

# **ENTANGLED TWO STAGE QKD PROTOCOL**

*A report submitted in partial fulfilment of the requirements for the award of  
the degree of*

**Bachelor of Technology**

**in**

**Electronics and Communication Engineering**

by

KALE VINAY

(ECB20053)



**Department of Electronics and Communication Engineering**

School of Engineering, Tezpur University

Tezpur-784028, Assam, India.

**2023-2024**

### **Declaration by the Students**

We hereby declare that the project work presented in this report entitled “***ENTANGLED TWO STAGE QKD PROTOCOL***”, submitted in partial fulfilment for the award of the degree of Bachelor of Technology in Electronics and Communication Engineering during the academic year 2023-2024, has been carried out by us and that it has not been submitted in part or whole to any institution for the award of any other degree or diploma.

Date:

Place

( KALE VINAY )



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

**TEZPUR UNIVERSITY**

**Tezpur-784028, Assam, India**

**Prof. P. P. Sahu**

**Professor**

**Phone: 03712-275258**

**email: pps@tezu.ernet.in**

---

**CERTIFICATE**

This is to certify that the report entitled “**ENTANGLED TWO STAGE QKD PROTOCOL**” submitted to the Department of Electronics and Communication Engineering, Tezpur University in partial fulfilment for the award of the degree of Bachelor of Technology in Electronics and Communication Engineering, is a record of project work carried out by **KALE VINAY (ECB20053)** under my supervision during the period from January 2023 to June 2024. All support received by him from various sources have been duly acknowledged. No part of this report has been submitted elsewhere for the award of any other degree or diploma.

Date:

**(Prof. P. P. Sahu)**

Place:

*Supervisor*



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

**TEZPUR UNIVERSITY**

**Tezpur-784028, Assam, India**

**Internal supervisor's name:**

**Phone:**

**Designation of supervisor:**

**email:**

---

**CERTIFICATE**

This is to certify that the report entitled “**ENTANGLED TWO STAGE QKD PROTOCOL**” submitted to the Department of Electronics and Communication Engineering, Tezpur University in partial fulfilment for the award of the degree of Bachelor of Technology in Electronics and Communication Engineering, is a record of project work carried out by **KALE VINAY (ECB20053)** under my supervision during the period from January 2023 to June 2024. All support received by him from various sources have been duly acknowledged. No part of this report has been submitted elsewhere for the award of any other degree or diploma.

Date:

Place:

*Internal Supervisor*



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**  
**TEZPUR UNIVERSITY**  
**Tezpur-784028, Assam, India**

**Prof. Bhabesh Deka**  
**Head of the Department**

**Phone: 03712-275262**  
**email: bdeka@tezu.ernet.in**

---

**CERTIFICATE**

This is to certify that the report entitled “*ENTANGLED TWO STAGE QKD PROTOCOL*” is a bonafide record of project work carried out by **KALE VINAY (ECB20053)** and submitted in partial fulfilment for the award of the degree of Bachelor of Technology in Electronics and Communication Engineering during the academic year 2023-2024. He has carried out his project work under the supervision of **Prof. P. P. Sahu, Professor, Dept. of ECE, Tezpur University.**

This approval does not necessarily endorse or accept every statement made, opinion expressed or conclusion drawn as recorded in the report. It only signifies the acceptance of this report for the purpose for which it is submitted.

Date:  
Place:

Prof. BHABESH DEKA  
*HoD, ECE*

### **Certificate by the Examiner**

This is to certify that the report entitled “**ENTANGLED TWO STAGE QKD PROTOCOL**” submitted by **KALE VINAY (ECB20053)** in partial fulfilment of the requirements for the degree of Bachelor of Technology in Electronics and Communication Engineering has been examined by me and is found satisfactory for the award of the degree.

This approval does not necessarily endorse or accept every statement made, opinion expressed or conclusion drawn as recorded in the report. It only signifies the acceptance of this report for the purpose for which it is submitted.

Date:

(Examiner)

Place:

## **ABSTRACT**

Quantum computing is a new branch of research that uses quantum phenomena to conduct data operations. Quantum computing aims to develop algorithms that are significantly faster than classical methods for tackling the same problem.

This report explores the field of Quantum computing for highly secure data communication. The implementation is done using Python programming in IBM Quantum Lab (Qiskit). Qubits are used in place of classical bits while transferring data from sender to receiver. Further, entangled qubits are generated and sent to the sender and receiver for successful encryption and description of data.

## **LIST OF FIGURES**

Figure 1.1: Flow Chart for Quantum Data Communication.

Figure 3.1: Qubit states for the values of  $A_k$  and  $B_k$ .

Figure 4.1: (a) Single qubit one state .

(b) Single qubit of zero state.

Figure 4.2: (a) Single qubit in superposition state of “+” state and phase of zero.

(b) Single qubit of “+” state.

Figure 4.3: (a) Single qubit in superposition state of “-” state and phase of  $\pi$ .

(b) Single qubit of “-” state.

Figure 4.4: Entanglement generation circuit for 2-qubit quantum entanglement.

