quantum information and quantum computation applications are primarily atoms, nuclei, and photons. One additional requirement especially important for quantum communication is the ability to exchange qubits over long distances. For such applications, the photon is the only practical information carrier because it is extremely robust to environmental noise and can be transmitted over long distances in optical fibers as discussed earlier [5]. Below we discuss the qubit requirements for the photonic qubit, which set the stage for our work.

The requirements for the photonic qubits to be useful in our quantum communication can be listed in the following ways.

1. **State preparation:** Qubit can be prepared using a single photon by the spatial mode, polarization mode, and time slot implementations.

    - In the first case, the single photon in mode 1 is split into two spatially separated modes 2 and 3 using a beamsplitter and a phase shifter hence the state of photon become

$$|1\rangle_1 \rightarrow |\psi_{qubit}\rangle = \cos\theta|1\rangle_2|0\rangle_3 + e^{i\phi}\sin\theta|0\rangle_2|1\rangle_3 \tag{2.10}$$

Thus binary information can be encoded in the presence of the photon as

$$\begin{aligned} |0\rangle &= |1\rangle_2 |0\rangle_3 \\ |1\rangle &= |0\rangle_2 |1\rangle_3 \end{aligned} \tag{2.11}$$

- In the polarization technique the two spatial modes are replaced by the two polarization states of a single spatial mode. Thus binary information can be encoded in horizontal or vertical polarization as

$$\begin{aligned} |0\rangle &= |H\rangle \\ |1\rangle &= |V\rangle \end{aligned} \tag{2.12}$$

  These techniques are not well suited for long distance communication because they are very sensitive to polarization drifts and phase instability in long optical fibers.

- There is another very practical implementation of photons that are well suited for long-distance communication. A single-photon in mode 1, which defines a transform-limited wavepacket in space and time, is sent through an unbalanced interferometer, which has a short and a long arm. The long arm introduces a time delay relative to the short arm, which is greater than the coherence length of the input photon. The output of the interferometer is two pulses separated in time. Assuming this time separation is sufficiently long so that the two time slots can be treated as orthogonal modes, we can define the modes corresponding to time slots t_1 and t_2. Qubit state after passing through the unbalanced interferometer becomes

$$|\psi_{qubit}\rangle = \cos\theta |t_1\rangle + e^{i\phi} \sin\theta |t_2\rangle \tag{2.13}$$

The information, in this case, is encoded in the relative phase of the two-time slots t_1 and t_2.

This information remains undisturbed during propagation in optical fiber because the time separation of the two pulses is usually very short, on the order of a nanosecond, while the phase and polarization drifts occur at long time scales, so the pulses undergo the same distortion in the fiber. This fact makes time slot implementation advantageous for long-distance quantum communication. The above technique is used in differential phase shifting QKD.

2. **Unitary Operation:** Manipulation of the quantum information needed to perform controlled unitary evolution, which means that we should be able to transform the qubit from its initial state to any other state on the Bloch sphere. The transformation must conserve probability, hence it must be described by unitary operators, which can be thought of as rotations or combinations of rotations on the Bloch sphere. Transformation is easy in the case of a photonic qubit.

3. **Measurement:**The theory of quantum measurement can be described by two postulates:

   - Postulate 1: The wavefunction of a quantum particle is represented by a vector in a normalized Hilbert space which is spanned by an orthonormal basis $|0\rangle, |1\rangle, ..., |n-1\rangle$, where n is the dimensionality of the Hilbert space. Every measurement is represented by a projection onto a complete orthonormal basis which spans the Hilbert space. Define this basis as $|P_0\rangle, |P_1\rangle, ..., |P_{n-1}\rangle$ The probability of measuring the qubit in the state

$|P_i\rangle$ is simply given by $|\langle P_i|\psi\rangle|^2$, where $|\psi\rangle$ is the wavefunction of the qubit.

- Postulate 2: Define the wavefunction of a quantum system before measurement as $|\psi\rangle$. Define the measurement basis as $|P_0\rangle, ..., |P_{n-1}\rangle$ Given that the the system was measured in the state $|P_i\rangle$, the wavefunction of the system after the measurement is also $|P_i\rangle$.

2.1.3 Classical and Quantum Gates

In any classical computation, logic gates are the fundamental building block of the circuit. They can be seen as the operator or transformation upon classical bits. Mathematically these classical logic gates can be seen as a square matrix and these classical bits as a column vector. Examples NOT gate, AND gate, OR gate, XOR gate, and so on. In quantum computing, manipulation of the qubits which corresponds to the quantum analog of the classical bits is acted upon by a quantum gate. These quantum gates act on these qubits which live in a two-dimensional Hilbert space and can be represented by a two-dimensional vector. The mathematical representation of these quantum gates can be done with a square matrix.

The main point of difference between the classical logic gate and the quantum gate is that the latter is reversible. In the quantum world, all operations that are not measurements are reversible and are represented by unitary matrices. AND gate is not reversible, one cannot determine the input from merely the output. In contrast, NOT and Ifentidty gate are their inverse and hence reversible. Reversible gates have a history that predates quantum computing. Our everyday computers lose energy and generate a tremendous amount of heat. In the 1960s, Rolf Landauer analyzed

computational processes and showed that erasing information, as opposed to writing information, is what causes energy loss and heat. This the notion has come to be known as Landauer's principle. A quantum gate is simply an operator that acts on qubits. Such operators will be represented by unitary matrices. These reversible gates can be represented as matrices, and as rotations around the Bloch sphere. Some of the standard gates used frequently in quantum computing are

1. **Pauli gates:** These are group of common three gates often represented as σ_x, σ_y and σ_z.

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$$

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

   All these gate perform π rotation around x, y and z axis.

2. **Hadamard Gate:** This creates a superposition of $|0\rangle$ and $|1\rangle$. The matrix representation of the is

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

   It acts upon the computational basis as

$$H|0\rangle = |+\rangle$$

$$H|1\rangle = |-\rangle$$

3. **P gate:** The P-gate (phase gate) is parameterised, that is, it needs a number (ϕ) to tell it exactly what to do. The P-gate performs a rotation of ϕ around the Z-axis direction. It has the matrix form

$$P(\phi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

where ϕ is a real number.

4. **I, S and T gate:**

- I is basically an identity matrix and used where the syntax need a gate but the logic does not.

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- S gate is a special form of P gate which turns around the bloch sphere with $\phi = \frac{\pi}{2}$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{2}} \end{bmatrix}$$

- T gate is a very common gate which does a turn of $\phi = \frac{\pi}{4}$

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$$

5. **CNOT Gate:** CNOT gate is a two qubit gate that act on two qubits. This gate is a conditional gate that performs a X-gate on the second qubit (target),

if the state of the first qubit (control) is $|1\rangle$.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

2.2 Quantum Communication

Quantum communication can be stated in a simple term as the transfer of a quantum state from one place to another. The motivation behind encoding our classical information in a quantum state is the unconditional security provided by this quantum system. Another motivation that excited physicists and engineers to switch from classical systems to the quantum system-the close correlation between quantum communication and quantum nonlocality as illustrated by the process of quantum teleportation. The quantum states are encoded in a quantum system-qubits that lives in a two-dimensional Hilbert space.

The best known and widely studied example of quantum communication is Quantum Key Distribution where the process of cryptographic key distribution is governed by the laws of quantum mechanics. Traditionally the two legitimate parties-sender and receiver depend on the orientation of the quantum states, polarization in the case of photonic qubits to either encode or decode information.

Some of the other quantum communication protocols besides QKD are Quantum Oblivious Transfer where the senders send much potential information to the receiver but the sender is himself not aware of the specific content of the transmission. Informally speaking the sender sends a message to the receiver which the receiver

received half of the time. The sender does not know anything about the outcome but the receiver knows whether he has received the message or not. The first prominent form of oblivious transfer was proposed by Shimon Even, Oded Goldreich, and Abraham Lempel called 1-out-of-2 quantum oblivious transfer or 1-2 oblivious transfer.
1-2 obvious transfer is basically two-party protocols where the sender chooses two input bits x_0 and x_1 and the receiver chooses a single input bit b. The protocol outputs x_b to Bob with the guarantees that Alice does not know b, and that Bob does not know $x_b \otimes 1$. A cheating Alice aims to find the value of b, while a cheating Bob aims to correctly guess both x_0 and x_1.
Another yet most important Quantum Communication protocol is the Quantum authentication Protocol which certifies the identity of the sender and the integrity of the message sent traditionally authentication and identification of the sender it's done through the use of the hash function. the security of these hash-based authentication models depends on the appropriate selection of the hash function and the use of long authentication keys. The use of quantum phenomenon makes it possible with the help of just one qubit. A different form of quantum communication technique that has motivated physicists and engineers over the decade is that of quantum teleportation as mentioned earlier. Quantum teleportation is based on the principle of quantum entanglement. Quantum teleportation involves sending quantum information between two distant parties. Quantum teleportation is achieved by the phenomenon of quantum entanglement. It allows transmitting an arbitrary qubit from a location a to location b using a preshared pair of entangled qubits sent over by some third party or central source.

2.2.1 Quantum Communication Techniques

1. **Quantum Key Distribution:**

   The goal of the quantum key distribution protocol is to generate a shared secret key between the sender and receiver over a public communication channel. The protocols are guided by the laws of physics or to be more specific by the law of quantum mechanics that guarantees the security against any possible attack that an adversary can perform. Generally, the QKD protocols can be divided into two-phase, the first phase is the quantum transmission phase where the two legitimate users encode or decode the quantum information to or from qubits. The second phase is that of the classical post-processing phase where they generate the secure key from the bit string generated during transmission. The quantum transmission task is usually performed by the polarization in the case of the photonic qubit where a specific degree of polarization orientation represents one specific bit of information (refer Figure 2.2). Example: The most prominent example here is the BB84 developed by Bennet and Brassard in the year 1984, other examples include Ekert E91 Protocol, B92 Protocol, and SARG04 protocol.

2. **Quantum Authentication:**

   The Quantum Authentication protocol is related to finding the identity of the sender and the integrity of the sender. The QKD technique had provided a new edge in the process of secure communication but there exists a serious loophole in it. The prior technique can easily detect the presence of the attacker but provides no information regarding the identity of the sender, i.e., the receiver can never know whether the message came from a legitimate user or attacker.

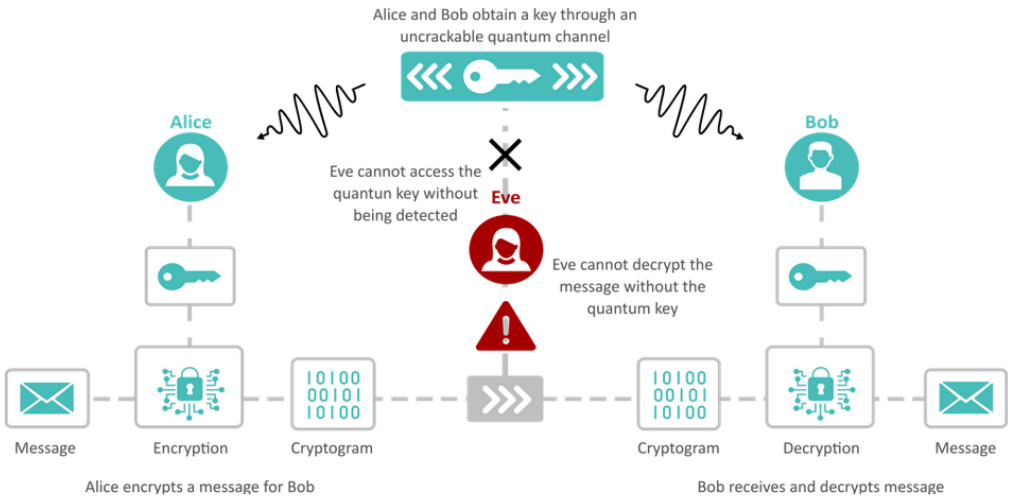

Figure 2.2: Schematic diagram of a typical Quantum Key Distribution protocol

The attacker can easily mislead the receiver by sending misleading information through the same channel as previously used by the sender. This is the point where the authentication came into play which guaranteed that the message just came from the legitimate sender and not from the attacker. In the classical area, the authentication is usually done by the use of the hash function to create a digital signature. Now in the case where the sender sends quantum information instead of classical information, the classical authentication technique won't work because it would no longer work as it fails to preserve the superposition, instead a new authentication protocol is needed based on the laws of quantum mechanics. In a standard quantum authentication scheme, the idea is to encode the quantum state in a quantum error-correcting code. Instead of using only one error-correcting code there is a need to use family of code to reduce the chances of creation of errors by attacker in the used correcting code (refer Figure 2.3).