Figure 4.5: Quantum measurement result for the entangled circuit.

Figure 4.6: Three stage protocol for QKD

Figure 4.7: Fig represents the visualisation of the qubits after the unitary rotational transformations applied by (a)  $\pi/3$ , (b) conjugate transpose of the  $\pi/3$ , (c)  $\pi/4$ , (d) conjugate transpose of the  $\pi/4$ .

Figure 4.8: three stage QKD protocol circuit

Figure 4.9: three stage QKD measurement result of 100110

Figure 4.10: Proposed Entangled two stage QKD Protocol

Figure 4.11: shows the implementation of the proposed Entangled two stage QKD Protocol circuit with  $U_A=60$  degree rotational operation by alice,  $U_B(X)=45$  degree rotational operation by bob.

Figure 4.12: shows the measurement result of the Entangled two stage QKD Protocol circuit.

Security analysis of the Entangled two stage QKD Protocol

Figure 4.13: shows the interception by eavesdropper in between the quantum communication channel where the eavesdropper used the  $U_E = 36$  degree rotational operation .

Figure 4.14: this figure shows the measurement result of the Entangled two stage QKD Protocol circuit when an eavesdropper was intercepted by performing his own unitary Transformation.

Figure 4.15: shows the interception by eavesdropper by measuring in between the quantum communication channel which destroys the entanglement property of the qubits.



Figure 4.16: this figure shows the measurement result of the Entangled two stage QKD Protocol circuit when an eavesdropper was intercepted by measuring the entangled qubits in between the quantum communication channel which destroys the entanglement property of the qubits.

Figure 4.17: Entangled two stage QKD protocol in noisy communication channel

Figure 4.18: average fidelity of AD and PD noise parameters is shown in this graph with the decoherence rate .

Figure 4.19: average fidelity of CD and CR noise parameters , when the quantum state of the qubit is subjected to collective noises.

Figure 4.18: Random measurement basis used by Alice and Bob.

Figure 4.19: Different axes along with observables (X,Z,W,V).

Figure 5.1: Quantum measurement circuit for Start Flag.

Figure 5.2: Quantum measurement result for Start Flag.

Figure 5.3: Quantum measurement circuit for Source IP Address.

Figure 5.4: Quantum measurement result for Source IP Address.

Figure 5.5: Quantum measurement circuit for Destination IP Address.

Figure 5.6: Quantum measurement result for Destination IP Address.

Figure 5.7: Quantum measurement circuit for Data Bits (1st and 2nd Character)

Figure 5.8: Quantum measurement result for Data Bits (1st and 2nd Characters)

Figure 5.9: Quantum measurement circuit for Data Bits (3rd and 4th Characters)

Figure 5.10: Quantum measurement result for Data Bits (3rd and 4th Character).

Figure 5.11: Quantum measurement circuit for Data Bits (5th and 6th Character).

Figure 5.12: Quantum measurement result for Data Bits (5th and 6th Character ).

Figure 5.13: Quantum measurement circuit for Data Bits (Last Character).

Figure 5.14: Quantum \result for Data Bits (Last Character).

Figure 5.15: Quantum measurement circuit for FCS.

Figure 5.16: Quantum measurement result for FCS.

Figure 5.17: Quantum measurement circuit for End Flag.

Figure 5.18: Quantum measurement result for End Flag.

Figure 6.1: Connection Establishment for Quantum Communication.

Figure 7.1: Three Qubit Entanglement Generation Circuit (GHZ)

Figure 7.2: Three qubit Entanglement Generation circuit measurement result

Figure 7.3: Three Qubit Entanglement measurement Circuit (GHZ)

Figure 7.4: Three Qubit Entanglement measurement result



# **CONTENTS**

## Page

Abstract.....	i
List of Figures.....	ii
CHAPTER 1 - Introduction.....	1
CHAPTER 2 - Proposed Flow Chart and Problem Statement.....	2
CHAPTER 3 - Framing of Data and Qubit Conversion.....	4
CHAPTER 4 - Proposed QKD Protocol.....	6
CHAPTER 5 - Receiver and Quantum decryption.....	30
CHAPTER 6 - Quantum Data Communication Through Network.....	47
CHAPTER 7 - Data Communication using GHZ Entangled Qubits.....	49
CHAPTER 8 - Conclusion.....	52
CHAPTER 9 - References.....	53

# **1. INTRODUCTION**

Quantum communication is a new field of research that explores the use of quantum mechanics to transmit information. Qubits, or quantum bits, are the basic unit of information in quantum communication. Qubits can be in a superposition of states, which means that they can be both 0 and 1 at the same time. This property of qubits makes them ideal for transmitting information securely, as it is impossible to eavesdrop on a quantum communication channel without being detected.

Current encryption techniques are based on the difficulty of solving certain mathematical problems. However, quantum computers are much faster than classical computers at solving these problems. This means that it is possible that in the future, quantum computers will be able to crack current encryption techniques, making secure communication impossible.

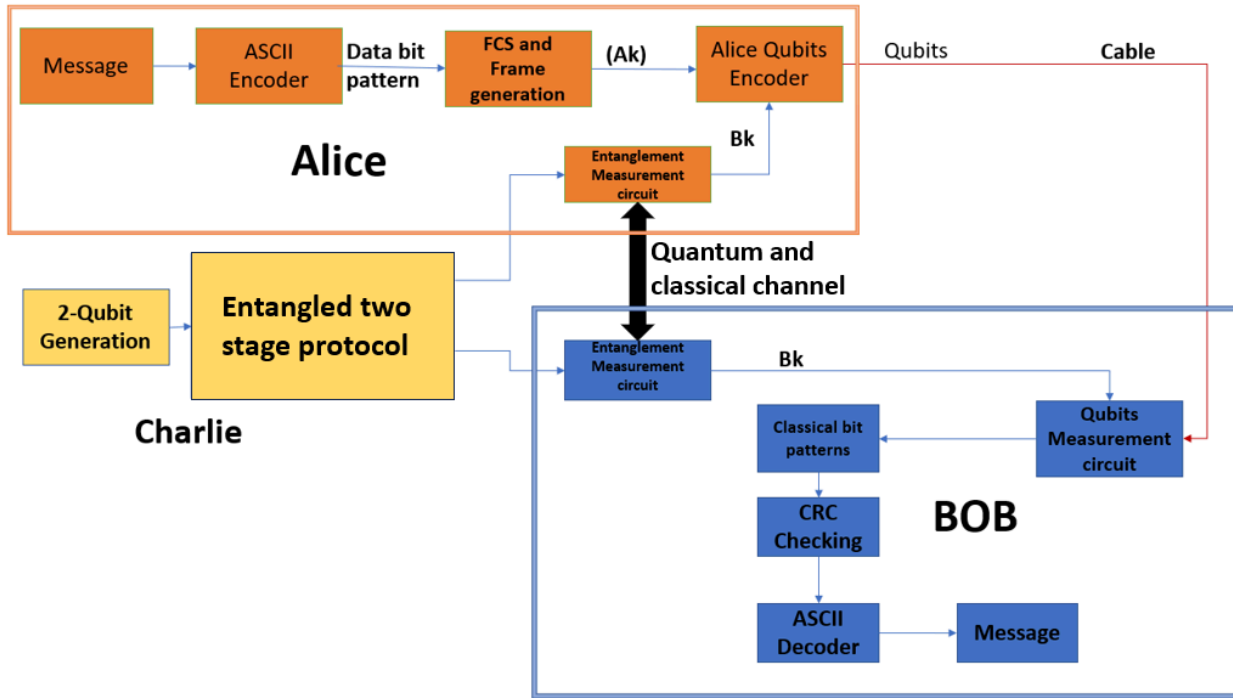
One of the most promising methods for secure quantum communication is quantum key distribution (QKD). QKD uses qubits to establish a shared secret key between two parties, usually named as Alice and Bob. This key can then be used to encrypt any subsequent communication between Alice and Bob. The quantum entanglement property to establish a shared secret key between Alice and Bob. This property of quantum entanglement makes it impossible for an eavesdropper to eavesdrop on a quantum communication channel without being detected.

The three stage protocol for quantum key distribution was proposed by Kak and the three-stage QKD algorithm, which Mandal et al. experimentally implemented in 2013. In comparison to the traditional BB84 protocol and its variations, this system provides a few advantages. For instance, multi-photon pulses can be used to implement it instead of a single photon source. It can also be changed to produce three-stage quantum protocols for additional activities involving quantum communication.

The quantum internet is a proposed new network that would use quantum communication to transmit information between different nodes. The quantum internet would be much faster and more secure than the current internet. It would be used for a variety of applications.

The quantum internet is still in its early stages of development, but it has the potential to revolutionize the way we communicate and compute.

## 2. PROPOSED FLOWCHART AND PROBLEM STATEMENT



**Figure 2.1:** Flow Chart for Quantum Data Communication

Figure 2.1 shows our proposed flow chart for Quantum data communication based on Entangled two stage quantum key distribution protocol using High level data link control (HDLC) of TCP/IP. The process begins with Alice, converting the message into binary bits using an ASCII encoder. Then, a Frame Check Sequence (FCS) is generated to ensure data integrity using error checking of data through Cyclic redundancy check (CRC). The HDLC generates frames consisting of Flag signal (start bits), TCP/IP address field, binary data bits, FCS and Flag signal (end bits).

At the same time, Charlie generates quantum qubits using photons and entangles them to create pairs of 2-qubit quantum states. Each entangled qubit pair is sent to Alice and Bob for performing measurements using an entanglement measurement circuit. Alice encodes the data bits into qubits using ASCII encoder and entangles qubits using a qubit encoder and sends them to Bob through the selected path. Bob decrypts the data by measuring the qubits one by one using a qubit measurement circuit. This allows him to obtain the classical bit pattern of the received message. He then checks for

errors using CRC (Cyclic Redundancy Check) to ensure the data's integrity. Finally, Bob decodes the message using an ASCII decoder.