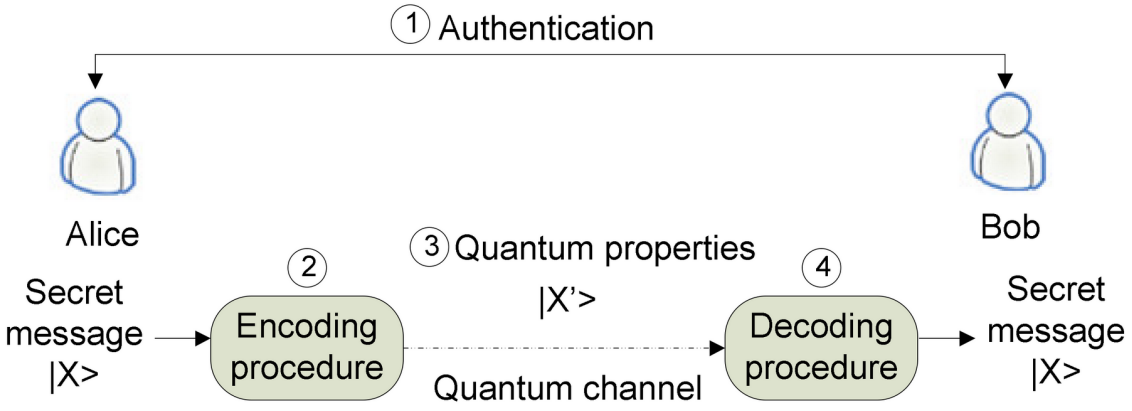

Figure 2.3: Schematic diagram of a typical Quantum Authentication Protocol where authentication is carried out in a separate channel apart from the transmission channel

3. **Quantum Teleportation:** Quantum teleportation is a technique for transferring quantum information from a sender at one location to a receiver some distance away. While teleportation is commonly portrayed in science fiction as a means to transfer physical objects from one location to the next, quantum teleportation only transfers quantum information. Moreover, the sender may not know the location of the recipient, and does not know which particular quantum state will be transferred.

   Classical communication uses two-state systems to encode a single bit of information. If one wants to send a certain amount of information, consequently one has to physically transfer the corresponding number of such systems. The question now arises as to whether one can use quantum systems to communicate classical information more efficiently and also whether it is possible to transfer quantum information, i.e., the state of a quantum system, itself. In the original proposal of quantum teleportation it was realized that the foremost

requirement for the sender and the receiver is first to share an entangled pair of particles (refer Figure 2.4).

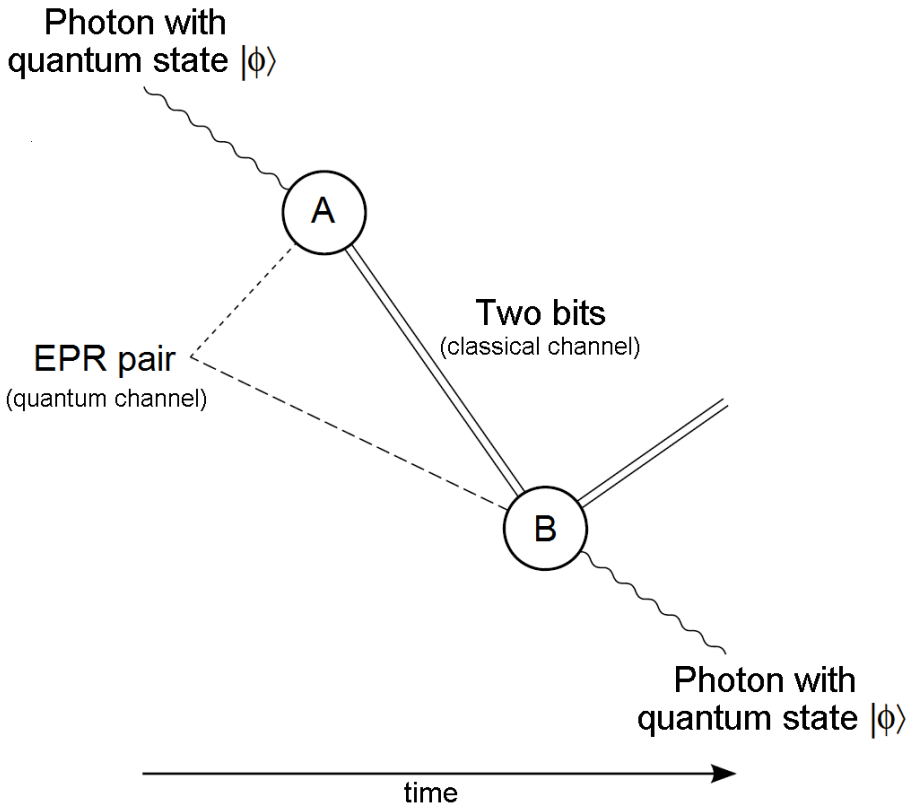

Figure 2.4: Schematic diagram of typical Quantum Teleportation Protocol where the entangled pair got transmitted through quantum channel and classical measurement result through a classical channel

The requirements of quantum teleportation are (i) the Einstein–Podolsky–Rosen (EPR) source for entangled pairs of particles; (ii) a component (U) performing unitary operations on a two-state quantum particle given one of four classical messages; and (iii) the so-called Bell-state measurement (BSM), where a pair of two-state particles is projected onto the Bell-state basis given by four

maximally entangled orthogonal states

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle \pm |V\rangle|H\rangle), |\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle|H\rangle \pm |V\rangle|V\rangle)$$

2.2.2 Quantum Cryptography-Quantum Key Distribution

The Quantum Key Distribution technique as discussed in the previous sections is not sufficient to use in the real world. The key obtained after decoding by the receiver contain a lot of error that need to be mitigated. Thus to achieve the goal of security and filter the key from errors two more steps are needed in addition to encoding and decoding the quantum information (refer Figure 2.5).

The general steps involves in a QKD Protocol are:

- **Quantum Transmission:** In the quantum transmission step, the sender and receiver share a random string of bits transmitted over a quantum channel. Most quantum key distribution protocols belong to one of two categories, single qubit protocols and entangled qubit protocols.

  Single qubit protocols make use of the measurement uncertainty properties to ensure secrecy. Important examples of single-qubit protocols are the BB84, B92, Koashi01 and six-state protocols.

  Entangled qubit protocols use the non local correlations to achieve security. They rely on the fact that if any local variable exists which can predict the state of an entangled qubit pair, then non local correlations are not observed. Important examples of entangled qubit protocols are the Ekert91 and BBM92 protocols.

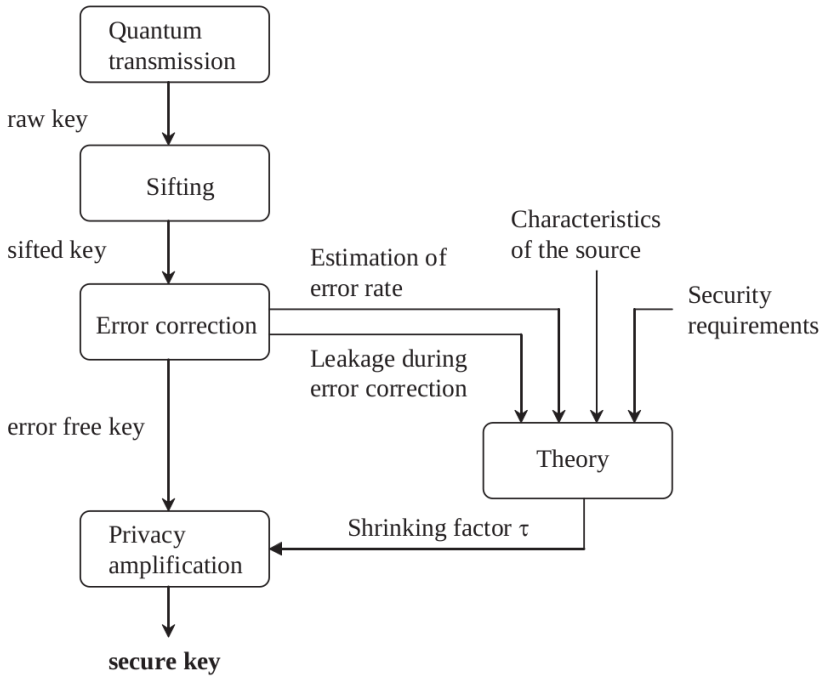

Figure 2.5: Schematic diagram of steps in a typical Quantum Key Distribution protocol explaining the flow from raw key to secure key

The outcome of the first step is an ensemble of bits called the raw key. The raw key generation rate R_{raw} is simply equal to the product of the repetition rate of the transmission and the probability of a photo detection event registered by the detectors in the measurement setup.

- **Shifting:** The shifting phase correspondence to the measurement stage where the sender and receiver discard those bits where their measurement basis does not match. The two legitimate users use a public channel to communicate information regarding the basis they choose for measurement. The process of discarding the bits in the cases where they used different bases is called sifting. The ensemble of bits remains after the basis reconciliation from the shifted key,

the rate of generation of the shifted key is given by:

$$R_{shifted} = sR_{raw} \tag{2.14}$$

If there are no errors in the cryptographic system then a potential eavesdropper cannot yield any information regarding the transmission of a message without being detected. In this case there the shifted key is unconditionally secure. However in any practical communication system error naturally occurs due to a defect in the device (circuit noise) or the line of transmission (channel noise). Thus, in practical systems, the statement that any eavesdropping will unavoidably cause errors and reveal that eavesdropping is there is not sufficient security proof. There is always a baseline system error rate so we must take into account that some information about the transmission had been leaked. Consequently, we must be able to bound the amount of information leaked given the error rate. A practical QKD system handles system error and eavesdropping by following two additional steps i.e. error correction and privacy amplification. These additional steps can be performed in a public channel.

- **Error Correction:** The error correction step serves the dual purpose of correcting all erroneously received bits and giving an estimate of the error rate. The sender reveals some additional information to the receiver about his or her key that will allow the receiver to find and correct all of the error bits. One possible technique is that the two parties can group their bits in the segment and check the parity and optimize the segment size as the error process continues.Since this process occurs in the public channel it would naturally leak some additional information to the attacker. Thus this information leaked needs to be as small as possible. The minimum number of bits in forming the

segment needed for the error correction is given by the result from the classical information theory, Shannon's noiseless coding theorem. The theorem asset that

$$\lim_{x\to\infty} \frac{\kappa}{n} = -e \log_2 e - (1-e)\log_2(1-e) \equiv h(e) \tag{2.15}$$

where n is the length of the shifted key and κ is the size of the disclosing segment. Unfortunately, Shannon's theorem has a nonconstructive proof,i.e. we know that there exists an error correction scheme disclosing only κ bits but the theorem does not provide an explicit procedure for this scheme. An error-correcting algorithm should ideally operate very close to this limit.

There are two classes of error-correcting schemes, unidirectional and bidirectional. In the prior case information, only flow from the sender to the receiver, and the4 sender provides the receiver with the additional string needed for error correction. It's difficult to design an algorithm that is both computationally efficient and works near the Shannon limit. In the bidirectional scheme, information flows from both ends. The receiver sends feedback to the sender and the sender work up[on the feedback to detect what additional information is needed for error correction. These two error correction algorithms classes can be further subdivided into algorithms that discard errors and algorithms that correct them. Discarding errors is usually done to prevent additional side information from leaking to the attacker. By correcting the errors we allow for this additional flow of side information, which can be accounted for during privacy amplification.

- **Privacy Amplification:** Privacy amplification corresponds to the compression needed to account for the information leaked during transmission and error correction. The amount of compression depends on the amount of information

leaked in the previous phases. For a security proof to be useful it must be bound to the amount of the information leaked and relates it to how much compression is needed in privacy amplification.

There are three categories of generalized attacks that have been considered: individual, collective, and coherent attacks. The ability to perform collective and coherent attacks is well beyond today's technological advancement. In this dissertation, we will focus on individual attacks because they can be realized with the current scenario with some assumptions.

The role of the privacy application step is to deduce the shrinking factor τ by which the corrected key need to be compressed to account for the information leaked during the transmission and error correction steps. This calculation is performed using the methods of the generalized privacy amplification theory, which makes the worst case assumption that all errors are potentially caused by eavesdropping. The shrinking factor τ is given by

$$\tau = -\frac{\log_2 p_c}{n} \tag{2.16}$$

where p_c is the average collision probability. The theory set the length of the final key as

$$r = n\tau - \kappa - t \tag{2.17}$$

The average collision probability is the measure of the attacker's mutual information with the two legitimate users. This factor is a function of the error rate and parameter of the specific cryptographic system.

The secure key generation rate is a much more important and useful quantity to study the effect of noise over QKD protocols. It can also be defined

normalized communication rate.If N is the length of the transmission, then $n = NR_{shifted} = NsR_{raw}$, secure key generation rate id given by

$$R = \lim_{N\to\infty} \frac{r}{N} = \lim_{x\to\infty} R_{shifted} \left(\tau - \frac{\kappa}{n} - \frac{t}{n} \right) \tag{2.18}$$

In the limit of long string $\frac{t}{n} = 0$ and $\frac{\kappa}{n}$ is the fraction of additional information disclosed during error correction.None of the practical algorithm work at the Shannon's limit.Thus,

$$\lim_{n\to\infty} \frac{\kappa}{n} = -f(e)[e \log_2 e - (1-e)\log_2(1-e)] = f(e)h(e) \tag{2.19}$$

where $f(e)$ is defined as the ratio of the performance of the algorithm to the Shannon's limit.

All the calculation in the dissertation,it had been assume that the algorithm is bidirectional.The algorithm work within 35% of the Shannon's limit.Values of $f(e)$ for several different error rates, produced by benchmark tests are represented in Table 2.1.

Table 2.1: Benchmark performance of a bidirectional error correction algorithm

e	**f(e)**
0.01	1.06
0.05	1.16
0.1	1.22
0.15	1.35

The final expression for the secure key generation rate is

$$R = R_{shifted}\{\tau + f(e)[e \log_2 e - (1-e)\log_2(1-e)]\} \tag{2.20}$$

where $R_{shifted}$ and τ depends on the QKD protocols and system parameter.

Here $f(e) \geq 1$, the function $f(e)$ can be determined by benchmark testing the algorithm under a broad range of strings.

The quantum key distribution can be of two types depending on the technique applied.
Now for the BB84 protocol, the secure key rate generation can easily be calculated. For BB84, the collision probability for each bit p_{c_0} is given by,

$$p_{c_0} \leq \frac{1}{2} + 2e - 2e^2 \tag{2.21}$$

Thus the average collision probaility for the n bit string is calculated as $p_c = p_{c_0}^n$.Thus the shrinking factor is given by,

$$\tau = -\frac{\log_2 p_c}{n} = -\log_2 p_{c_0} = -\log_2(\frac{1}{2} + 2e - 2e^2) \tag{2.22}$$

The final expression for the secure key generation rate is

$$R = R_{shifted}\{-\log_2(\frac{1}{2} + 2e - 2e^2 + f(e)[e\log_2 e - (1-e)\log_2(1-e)]\} \tag{2.23}$$

Prepare and Measure Protocols

Sender prepares the quantum states he or she wants to transfer according to the classical information and on the other hand receiver measures the received quantum state to obtain the information. It's a two-way channel protocol.

The sender prepares the quantum states and sent them over the quantum chan-

nel. Its one way channel. Information can flow from sender to receiver. The second channel is a classical authenticated channel which they would use for the authentication of the message transmits and received. Information back and forth between the two users. The fact that the channel is authenticated means the two parties are guaranteed to talk to each other and the attacker could do nothing even after getting all the messages. Example BB84,B92,SARG04 (refer Figure 2.6).

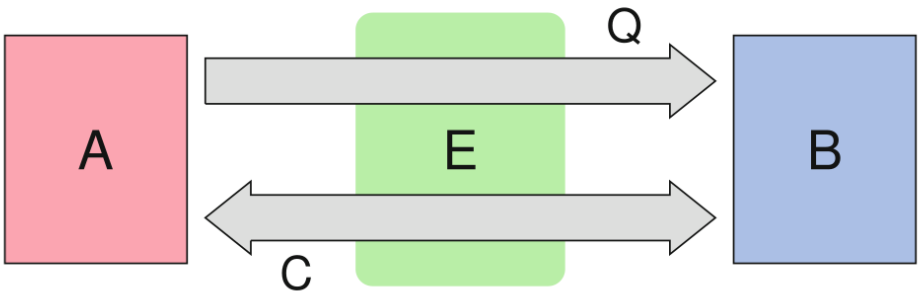

Figure 2.6: Schematic diagram of a typical Prapere and Measure QKD Protocol where transmission of quantum states takes place through Quantum Channel and basis announcement through public classical channel

Entanglement Based Protocols

Sender and receiver depend on some central source or some third party to transmit the entangled pair-a part of which belongs to the sender and the other to the receiver.No restrictions on who can owe the source even if it can be the attacker. The two users measure their part of the entangled pair and keep that measurement where they measure in the same direction. They can also perform CHSH inequality to check the presence of eve. These categories of protocols are perfectly guided by the laws of quantum mechanics. Example: Ekert E91 (refer Figure 2.7).

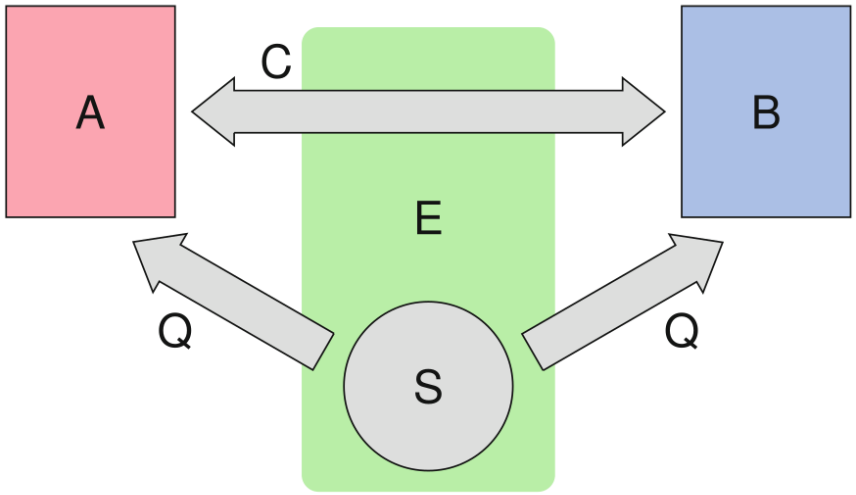

Figure 2.7: Schematic diagram of a typical Entanglement QKD Protocol where a central source distribute entangled pair through Quantum Channel and measurement direction takes place through public classical channel

2.3 Noise Models

Noise is the central obstacle in developing long-distance quantum communication. The noise may arise either due to infidelities in the hardware (i.e., gates, measurement device) or due to unwanted interaction with the environment (i.e., thermal, electromagnetic, and gravitational decoherence) Noisy Quantum channel Quantum communication got highly affected due to the noise in the channel. Three sources of errors concern us: (1) Hardware infidelities in the form of depolarizing Pauli noise (2) state preparation and measurement (SPAM) error and (3) decoherence in the form of thermal relaxation and depahsing.

1. **Depolarizing Channel** The term symmetric depolarizing channel is often in-

terchangeably used with gate infidelities or depolarizing channels. It essentially stimulates the bitflips and phase flip error due to gate infidelities within the hardware as a depolarizing channel. The bit flip and phase flip error is often represented through the Pauli X and Pauli Z operation. the combined effect of bit and phase flip is represented through Pauli Y. The depolarizing channel can be represented by the following operator.

$$\begin{aligned} K_{D_0} &= \sqrt{1-p_1}I, \\ K_{D_1} &= \sqrt{\frac{p_1}{3}}X, \\ K_{D_2} &= \sqrt{\frac{p_1}{3}}Z, \\ K_{D_3} &= \sqrt{\frac{p_1}{3}}Y \end{aligned} \tag{2.24}$$

the effect of the depolarizing channel on a quantum system can be expreseed as

$$\rho \mapsto \mathcal{D}(\rho) = \sum_{i=0}^{3} K_{D_i} \rho K_{D_i}^{\dagger} \tag{2.25}$$

where ρ is the density matrix of the qubit.

2. **State Preparation and Measurement(SPAM) Channel:** This channel is essentially a simple Pauli X error, but it affect the measurement aspect of the computation. Thus one can represent SPAM quantum channel for the measurement error by following Kraus Operator

$$\begin{aligned} K_{M_0} &= \sqrt{1-p_2}I, \\ K_{M_1} &= \sqrt{p_2}X \end{aligned} \tag{2.26}$$

where p_2 is the probability of incorrect measurement. The effect of the SPAM channel for measurement error is given by

$$\rho \mapsto \mathcal{S}(\rho) = K_{M_0}\rho K_{M_0} + K_{M_1}\rho K_{M_1} \tag{2.27}$$

In the case of the state preparation the error channel is of a similar form as that of the measurement case (i.e., $\rho \mapsto \mathcal{S}'(\rho)$), with the qubit fail to prepare in the desired state, resulting in the inverted state by X with the probability p_2'.

3. **Thermal Decoherence and Dephasing Channel:** There are two aspects of noise within this error group: (i) the thermal decoherence (or relaxation) that occurs over time in the form of excitation/de-excitation and (ii) the dephasing of the qubits over time. Thermal Decoherence is defined as the loss of quantum coherence due to a quantum system's physical interaction with its environment. It can affect the qubits in a variety of ways.[11][6][8] One among which is that the qubits were at state $|0\rangle$ ground state and ends at $|1\rangle$ excited state. It's a form of non-unital (i.e., irreversible) that describes the thermalization of the qubit spins toward equilibrium at the temperature of their environment. There is an exchange of energy between the qubits and the environment. It can either drives to the ground state (de-excitation) or to the excited state (excitation). The time required to relax(moving toward either of the equilibrium state $|0\rangle$ or $|1\rangle$), coincidentally called the energy relaxation time, is denoted as T_1. It can be thought of as the longitudinal loss (oriented along the z axis).

The other aspect of noise that came under this third group is Dephasing, which

explains how coherence behavior decay over time. It is a mechanism that describes the transition of a quantum system toward classical behavior. That's the phase information spread out widely so the phase information is lost. The time of dephasing is denoted as T_2.

There already exists an implementation in Qiskit which takes into account another third parameter referred to as average execution time for each type of quantum gate denoted as T_g.

In other words, T_1 describes an evolution towards equilibrium as a perturbation orthogonal to the quantization axis (x, y component of the Bloch vector) and T_2 describes a slow perturbation along the quantization axis (z component of the Bloch vector), or otherwise, the behavior of the off-diagonal elements over time for each qubit. These two times are related as $T_2 \leq 2T_1$. The probability for a qubit to relax (Thermal Relaxation) (pT_1) and probability for a qubit to dephase (pT_1) is given by,

$$\begin{aligned} pT_1 &= e^{-\frac{T_g}{T_1}}, \\ pT_2 &= e^{-\frac{T_g}{T_2}} \end{aligned} \tag{2.28}$$

Theoretically, thermal relaxation causes a shift of the qubit to either the equilibrium state of $|0\rangle$ or $|1\rangle$ when the temperature of the quantum processor is not 0, but practically excitation is an extremely rare event due to the extremely low temperature of the quantum processor and other associated components and high frequency of the qubits of order $10^9 Hz$. Thus we can effectively assume that the reset the error takes the form of only reset to the ground state. Thus, we can now refer to thermal relaxation simply as relaxation or spontaneous emission. If $T_2 \leq 2T_1$ is held for every qubit in the system then relaxation and dephasing noise can be expressed as a mixed reset and unital quantum chan-

nel. If the temperature of the device is 0 we can have the following form of noise.