During the communication between Alice and Bob, the information about the measurement bases are exchanged between them using HDLC supervised frames. This information is shared through a dedicated path connecting them.

The process begins with Alice, the receiver, converting the message into binary bits using an ASCII encoder. Then, a Frame Check Sequence (FCS) is generated to ensure data integrity.

On the other end, Charlie generates quantum qubits using photons and entangles them to create pairs of 2-qubit quantum states. Each entangled qubit pair is sent to Alice and Bob for performing measurements using an entanglement measurement circuit. Alice encodes the data and entangles qubits into qubits using a qubit encoder and sends them to Bob.

Bob decrypts the data by measuring the qubits one by one using a qubit measurement circuit. This allows him to obtain the classical bit pattern of the received message. He then checks for errors using CRC (Cyclic Redundancy Check) to ensure the data's integrity. Finally, Bob decodes the message using an ASCII decoder.

During the communication between Alice and Bob, they exchange information about the measurement bases they use. This information is shared through the path connecting them.

In summary, Alice receives the message, converts it into binary, and generates an FCS. Charlie generates entangled qubits that Alice and Bob use for measurements. Alice encodes the data and qubits, which are then sent to Bob. Bob measures the qubits, checks for errors, and decodes the message.

## **2.1 Problem statements**

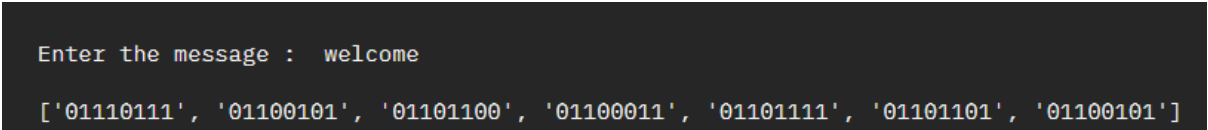
- Perform highly secured data communication between Alice and Bob.
- Encoding the classical bits of information into qubits for data transmission.
- Measuring quantum qubits using proper quantum circuits for data decryption.
- Proposing new quantum protocols for quantum communication with qubits.
- Generating three entangled qubits using the GHZ circuit.

### **3. FRAMING OF DATA AND QUBIT CONVERSION**

#### **3.1 Conversion of Message Data into Classical Bit Patterns**

In order to facilitate the transmission and processing of messages consisting of characters and symbols in a classical system, it is essential to convert the original message into bit patterns using ASCII coder in a format compatible with classical computing and communication technologies.

The process of converting message data into classical bit patterns involves mapping each character or symbol in the message to its corresponding bit representation. This mapping can be achieved using various encoding techniques. Here we have used an encoding method of ASCII (American Standard Code for Information Interchange) to Binary representation, where each character is represented by a 8-bit binary code.



```
Enter the message : welcome
['01110111', '01100101', '01101100', '01100011', '01101111', '01101101', '01100101']
```

The above image shows the bit pattern assigned by the ASCII encoding scheme for the message “welcome”.

#### **3.2 Frame Generation**

**Start flag bits:** The frame begins with 8-bit start bits, which serve as a synchronization mechanism between the sender and receiver. Start bits indicate the start of the frame and enable the receiver to identify the beginning of the transmitted data.

**IP Addresses of Sender and Receiver:** The frame includes 16-bit IP (Internet Protocol) addresses of both the sender and receiver. In the context of the frame, these addresses help direct the message to the intended recipient.

**Message Character Encoding:** The frame contains the message data, where each character is encoded into 8 bits. The encoded characters are organized sequentially within the frame to maintain the original order of the message.

**FCS (Frame Check Sequence):** To ensure the integrity of the transmitted message, the frame includes a 6-bit Frame Check Sequence (FCS). The FCS refers to the checksum generated using the CRC 6-UTI

algorithm with the '1000011' key, as discussed earlier. It serves as a means of error detection, allowing the receiver to check the bit errors of the frames for recovering the message.

End flag Bits: Similar to the start bits, the frame ends with 8-bit end bits, which mark the completion of the frame. These bits help the receiver identify the end of the transmitted data and synchronize with subsequent frames if necessary.

```
:['01111110', '1011001011101011', '1100111010101100', '0111011101100101', '0110110001100011', '0110111101101101', '01100101', '101000', '01111110']
```

The image above shows the bit pattern of the data frame for the message “welcome”.

### 3.3 FCS Generation

```
Frame data :['01111110', '1011001011101011', '1100111010101100', '0111011101100101', '0110110001100011', '0110111101101101', '01100101', '101000', '01111110']
```

In the project, CRC 6-UTI is selected as a CRC (cyclic redundancy variant) for error detection of the frame and represented as a binary number of 1000011. The polynomial division process is used for finding FCS with the CRC scheme.

CRC 6-UTI is chosen due to its effectiveness in detecting errors in transmitted data. It provides a balance between error detection capabilities and computational efficiency. The 6-bit length of the CRC ensures that it can detect a wide range of errors in the message data.