- Dephasing: A phase flip occur with probability $p_z = (1 - p_{reset})(1 - pT_2 pT_1{}^{-1})/2$ where $p_{reset} = 1 - pT_1$.
- Identity: Nothing happens to the qubit or the identity I occurs with probability $p_I = 1 - p_z - p_{reset}$.
- Reset to ground state: Thermal decay or jump toward ground state with probability $p_{reset} = 1 - pT_1$. The above cases cn be represented with the folowing operators

$$\begin{aligned} K_I &= \sqrt{p_I} I, \\ K_Z &= \sqrt{p_Z} Z, \\ K_{reset} &= \sqrt{p_{reset}} |0\rangle\langle 0| \end{aligned} \tag{2.29}$$

Thus the effect of relaxation channel when $T_2 \leq 2T_1$ is given by

$$\rho \mapsto \mathcal{N}(\rho) = \sum_{k \in I,Z,reset} K_k \rho K_k^\dagger \tag{2.30}$$

2.4 Motivation

2.4.1 Challenges in large scale Quantum Communication

Quantum Communication System suffers from a major drawback due to the presence of noise in the channel. Large scale reliable Quantum Communication System can never be possible if the central hurdles-Noise had not been eliminated. The main candidates in the quantum communication system - QKD protocols can't be applied

to the real world to be a part of the communication system if noise and error in the channel do not take care of. The powerful feature of the QKD protocols can only be realized in a real sense of the noise and error in the channel being taken care of. It motivated me to conduct my research on the implementation of a popular QKD protocol in the popular three noise channels viz. Depolarizing Channel, State Preparation and Measurement(SPAM) Channel, and Thermal Decoherence and Dephasing Channel to calculate the secure key generation rate in presence of noise.

2.4.2 Comparative Study

The dissertation focus on the three noise channel viz. Depolarizing Channel, State Preparation and Measurement (SPAM) Channel, and Thermal Decoherence and Dephasing Channel to study the comparative effectiveness of these noisy channels and calculate the secure key generation rate for BB84 protocol for the 5% and 10% noise.

Chapter 3

Methodology

The study of the BB84 QKD protocol in a noisy environment had been carried out in two different ways. In the first case, the protocol had been executed with four qubits to study the effect of each type of the noisy channel over every single qubit by calculating the probability of getting each bit. The probability distribution of generated key had been depicted through the "plot_histogram" method under the "qiskit.visualization" package.

In the second case the protocol had been carried out with 2016 qubits to compute the secret key rate. The method used for calculating the secret key rate had been proposed by [5].

The protocol had been executed in three noisy channels viz. Depolarizing Channel, State Preparation and Measurement(SPAM) Error Channel, and finally the Decoherence and Dephasing Channel to examine the effect of each noisy channel over the protocol.

3.1 Proposed approach

The proposed approach is very simple yet effective in computing the secret key rate. Firstly the noise model had been created using Qiskit standard packages. Then it is followed by encoding the message in the desired basis which is chosen at random using the python standard random number generating package. It is followed by adding the noise model in the protocol with desired noise percentage. This dissertation it had been carried out with 5% and 10% noise separately.
The next step had been carried out from two different perspectives, in the first case the message had been measured directly representing the scenario without eavesdropping and in the second case, interception had been presented by adding an extra measurement before the receiver.It is then followed by key shifting and finally appending the generated key to a list.

The same process repeats in a loop 63 times, where each loop executes the protocol for 32 qubits, and thus the protocol executes for a total of 2016 qubits. Each loop appends the shifted key and the process continues 63 times.
The proposed approach had been presented in refer (Figure 3.1).

3.1.1 Algorithm

The generic BB84 protocol which had been proposed by [1] had been presented in algorithmic form.

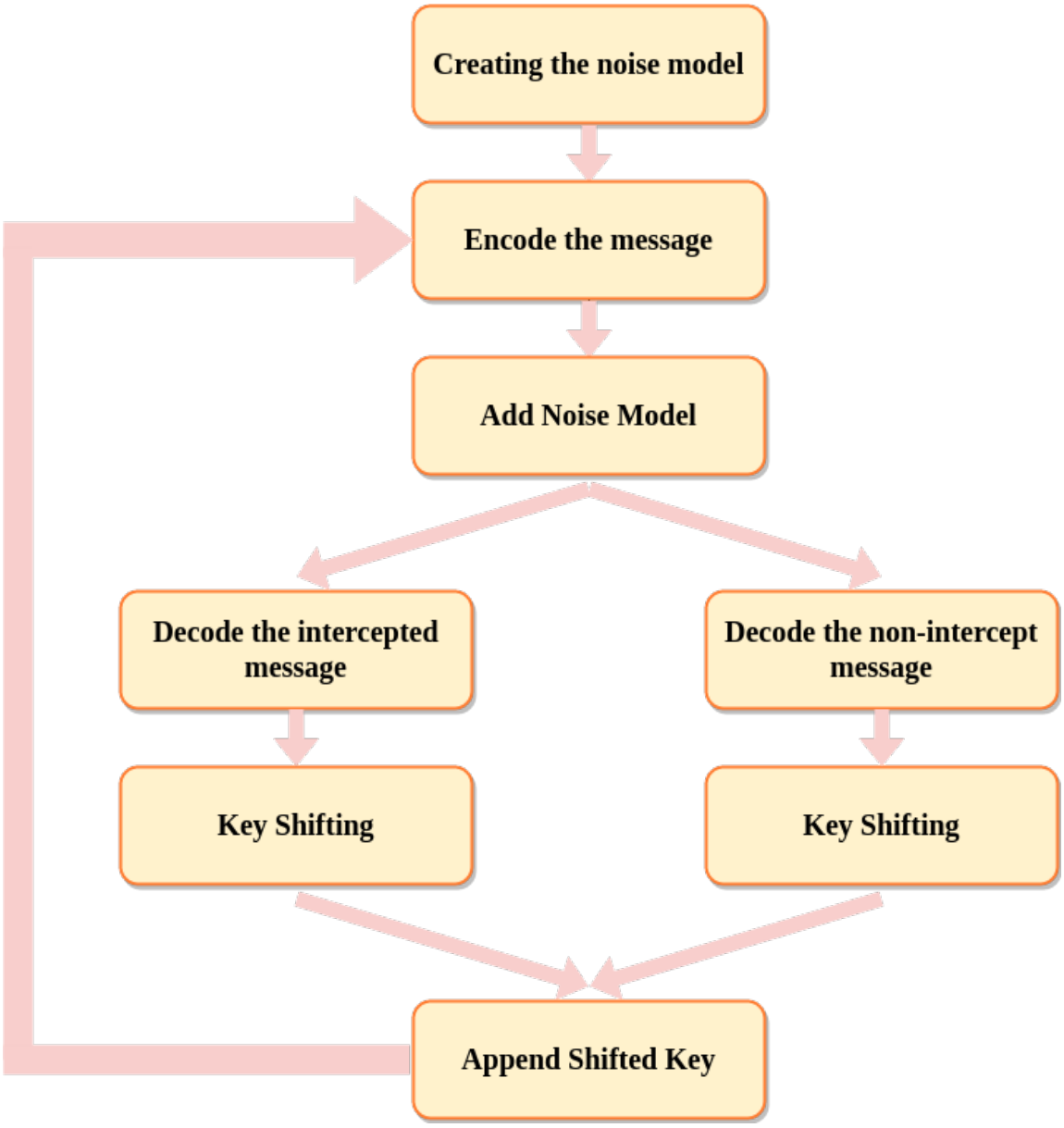

Figure 3.1: Schematic diagram of work flow our the proposed idea.The left part indicate the eavesdropping and right part the ideal case.The process append the shifted key after each cycle and the process continue.

Algorithm 1: BB84

Sender encoding :
$i \leftarrow 0$ **while** $i \neq n$ **do**
  if *sender basis is* $|0\rangle|1\rangle$ **then**
    if *sender's bit is 0* **then**
      create $|0\rangle$ state
    else
      create $|1\rangle$ state
    end
  else
  end
  if *sender basis is* $|+\rangle|-\rangle$ **then**
    if *sender's bit is 0* **then**
      create $|+\rangle$ state
    else
      create $|-\rangle$ state
    end
  else
  end
end
$i \leftarrow i + 1$ **Receiver measurement :**
$i \leftarrow 0$ **while** $i \neq n$ **do**
  if *Receiver basis is* $|0\rangle|1\rangle$ **then**
    Measure in the Z basis
  end
  if *Receiver basis is* $|+\rangle|-\rangle$ **then**
    Measure in the X basis
  end
end
$i \leftarrow i + 1$ **Key Selection:**
while $i \neq n$ **do**
  if *Sender Basis match Receiver basis* **then**
    Keep the corresponding bits from both sender and receiver end
  end
end
$i \leftarrow i + 1$

3.1.2 Stimulation in Noiseless Environment

The study had been carried out in both noiseless and noisy environments. The study in the noiseless environment had been carried out through Qiskit "aer simulator" in the IBM Quantum Experience's cloud notebook platform "IBM Quantum Lab". To build the circuit following three packages had been used "QuantumRegister, ClassicalRegister, and QuantumCircuit". The "QuantumRegister and ClassicalRegister" package had been used to build qubits and classical bits to take the measurement respectively. The "QuantumCircuit" package had been used to combine the state preparation and measurement part. The compilation of the quantum circuit had been done with the Qiskit package, "transpiler". To assemble the quantum circuit representing each qubit in the transmission Qiskit's "assembler" package had been used. Each of the experiments had been repeated with a shot of 1024.
The experiment had been done in two different ways, in the first time the protocol had been run 4 qubits had been built to see the effect of eavesdropping by plotting the data in the histogram and the second time the protocol had been tested with 32 qubits and repeated 63 times, each time appending the result; getting the length of the shifted key near to 900. To visualize the result from the first part of the experiment with 4 qubits Qiskit's "plot_histogram" package had been used. The sample size had been kept at 25% of the shifted key.

3.1.3 Simulation in Noisy Environment

The noise had been deployed with Qiskit Aer Noise Module. The "NoiseModel" class had been used to store a noise model used for noisy simulation. The "QuantumError" class which describes CPTP gate errors had been used to generate the noisy channel.

The protocol had been tested with 5% and 10% noise. "depolarizing_error()" function which comes under Qiskit Aer Noise Module's class "QuantumError" had been used to create a depolarising channel. To create a noisy SPAM channel "pauli_error()" function which comes under Qiskit Aer Noise Module's class "QuantumError" had been used. Now finally for the Thermal Decoherence and Dephasing Channel "thermal_relaxation_error()" function which comes under Qiskit Aer Noise Module's class "QuantumError" had been used. Likewise in a noiseless environment, the experiment had been done in two different ways, the first time the protocol had been run 4 qubits had been built to see the effect of eavesdropping by plotting the data in the histogram and the second time the protocol had been tested with 32 qubits and repeated 63 times, each time appending the result; getting the length of the shifted key near to 900. To visualize the result from the first part of the experiment with 4 qubits Qiskit's "plot_histogram" package had been used. Each of the experiments had been repeated with a shot of 1024. The sample size had been kept at 25% of the shifted key.

Chapter 4

Result

The result of execution of BB84 QKD protocol in both noiseless and noisy environment had been presented in section 4.1 and 4.2 respectively.In both cases it had been executed with four qubits and 2016 qubits separately.The prior had been done to examine the effect of noise over each qubit and the later had been done to compute the secure key rate in presence of noise or eaves dropping or both.