Upon receiving the message, the receiver performs the same polynomial division process using the CRC 6-UTI key. If the calculated checksum matches the received checksum, it indicates that no errors occurred during transmission. Otherwise, the receiver detects an error in the message.

The Frame Check Sequence (FCS) in the project refers to the CRC 6-UTI checksum that is generated and appended to the frame. It serves as a reliable means of error detection, enabling the receiver to verify the integrity of the received message and identify any potential errors.

By employing CRC 6-UTI with the 1000011 key, the project aims to detect and identify errors in the transmitted message data, enhancing the overall reliability and accuracy of the communication system.

```
The FCS generated is :  
['1', '0', '1', '0', '0', '0']
```



The above image shows the FCS generated for the message bits.

### 3.4 Preparation of Qubits for Data Transmission

After the frame is generated, Alice prepares the qubit states for the values of message bit string  $A_k$  and the values of binary string of entangled qubits  $B_k$  and sends it through the optical fiber to Bob.

$$|\psi\rangle = \bigotimes_{k=1}^n |\psi_{a_k b_k}\rangle \quad \begin{array}{ll} |\psi_{00}\rangle = |0\rangle, & |\psi_{01}\rangle = |+\rangle \\ |\psi_{10}\rangle = |1\rangle, & |\psi_{11}\rangle = |-\rangle \end{array}$$

**Figure 3.1:** Qubit states for the values of  $A_k$  and  $B_k$

The qubit states can be described as follows:

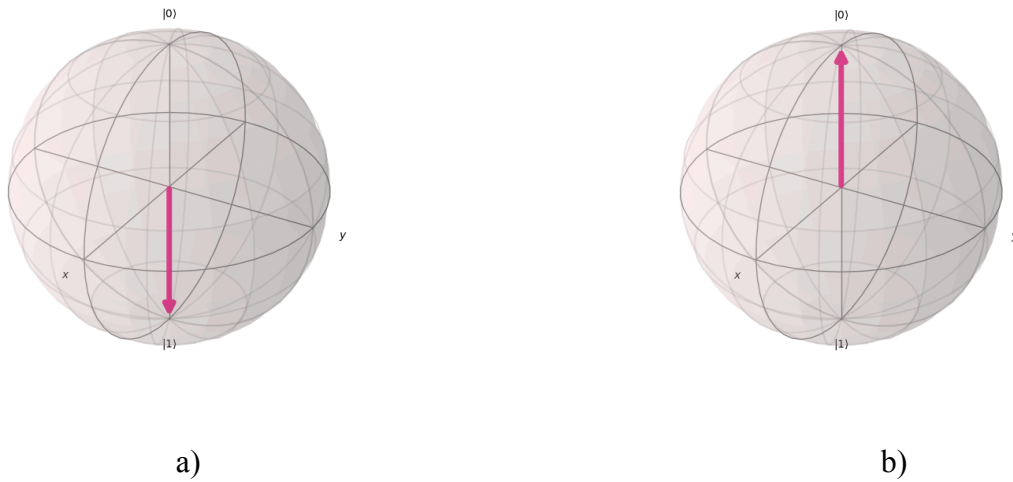
- If  $A_k = 0$  and  $B_k = 0$  then Alice will initialize the qubit in **0** state .
- If  $A_k = 0$  and  $B_k = 1$  then Alice will initialize the qubit in **+** state .
- If  $A_k = 1$  and  $B_k = 0$  then Alice will initialize the qubit in **1** state .
- If  $A_k = 1$  and  $B_k = 1$  then Alice will initialize the qubit in **-** state .

## 4. Proposed QKD Protocol

### 4.1 Hadamard Gate

In quantum computing, the Hadamard gate is a fundamental single-qubit gate that is commonly used to create superposition states. It is named after Jacques Hadamard, a French mathematician. The Hadamard gate is represented by the matrix:

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

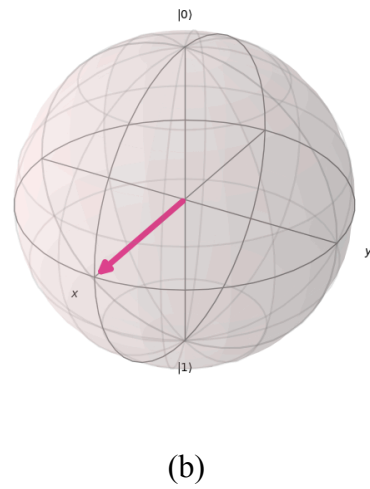
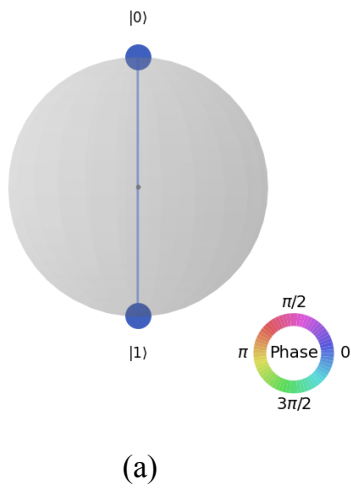