4.1 Execution in Noiseless Environment

4.1.1 Execution with Four Qubits

Experiment had been carried out with four qubits to examine the effect of eavesdropping in a noiseless environment.

BB84 without eavesdropping

Result of Chosen basis:

```
Sender chooses to sent the following string of bits
[1 0 0 1]
Sender choose the following basis where 1 denotes Z basis
and 0 denotes X basis
[1 0 0 1]
Receiver choose following basis where 1 denotes Z basis and 0
denotes X basis
[0 0 1 1]
```

The result had been presented in (refer Table 4.10) and the probability distribution had been presented in (refer Figure 4.1).

Table 4.1: Experimental result of the BB84 in noiseless environment without the presence of eve

q[0]	**q[1]**	**q[2]**	**q[4]**
0(51.2%),1(48.7%)	0(100%),1(0%)	0(52.2%),1(47.7%)	0(0%),1(100%)

BB84 with eavesdropping

Result of Chosen basis:

```
Sender chooses to sent the following string of bits
[0 1 1 0].
Sender choose the following basis where 1 denotes Z basis
and 0 denotes X basis
[0 1 0 1].
```

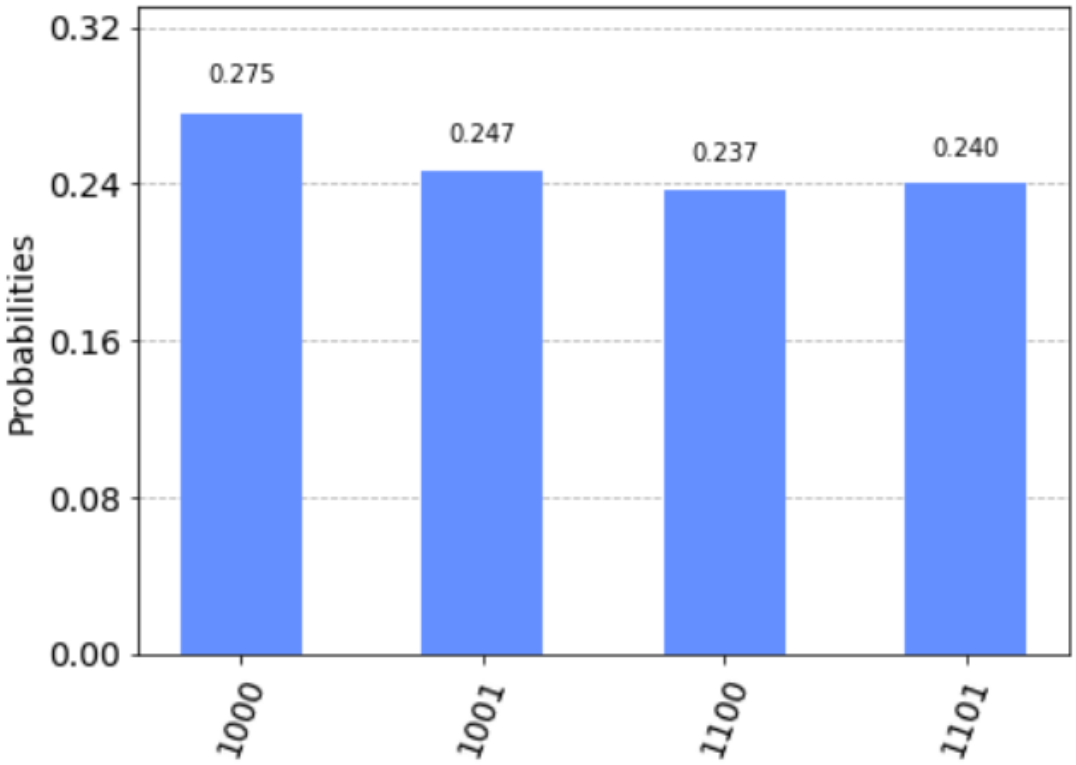

Figure 4.1: Probability Distribution for experimental result of BB84 without eavesdropping

Now the attacker choose the following basis where 1 denotes Z basis and 0 denotes X basis

[1 1 1 1].

Receiver choose following basis where 1 denotes Z basis and 0 denotes X basis

[0 1 0 1].

The result had been presented in (refer Table 4.2) and the probability distribution

had been presented in (refer Figure 4.2).

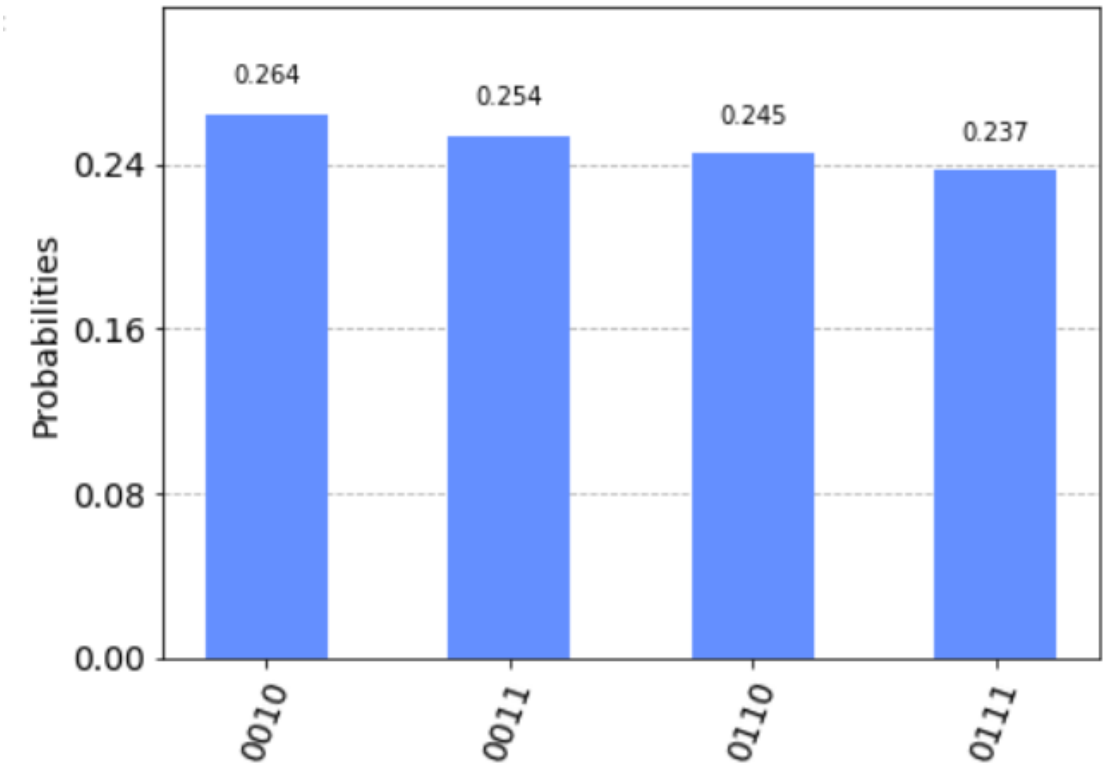

Figure 4.2: Probability Distribution for experimental result of BB84 with eavesdropping

4.1.2 Execution with 2016 Qubits

BB84 without eavesdropping

```
The length of the shifted key is:
997
 sample ....  250
```

Table 4.2: Experimental result of the BB84 in noiseless environment with the presence of eve

q[0]	**q[1]**	**q[2]**	**q[4]**
0(50.9%),1(49.1%)	0(0%),1(100%)	0(51.8%),1(48.2%)	0(100%),1(0%)

```
length of sifted key is  997
length of sample taken is  190
Length of the sender sample is
190
Length of the receiver sample is
190
Cryptographic_key_is length is
807
```

This is the ideal case which doesn't happen there is no error and consequently secret key rate is undefined. **BB84 with eavesdropping**

```
The length of the shifted key is:
1000
 sample ....  250
length of sifted key is  1000
length of sample taken is  235
Length of the sender sample is
235
Length of the receiver sample is
235
Error
```

```
Error_rate= 0.40425531914893614
```

Since error e is greater than 11% we would discard it.

4.2 Execution in Noisy Environment

4.2.1 Execution with Four Qubits

Experiment had been carried out with four qubits to examine the effect of eavesdropping in a noisy environment. Primarily three category of noisy channel had been considered viz. Depolarizing Channel, State Preparation and Measurement Error Channel and Thermal Decoherence and Dephasing Error Channel.

Depolarizing Channel:

Depolarization without eavesdropping:

Result of the Chosen basis:

```
Sender chososes to sent the following string of bits
[1 0 1 1]
Sender choose the followwing basis where 1
denotes Z basis and 0 denotes X basis
[0 1 1 0]
Reciever choose folowing basis where 1 denotes
Z basis and 0 denotes X basis
[1 0 1 0]
```

The result had been presented in (refer Table 4.3) and the probability distribution had been presented in (refer Figure 4.3) with 5% noise.

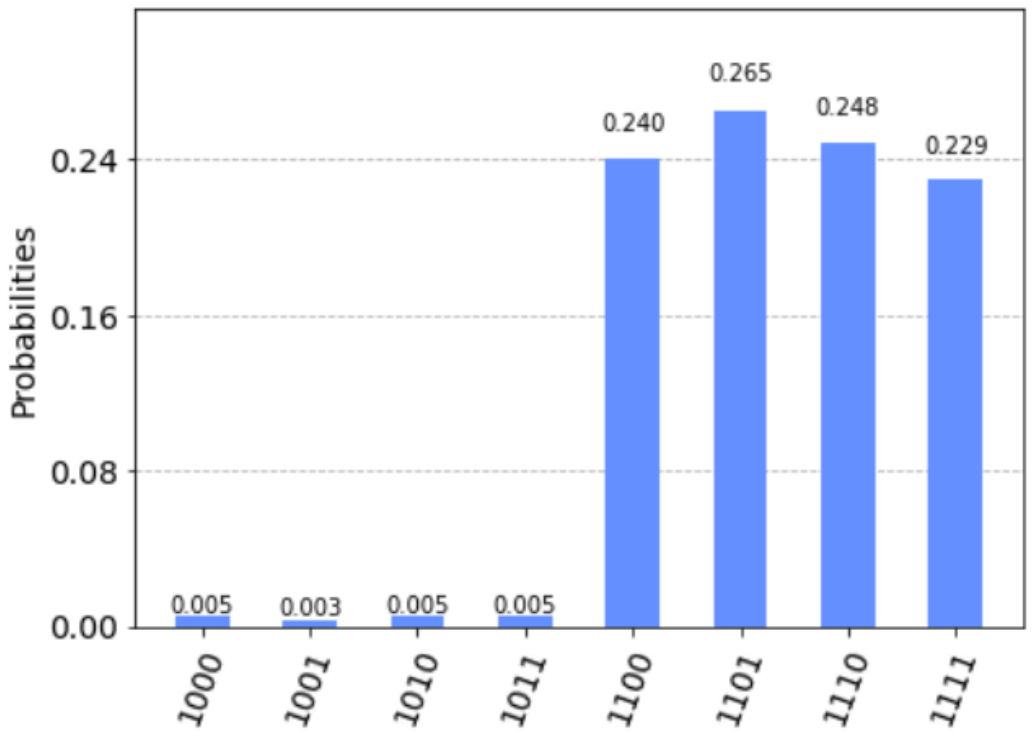

Figure 4.3: Probability Distribution for experimental result of BB84 in Depolarizing without eavesdropping

Depolarization with eavesdropping:

Result of Chosen basis:

```
Sender chososes to sent the following string of bits
[1 0 1 0]
Sender choose the followwing basis where 1 denotes Z
basis and 0 denotes X basis
```

Table 4.3: Experimental result of the BB84 in depolarizing environment with 5% noise without the presence of eve

q[0]	**q[1]**	**q[2]**	**q[4]**
0(49.8%),1(50.2%)	0(51.3%),1(49.1%)	0(1.8%),1(98.2%)	0(0%),1(100%)

```
[1 1 1 0]
Now the attacker choose the foloowing basis where 1
denotes Z basis and 0 denotes X basis
[1 0 0 1]
Reciever choose folowing basis where 1 denotes Z
basis and 0 denotes X basis
[1 1 0 0]
```

The result had been presented in (refer Table 4.4) and the probability distribution had been presented in (refer Figure 4.4).

Table 4.4: Experimental result of the BB84 in depolarizing environment at 5% noise with the presence of eve

q[0]	**q[1]**	**q[2]**	**q[4]**
0(2.3%),1(97.7%)	0(50.4%),1(49.6%)	0(48%),1(52%)	0(51.1%),1(48.9%)

State Preparation and Measurement(SPAM) Channel:

SPAM without eavesdropping

Result of the Chosen basis:

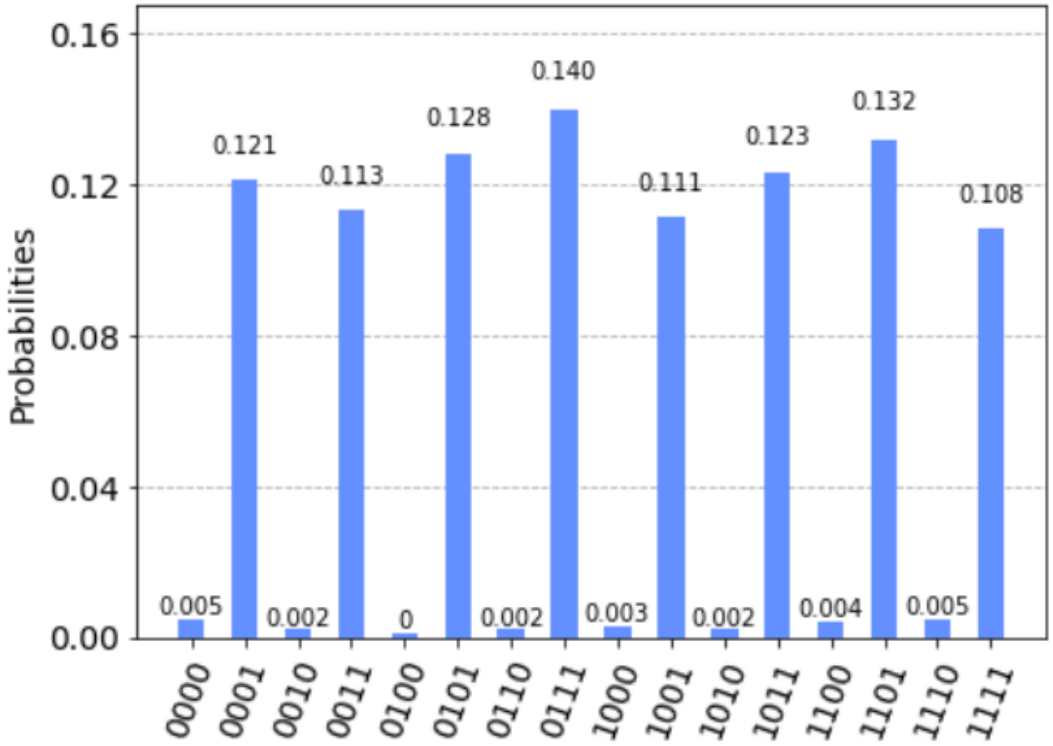

Figure 4.4: Probability Distribution for experimental result of BB84 in Depolarizing with eavesdropping

```
Sender chososes to sent the following string of bits
[0 0 1 1]
Sender choose the following basis where 1 denotes
Z basis and 0 denotes X basis
[0 1 1 1]
Receiver choose following basis where 1 denotes Z basis
and 0 denotes X basis
[0 1 0 1]
```

The result had been presented in (refer Table 4.5) and the probability distribution had been presented in (refer Figure 4.5) with 5% noise.

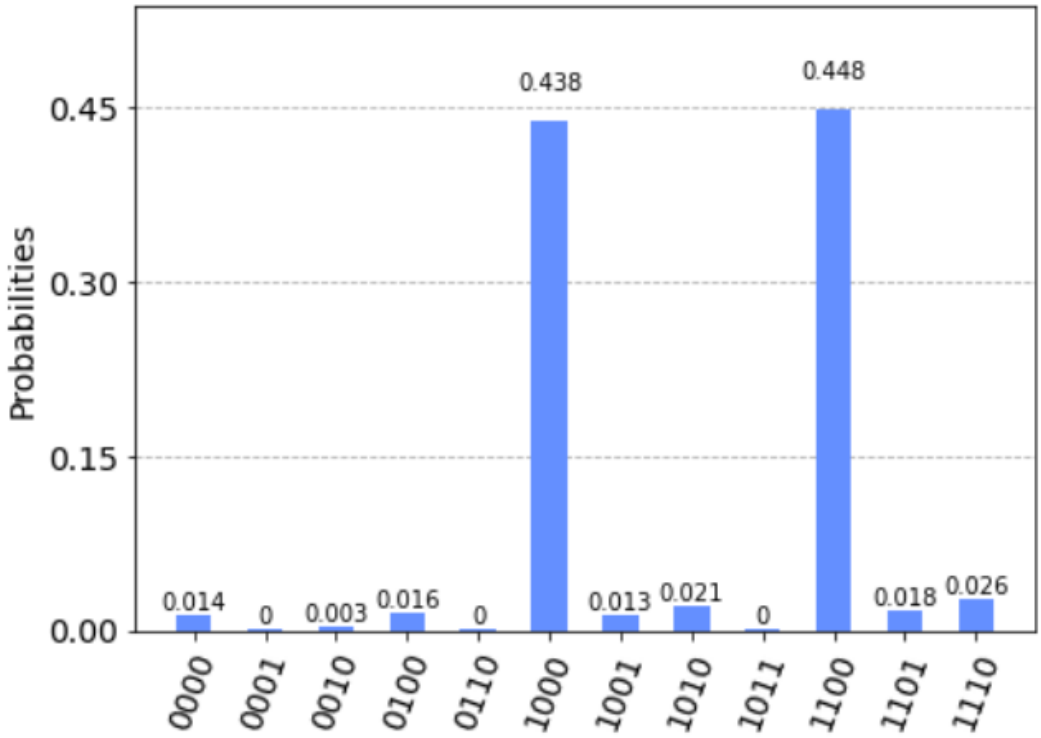

Figure 4.5: Probability Distribution for experimental result of BB84 in SPAM Channel without eavesdropping

SPAM with eavesdropping

Result of the Chosen basis:

```
Sender chososes to sent the following string of bits
[1 0 1 0]
Sender choose the followwing basis where 1 denotes Z basis
and 0 denotes X basis
```

Table 4.5: Experimental result of the BB84 in SPAM Error environment with 5% noise without the presence of eve

q[0]	**q[1]**	**q[2]**	**q[4]**
0(96.6%),1(3.4%)	0(94.7%),1(5.3%)	0(48.9%),1(51.1%)	0(3.3%),1(96.7%)

[0 0 0 1]

Now the attacker choose the foloowing basis where 1 denotes Z basis and 0 denotes X basis

[1 0 1 1]

Reciever choose folowing basis where 1 denotes Z basis and 0 denotes X basis

[0 1 0 0]

The result had been presented in (refer Table 4.6) and the probability distribution had been presented in (refer Figure 4.6).

Table 4.6: Experimental result of the BB84 in SPAM Error environment with 5% noise with the presence of eve

q[0]	**q[1]**	**q[2]**	**q[4]**
0(50.4%),1(49.6%)	0(90.2%),1(9.8%)	0(50.9%),1(49.1%)	0(49.8%),1(50.2%)

Thermal Decoherence and Dephasing Channel:

Thermal Decoherence and Dephasing without eavesdropping

Result of Chosen basis:

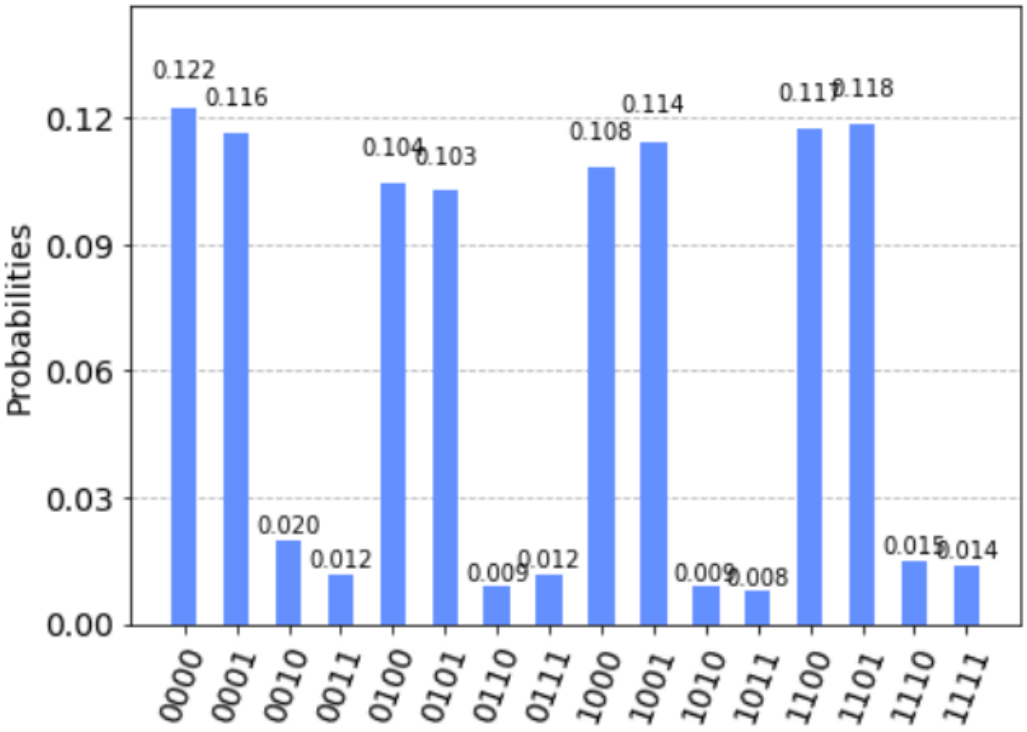

Figure 4.6: Probability Distribution for experimental result of BB84 in SPAM Channel with eavesdropping

```
Sender chososes to sent the following string of bits
[0 0 0 1]
Sender choose the followwing basis where 1 denotes
Z basis and 0 denotes X basis
[0 1 1 1]
Reciever choose folowing basis where 1 denotes Z basis
and 0 denotes X basis
[1 0 0 0]
```

The result had been presented in (refer Table 4.7) and the probability distribution

had been presented in (refer Figure 4.7) with $T_1 = 0.0125$ and $T_2 = 0.0025$.