**Figure 4.1:** (a) Single qubit one state .  
(b) Single qubit of zero state.

When applied to a single qubit, the Hadamard gate transforms the basis states  $|0\rangle$  and  $|1\rangle$  into superposition states. It has the following effect:

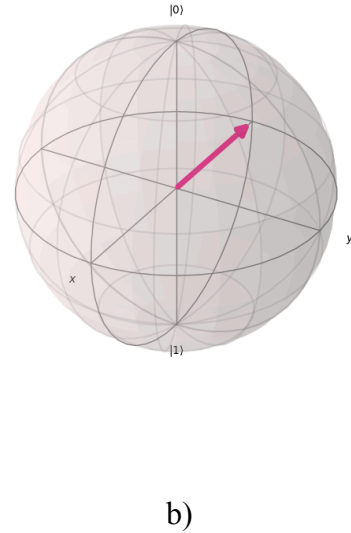
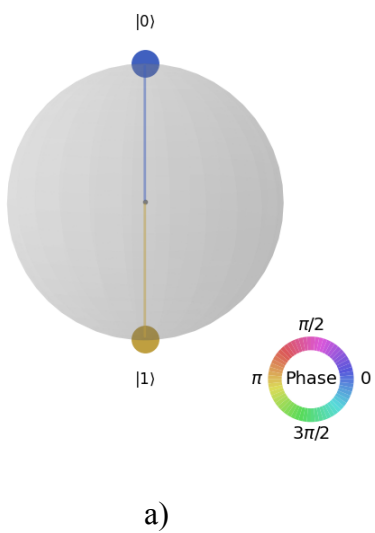
$$H(|0\rangle) = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$H(|1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$



**Figure 4.2:** (a) Single qubit in superposition state of “+” state and phase of zero.

(b) Single qubit of “+” state.



**Figure 4.3:** (a) Single qubit in superposition state of “-” state and phase of  $\pi(\pi)$ .

(b) Single qubit of “-” state.

Figure 4.2 and figure 4.3 are visual representations of “+” state and “-” state of a qubit after the operation of Hadamard gate with a qubit in its “0” state and “1” state respectively.

The Hadamard gate is particularly useful because it allows us to prepare states that are simultaneously in both the  $|0\rangle$  and  $|1\rangle$  states. This superposition property is crucial for various quantum algorithms. Additionally, applying the Hadamard gate twice to a qubit returns it to its original state. In multi-qubit systems, the Hadamard gate can be used to create entangled states and perform quantum computations. It is an essential building block in many quantum circuits and plays a significant role in quantum algorithms like the quantum search algorithm and quantum error correction codes.

## 4.2 Controlled-NOT Gate

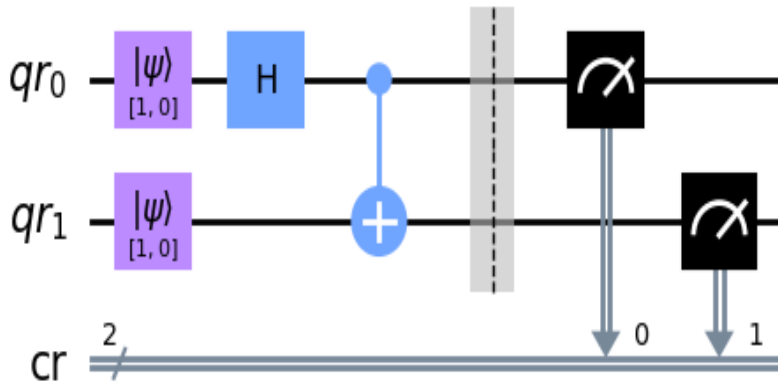
In quantum computing, the controlled NOT gate, often abbreviated as CNOT or CX gate, is a two-qubit gate that operates on a control qubit and a target qubit. It flips the state of the target qubit if and only if the control qubit is in the state  $|1\rangle$ . The controlled NOT gate is a crucial component in quantum circuits for creating entanglement and implementing quantum gates.

The controlled NOT gate can be represented by the following matrix:

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

The first two rows correspond to the control qubit being in the state  $|0\rangle$ , and the last two rows correspond to the control qubit being in the state  $|1\rangle$ . The first column represents the target qubit being in the state  $|0\rangle$ , and the second column represents the target qubit being in the state  $|1\rangle$ .