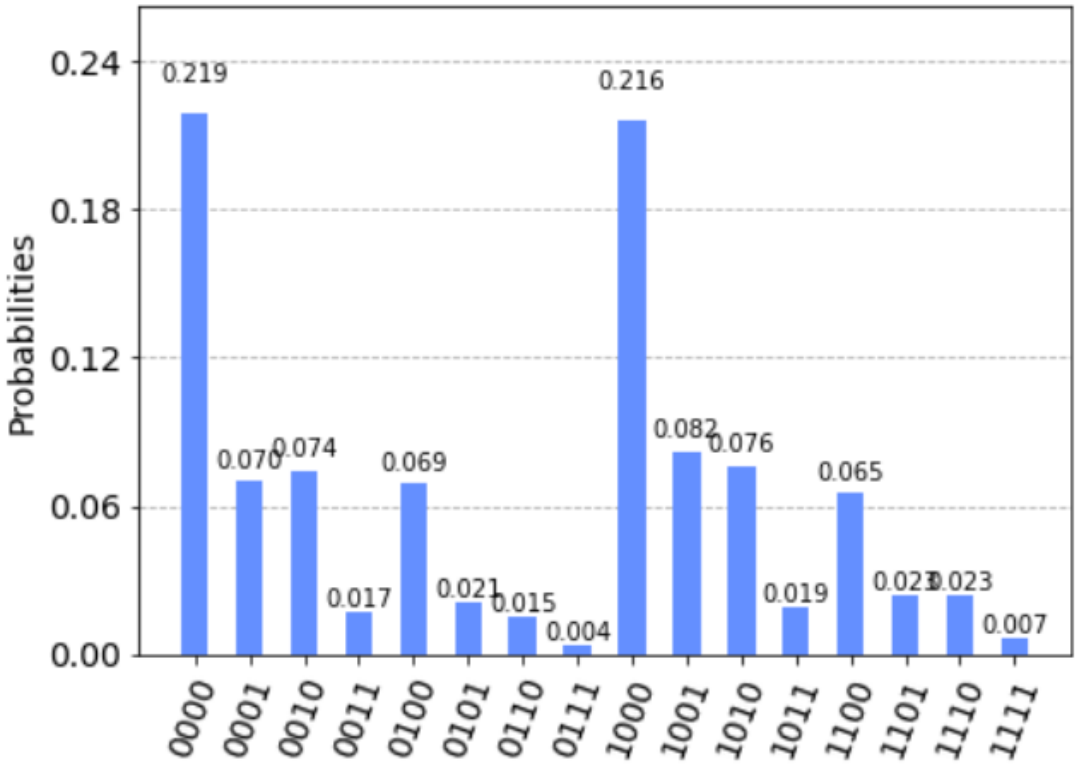

Figure 4.7: Probability Distribution for experimental result of BB84 in Thermal Decoherence and Dephasing without eavesdropping at $T_1 = 0.0125$ and $T_2 = 0.0025$

Thermal Decoherence and Dephasing with eavesdropping Result of Chosen basis:

```
Sender chososes to sent the following string of bits
[1 0 1 1]
Sender choose the followwing basis where 1 denotes
Z basis and 0 denotes X basis
```

Table 4.7: Experimental result of the BB84 in Thermal Decoherence and Dephasing without the presence of eve

q[0]	**q[1]**	**q[2]**	**q[4]**
0(75.7%),1(24.3%)	0(76.5%),1(23.5%)	0(77.3%),1(22.7%)	0(48.9%),1(51.1%)

```
[1 1 0 1]
Now the attacker choose the foloowing basis where 1 denotes
Z basis and 0 denotes X basis
[1 1 1 1]
Reciever choose folowing basis where 1 denotes Z
basis and 0 denotes X basis
[1 0 1 0]
```

The result had been presented in (refer Table 4.8) and the probability distribution had been presented in (refer Figure 4.8).

Table 4.8: Experimental result of the BB84 in depolarizing environment with the presence of eve at $T_1 = 0.0125 and T_2 = 0.0025$

q[0]	**q[1]**	**q[2]**	**q[4]**
0(57.1%),1(42.9%)	0(77.6%),1(22.4%)	0(50.6%),1(49.4%)	0(76.7%),1(23.3%)

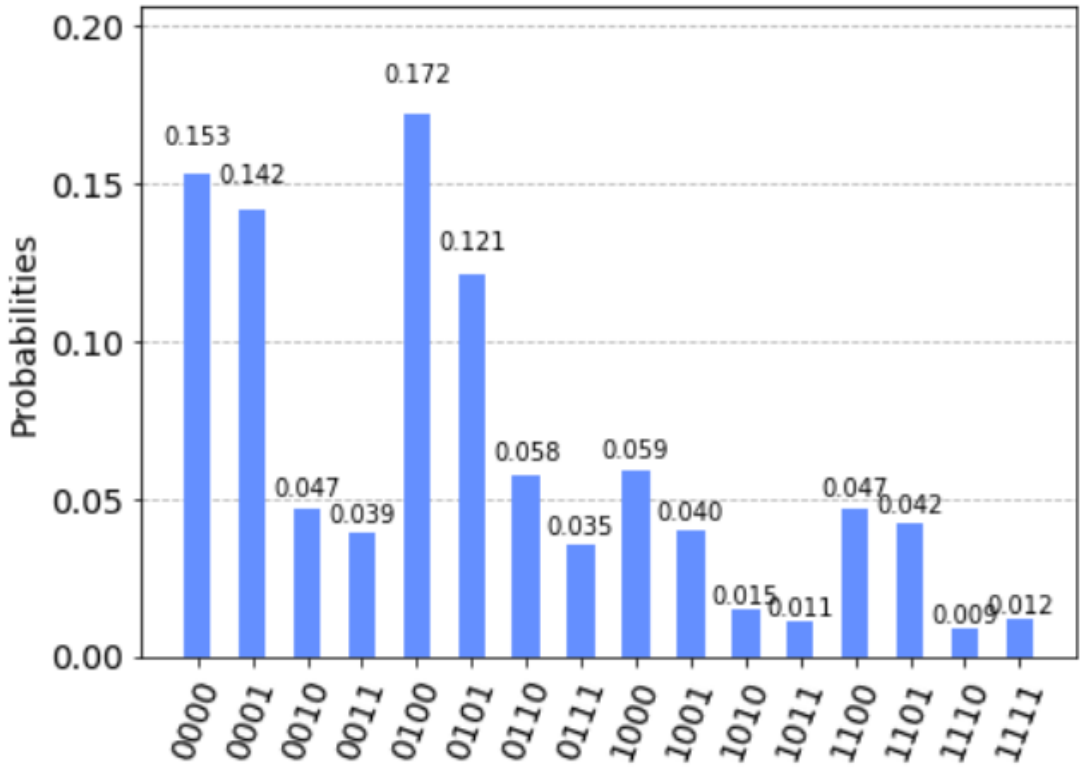

Figure 4.8: Probability Distribution for experimental result of BB84 in Thermal Decoherence and Dephasing with eavesdropping

4.2.2 Execution with 2016 Qubits

Depolarizing Channel:

BB84 Protocol had been executed with 2016 qubits in Depolarizing Error Channel environment with 5% noise to calculate the secure key rate generation.

Execution of BB84 QKD protocol with 2016 qubits in Depolarizing Channel without eavesdropping

The length of the shifted key is:

```
1010
 sample ....  253
length of sifted key is  1010
length of sample taken is  80
Length of the sender sample is
80
Length of the receiver sample is
80
Error
Error_rate= 0.075
```

Secret Key Rate=179.59479125280467

Execution of BB84 QKD protocol with 2016 qubits in Depolarizing Channel with eavesdropping

```
The length of the shifted key is:
1039
 sample ....  260
length of sifted key is  1039
length of sample taken is  246
Length of the sender sample is
246
Length of the receiver sample is
246
Error
Error_rate= 0.3252032520325203
```

Since the error rate is more than 11% we would reject it.

BB84 Protocol had been executed with 2016 qubits in depolarizing environment with 10% noise to calculate the secure key rate generation.

Execution of BB84 QKD protocol with 2016 qubits in Depolarizing Channel without eavesdropping:

```
The length of the shifted key is:
1018
 sample ....  255
length of sifted key is  1018
length of sample taken is  154
Length of the sender sample is
154
Length of the receiver sample is
154
Error
Error_rate= 0.06493506493506493
```

Secret Key Rate = 289.2254458175412

Execution of BB84 QKD protocol with 2016 qubits in Depolarizing Channel with eavesdropping:

```
The length of the shifted key is:
1041
 sample ....  261
```

```
length of sifted key is  1041
length of sample taken is  250
Length of the sender sample is
250
Length of the receiver sample is
250
Error
Error_rate= 0.392
```

Since the error rate is more than 11% we would reject it.

State Preparation and Measurement (SPAM) Channel:

BB84 Protocol had been executed with 2016 qubits in SPAM Error environment with 5% noise to calculate the secure key rate generation.

Execution of BB84 QKD protocol with 2016 qubits in SPAM Error Channel without eavesdropping:

```
The length of the shifted key is:
1029
 sample ....  258
length of sifted key is  1029
length of sample taken is  89
Length of the sender sample is
89
Length of the receiver sample is
```

```
89
Error
Error_rate= 0.033707865168539325
```

Secret Key Rate=593.349562424053

Execution of BB84 QKD protocol with 2016 qubits in SPAM Error with eavesdropping:

```
The length of the shifted key is:
1033
 sample ....  259
length of sifted key is  1033
length of sample taken is  216
Length of the sender sample is
216
Length of the receiver sample is
216
Error
Error_rate= 0.4212962962962963
```

Since the error rate is more than 11% we would reject it.

BB84 Protocol had been executed with 2016 qubits in depolarizing environment with 10% noise to calculate the secure key rate generation.

Execution of BB84 QKD protocol with 2016 qubits in Depolarizing Channel without eavesdropping:

```
The length of the shifted key is:
1007
```

```
 sample ....  252
length of sifted key is  1007
length of sample taken is  55
Length of the sender sample is
55
Length of the receiver sample is
55
Error
Error_rate= 0.03636363636363636
```

Secret Key rate = 553.1805385460923

Execution of BB84 QKD protocol with 2016 qubits in Depolarizing Channel with eavesdropping:

```
The length of the shifted key is:
1025
 sample ....  257
length of sifted key is  1025
length of sample taken is  85
Length of the sender sample is
85
Length of the receiver sample is
85
Error
Error_rate= 0.3176470588235294
```

Since the error rate is more than 11% we would reject it.

Thermal Decoherence and Dephasing Channel:

Thermal Decoherence and Dephasing Channel Noise with T_1 = 0.0125 and T_2 = 0.0025

BB84 Protocol had been executed with 2016 qubits in Thermal Decoherence and Dephasing Channel with 5% noise to calculate the secure key rate generation.

Execution of BB84 QKD protocol with 2016 qubits in Thermal Decoherence and Dephasing Channel without eaves dropping:

```
The length of the shifted key is:
1025
 sample ....  257
length of sifted key is  1025
length of sample taken is  154
Length of the sender sample is
154
Length of the receiver sample is
154
Error
Error_rate= 0.474025974025974
```

Since the error rate is more than 11% we would reject it.

Execution of BB84 QKD protocol with 2016 qubits in Depolarizing Channel with eavesdropping:

```
The length of the shifted key is:
981
 sample ....  246
```

```
length of sifted key is  981
length of sample taken is  113
Length of the sender sample is
113
Length of the receiver sample is
113
Error
Error_rate= 0.3805309734513274
```

Since the error rate is more than 11% we would reject it.

To Summarise we can wind up the result in the following tables

Table 4.9: Error rates and Secure Key Generation Rate(if Error $\leq$ 11) for 5% noise and $T_1 = 0.0125$ and $T_2 = 0.0025$

Noise	**Ideal**	**Eavesdropping**
Depolarizing Noise	e = 0.075,Secret Key Rate = 179.594	e=0.3252,Discarded
SPAM	e = 0.033,Secret Key Rate = 593.349	e=0.421,Discarded
Decoherence and Dephasing	e = 0.474;Discarded	e=0.380,Discarded

Table 4.10: Error rates and Secure Key Generation Rate(if Error $\leq$ 11) for 10% noise and $T_1 = 0.0125$ and $T_2 = 0.0025$

Noise	**Ideal**	**Eavesdropping**
Depolarizing Noise	e = 0.064,Secret Key Rate = 289.225	e=0.392,Discarded
SPAM	e = 0.036,Secret Key Rate = 553.180	e=0.317,Discarded
Decoherence and Dephasing	e = 0.474;Discarded	e=0.380,Discarded

Chapter 5

Discussion and Conclusion

5.1 Execution in Noiseless Environment

5.1.1 Execution with Four Qubits

The experimental result matches the theoretical prediction with little marginal error due to imperfection in simulation. For example, the probability of getting 0 or 1 is not exactly 50% for the first and third qubits where the basis does not match.
In the case of eavesdropping, the sender and receiver had chosen the same basis for the first qubit but due to eavesdropping, the probability got split. Same for the third qubit.

5.1.2 Execution with 2016 Two Qubits

There is no error in ideal i.e., without eavesdropping. A successful cryptographic key of length 807 had been created. In the eavesdropping case error had been detected of value 0.40, which is pretty high thus the presence of eve had been detected.
The experimental results tally with theoretical assumptions.