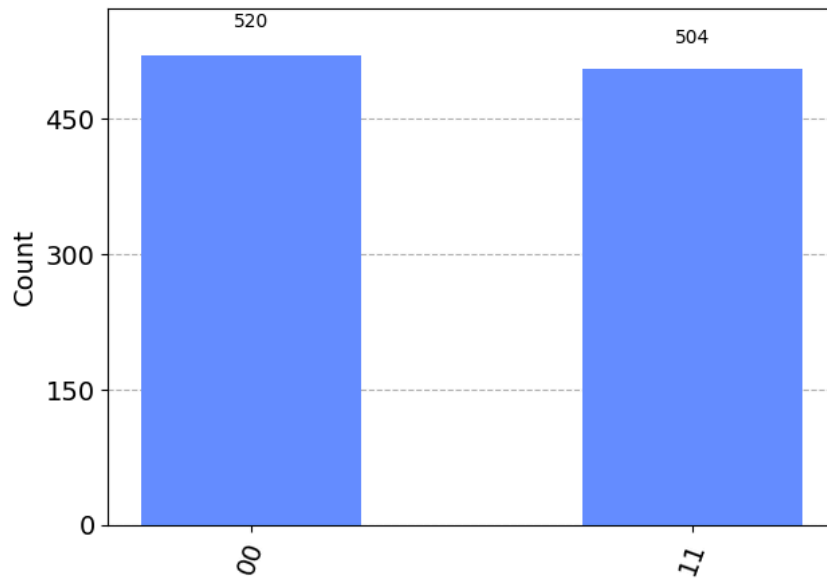
When the controlled NOT gate is applied to a pair of qubits, its effect depends on the state of the control qubit. If the control qubit is in the state  $|0\rangle$ , the target qubit remains unchanged. However, if the control qubit is in the state  $|1\rangle$ , the target qubit gets flipped (i.e., the state  $|0\rangle$  becomes  $|1\rangle$ , and vice versa).



**Figure 4.4:** Entanglement generation circuit for 2-qubit quantum entanglement

In figure 4.4 the qubits are generated using photons through precise control over their properties such as polarization, or phase. The process of subsequent entanglement of the qubits are performed wherein there is initialization of the two qubits to the zero state within the entangled circuit. Next, a Hadamard gate is applied to the first qubit, followed by a controlled-NOT (CNOT) gate. The CNOT gate utilizes the first qubit as the control bit and the second qubit as the target bit. As a result, the first qubit enters a superposition state, allowing it to flip its bit whenever the control bit is in the one state. As shown in the figure.

$$\begin{aligned}
 & \left. \begin{array}{l} |0\rangle \rightarrow \boxed{H} \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |0\rangle \rightarrow \oplus \end{array} \right\} |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
 & H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left[ \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
 & |0\rangle \oplus |0\rangle = |0\rangle \quad , \quad |1\rangle \oplus |0\rangle = |1\rangle \\
 & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \xrightarrow{(C-NOT) \text{ gate}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)
 \end{aligned}$$



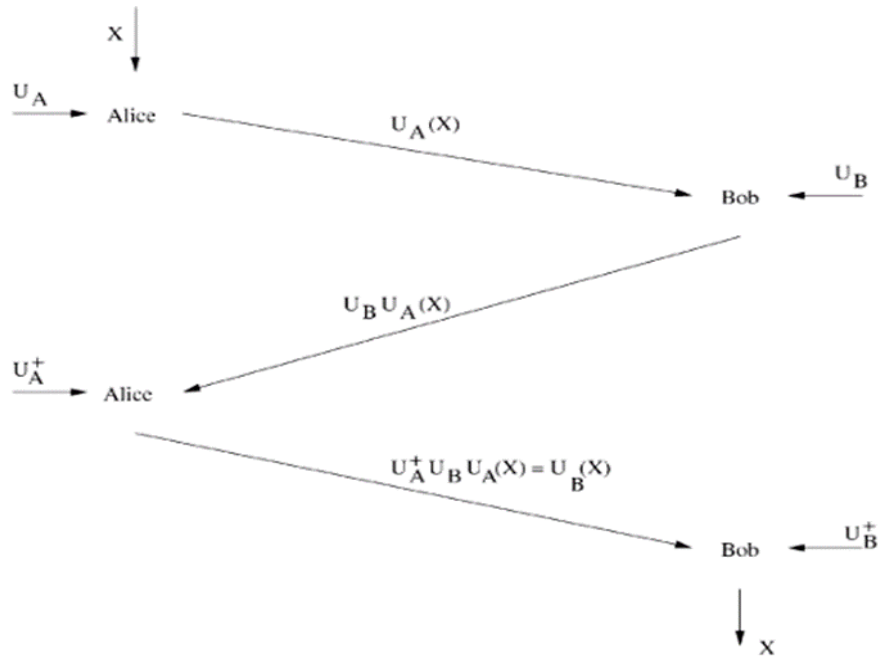
**Figure 4.5:** Quantum measurement result for the entangled circuit

In figure 4.5, upon completion of these operations, the entangled qubits are obtained, with a 50% probability of being in the '00' state and a 50% probability of being in the '11' state. The entanglement arises from the correlations established between the two qubits, whereby their states become intrinsically linked regardless of spatial separation. This entanglement enables the transmission of quantum information and serves as a fundamental resource for various quantum information processing tasks.

#### 4.4 Three stage QKD protocol

The Three-stage quantum cryptography protocol is an encryption technique that continuously encrypts data using single photons using random polarization rotations by the two authenticated parties. It can also be used to exchange keys and can be modified to counter man-in-the-middle attacks.