5.2 Execution in Noisy Environment

5.2.1 Execution with Four Qubits

Depolarizing Channel:

In the ideal i.e., without eve dropping, the basis for measurement of third qubit match but due to the error of 5% the probability of getting 1 had been fallen to 98.2%. The reduced probability is negligible thus it may be concluded that depolarization had not affected our system.
In the eavesdropping case, except for the third qubit, all the qubit had been measured on the same basis but due to the presence of eve probability split into half for the second and fourth qubit thus the attacker had been noticed. Noise does not help the attacker in any way.

State Preparation and Measurement (SPAM) Channel:

In the ideal i.e. without eve dropping, the basis for measurement of first, second and fourth qubit match but due to the error of 5% the probability of getting correct message had been fallen to 96.6%,94.7% and 96.7% respectively. The reduced probability is negligible thus it may be concluded that depolarization had not affected our system.
In the eavesdropping case, the basis for measurement of the second and fourth qubit does not match but for the second qubit, the probability of getting 0 is higher than 1. Thus eve measured the second qubit and got 0. Since the basis is not the same sender and receiver would drop that position. Noise does not help the attacker in any way.

Thermal Decoherence and Dephasing Channel:

In an ideal case basis does not match yet for the first, second, and third qubit receiver got high probability for the correct message thus it may be concluded that Decoherence and Dephasing increase the probability of getting correct result despite the wrong basis. On the other hand in the case of eavesdropping Decoherence and Dephasing is helping the users to get a trace of the attacker by splitting the probability for the first qubit where every three including the attacker choose the same basis.

5.2.2 Execution with 2016 Qubits

The increase in the noise for a depolarizing channel the secure key rate generation got increase. For a increase in noise of 5% the secure key rate got increase by 109.631 part while for SPAM error channel the key rate generation got decreased by 40.169 part.The eavesdropping got easily detected by an incrase in error rate and decohernce and depahsing had an devastating effect on generating a long key.The error rate for $T_1 = 0.0125$ and $T_2 = 0.0025$ is nearabout 50%.

Chapter 6

Challenges and Future Direction

6.0.1 Challenges

The main challenges that had been faced include the unavailability of reliable articles that describe the mathematics of the noise model. Apart from the unavailability of reference articles, the work had not been extended much far as it had been expected due to the limitation of time and funds. The unavailability of the IBMQ server and a limited number of qubits on the risk remains a big obstacle. The simulators and IBMQ platform does not well mimic the real-life scenario of the Quantum Communication System and thus the accuracy may not tally exactly with the real-life cases.Yet the results may give some insight.

6.0.2 Future Direction

In the future, the work may be extended over a much wide range covering a much wider range of protocols and noise models. In the future, we may expect to have access to real time Quantum Processor with a large number of qubits to study the effect on a much more practical ground with a higher rate of accuracy.

Bibliography

[1] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[2] Sawan Bhattacharyya and Amlan Chakrabarti. Post-quantum cryptography. In Neha Sharma, Amlan Chakrabarti, Valentina Emilia Balas, and Alfred M. Bruckstein, editors, *Data Management, Analytics and Innovation*, pages 375–405, Singapore, 2022. Springer Singapore.

[3] Claude Crépeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2445–2454, 1994.

[4] Marcos Curty and David J. Santos. Quantum authentication of classical messages. *Phys. Rev. A*, 64:062309, Nov 2001.

[5] Eleni Diamanti. *Security and implementation of differential phase shift quantum key distribution systems*. PhD thesis, Stanford University, California, January 2006.

[6] Konstantinos Georgopoulos, Clive Emary, and Paolo Zuliani. Modeling and simulating the noisy behavior of near-term quantum computers. *PRA*, 104(6):062432, December 2021.

[7] Nicolas Gisin and Rob Thew. Quantum communication. *Nature Photonics*, 1(3):165–171, mar 2007.

[8] Sayantan Gupta, Kartik Sau, Jyotirmoy Pramanick, Swarnava Pyne, Rizwan Ahamed, and Rahul Biswas. Quantum computation of perfect time-eavesdropping in position-based quantum cryptography: Quantum computing and eavesdropping over perfect key distribution. In *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, pages 162–167, 2017.

[9] P.L. Knight. Quantum communication and quantum computing. In *Technical Digest. Summaries of Papers Presented at the Quantum Electronics and Laser Science Conference*, pages 32–, 1999.

[10] Ali Shaib, Mohamad H. Naim, Mohammed E. Fouda, Rouwaida Kanj, and Fadi Kurdahi. Efficient noise mitigation technique for quantum computing, 2021.

[11] Amoldeep Singh, Kapal Dev, Harun Siljak, Hem Dutt Joshi, and Maurizio Magarini. Quantum internet- applications, functionalities, enabling technologies, challenges, and research directions, 2021.

[12] Ramona Wolf. *Quantum Key Distribution, An Introduction with Exercises*. 2021.

[13] Tianqi Zhou, Jian Shen, Xiong Li, Chen Wang, and Jun Shen. Quantum cryptography for the future internet and the security analysis. *Security and Communication Networks*, 2018:1–7, 02 2018.

Appendix A

Appendix

A.1 Python code for enhanced key

A.1.1 Inclusion of packages and modules

```
import qiskit
import numpy as np
import math
import random
from qiskit import providers,execute,QuantumRegister,
ClassicalRegister,QuantumCircuit,transpile,
Aer,assemble,IBMQ
from qiskit.tools import job_monitor
from qiskit.providers.aer import AerSimulator
from qiskit.visualization import plot_histogram
```

```
from numpy.random import randint,random_integers
from qiskit.providers.aer.noise import NoiseModel
from qiskit.providers.aer.noise import NoiseModel
from qiskit.providers.aer.noise import QuantumError
from qiskit.providers.aer.noise import pauli_error
from qiskit.providers.aer.noise import
thermal_relaxation_error
aer_sim = Aer.get_backend('aer_simulator')
```

A.1.2 Definition of noise model

```
def get_noise(p_bit,p_phase,p_gate1):
    bit_flip = pauli_error([('X',p_bit), ('I', 1 - p_bit)])
    phase_flip = pauli_error([('Z', p_phase), ('I', 1 - p_phase)])
    error_gate1 = depolarizing_error(p_gate1, 1)
    t_error = thermal_relaxation_error(0.0125, 0.0025, 0.01)

    noise_model = NoiseModel()
    # Measurement error had been applied
    noise_model.add_all_qubit_quantum_error(bit_flip, "measure")
    # Depolarizing channel had been applied
    noise_model.add_all_qubit_quantum_error(error_gate1, ["x","h"])
    # Thermal relaxation error had been applied
    noise_model.add_all_qubit_quantum_error(t_error,["x","h"])
    return noise_model
```

A.1.3 Functions for Encoding and Decoding

```
def encode_message(bits,bases):
    message=[]
    for i in range(n):
        qc=QuantumCircuit(1,1)
        if(bases[i]==1):#z basis
            if(bits[i]==0):
                pass#creating |0> state
            else:
                qc.x(0)#creating |1> state
        else:#x basis
            if(bits[i]==0):
                qc.h(0)#creating |+> state
            else:
                qc.x(0)
                qc.h(0)#creating |-> state
        message.append(qc)
    return message

def measure_message(message,bases):
    measured=[]
    for j in range(n):
        if(bases[j]==1):# z bases
            message[j].measure(0,0)
        else:# x bases
```

```
            message[j].h(0)
            message[j].measure(0,0)
        simul=Aer.get_backend('aer_simulator')
        qobj=assemble(message[j],shots=8192,memory=True)
        result=simul.run(qobj,noise_model=noise_model).result()
        measurement=int(result.get_memory()[0])
        measured.append(measurement)
    return measured

def key_selection(s_bases,r_bases,bits):
    good_bits=[]
    for i in range(n):
        if(s_bases[i]==r_bases[i]):
            good_bits.append(bits[i])
    return good_bits

def sampling(bits,string):
    sample=[]
    for i in string:
        i=np.mod(i,len(bits))# sample string doesnot exceed the key
        sample.append(bits.pop(i))
    return sample

'''
Function to calcuate the enhanced key in absence of eve
```

```
'''
def enhanced_key():
    enhanced_key=[]
    enhanced_key_r=[]
    for i in range(63):
        sender_bits=np.random.randint(2,size=n)
        sender_basis=randint(2,size=n)
        reciever_basis=randint(2,size=n)
        data=encode_message(sender_bits,sender_basis)
        key=measure_message(data,reciever_basis)
        s_key=key_selection(sender_basis,reciever_basis,sender_bits)
        for j in range(len(s_key)):
            enhanced_key.append(s_key[j])
        r_key=key_selection(sender_basis,reciever_basis,key)
        for j in range(len(r_key)):
            enhanced_key_r.append(r_key[j])

    return enhanced_key,enhanced_key_r
'''
Function to calcuate the enhanced key in presence of eve
'''
def enhanced_key_eve():
    enhanced_key=[]
    enhanced_key_r=[]
    for i in range(63):
```

```
        sender_bits=np.random.randint(2,size=n)
        sender_basis=randint(2,size=n)
        attacker_basis=randint(2,size=n)
        reciever_basis=randint(2,size=n)
        data=encode_message(sender_bits,sender_basis)
        intercepted_message = measure_message(data,attacker_basis)
        key=measure_message(data,reciever_basis)
        s_key=key_selection(sender_basis,reciever_basis,sender_bits)
        for j in range(len(s_key)):
            enhanced_key.append(s_key[j])
        r_key=key_selection(sender_basis,reciever_basis,key)
        for j in range(len(r_key)):
            enhanced_key_r.append(r_key[j])

    return enhanced_key,enhanced_key_r
```

A.1.4 Driver Code,without eve

```
#Without Eve
from qiskit.circuit import quantumcircuit
n=32
noise_model = get_noise(0.1,0.1,0.1)#Omit the line to get noisless
enviorment
s_key,r_key=enhanced_key()
print("The length of the shifted key is:")
```

```
print(len(s_key))

'''
Keeping the sample size 25% of the shifted key length
'''
s=math.ceil(len(s_key) * 0.25)
print(" sample .... ", s)
sample_size=randint(0,s)
'''
Sampling is doen with 25% of shifted key length
'''
print("length of sifted key is ",len(s_key) )
print("length of sample taken is ",sample_size)
sample_string = randint(n, size=sample_size)
sender_sample=sampling(s_key,sample_string)
reciever_sample=sampling(r_key,sample_string)
'''
Code to calcuate the error rate e
'''
mismatch = 0
for i in range(sample_size):
    if(sender_sample[i]!=reciever_sample[i]):
        mismatch = mismatch+1
print("Length of the sender sample is")
print(len(sender_sample))
```

```
print("Length of the receiver sample is")
print(len(reciever_sample))


if sender_sample==reciever_sample:
    print("Cryptographic_key_is length is")
    print(len(s_key))
else:
    print("Error")
    error_rate=mismatch/sample_size
    print("Error_rate=",error_rate)
```

A.1.5 Driver Code,in presence of eve

```
#In presence of Eve
from qiskit.circuit import quantumcircuit
#np.random.seed(seed=0)
n=32
noise_model = get_noise(0.1,0.1,0.1,0.1)
s_key,r_key=enhanced_key_eve()
print("The length of the shifted key is:")
print(len(s_key))


s=math.ceil(len(s_key) * 0.25)
```

```
print(" sample .... ", s)
sample_size=randint(0,s)

print("length of sifted key is ",len(s_key) )
print("length of sample taken is ",sample_size)
sample_string = randint(n, size=sample_size)
sender_sample=sampling(s_key,sample_string)
reciever_sample=sampling(r_key,sample_string)

mismatch = 0
for i in range(sample_size):
    if(sender_sample[i]!=reciever_sample[i]):
        mismatch = mismatch+1
print("Length of the sender sample is")
print(len(sender_sample))
print("Length of the receiver sample is")
print(len(reciever_sample))



if sender_sample==reciever_sample:
    print("Cryptographic_key_is length is")
    print(len(s_key))
else:
    print("Error")
    error_rate=mismatch/sample_size
```

```
print("Error_rate=",error_rate)
```