**Kak's three-stage protocol for QKD:**



**Figure 4.6:** Three stage protocol for QKD

1. Alice delivers quantum state  $X$  to Bob after applying a unitary transformation ( $U_A$ ) to it.

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

2. Bob chooses at random whether to give Alice the received signal,  $U_A(X)$ , with  $U_B$  applied, or to keep it for authentication.
3. Alice decides at random to give Bob the received signal,  $U_B U_A(X)$ , with the complex conjugate transpose of  $U_A$  applied, or to keep it for authentication.
4. Bob obtains the information of quantum state  $X$  by applying  $U_B^+$  on  $U_A^+ U_B U_A(X) = U_B(X)$ .

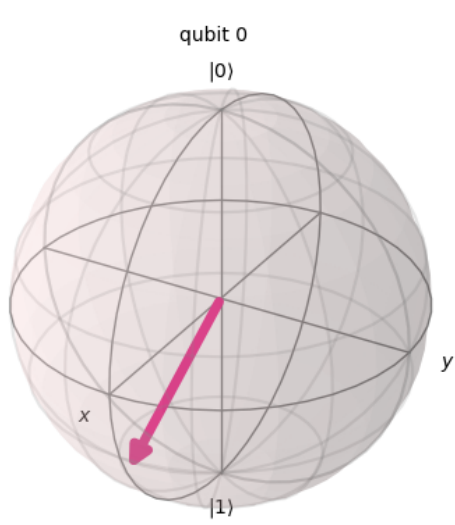
5. Bob makes public the pulses he has measured after obtaining all of the pulses. After that, Alice throws out the pulses that Bob failed to measure. A key that has an excessively low bit rate is abandoned.

6. Bob discloses to Alice the qubits he selected for verification. He is shown by Alice the matching transformations and  $X$  that she applied for those qubits. The changes are employed to calculate the likelihood of a man-in-the-middle assault. The pulses that Alice saved can also be used for the authentication. Subsequently, Alice divulges to Bob a segment of the shared data  $X$  in order to assess the error rate. If the errors in the key and the transformations are less than predetermined limits, they accept the remaining portion of the key.

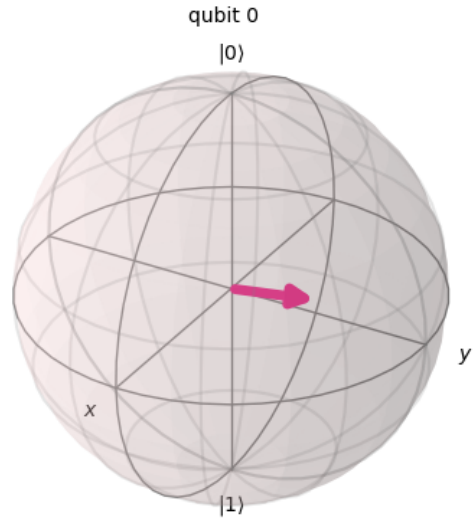
7. In order to reduce Eve's information, Alice and Bob finally carry out post-processing (error correction and privacy amplification) as normal.

At the conclusion of the process, Bob has received the state  $X$ , which was selected by Alice and sent over a public channel. Even though Eve, the eavesdropper, may stop the exchange by substituting her own qubits for the transmitted ones, she is unable to get any information by intercepting the transmitted qubits. Appending parity bits, previously selected bit sequences—which can include the transmitting and destination addresses or their hashed values—or any other mutually agreed-upon sequence can be used to detect this. Eve cannot intercept the qubits and acquire any statistical clues regarding the nature of the  $U$  transformations as they are freely modified.

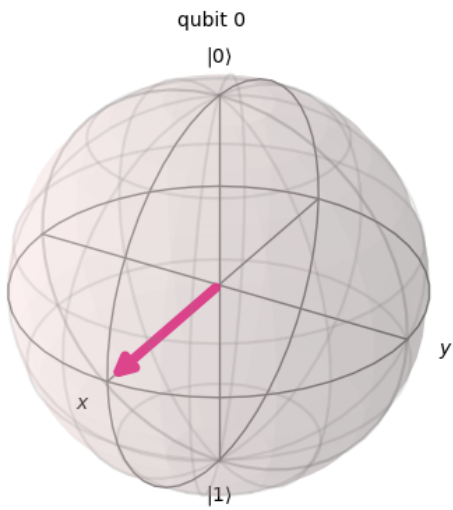




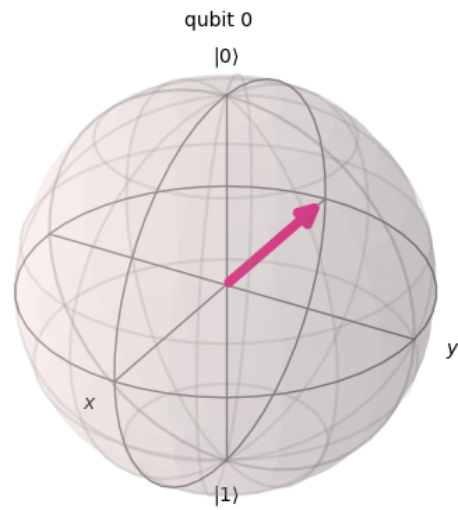
(a)



(b)



(c)

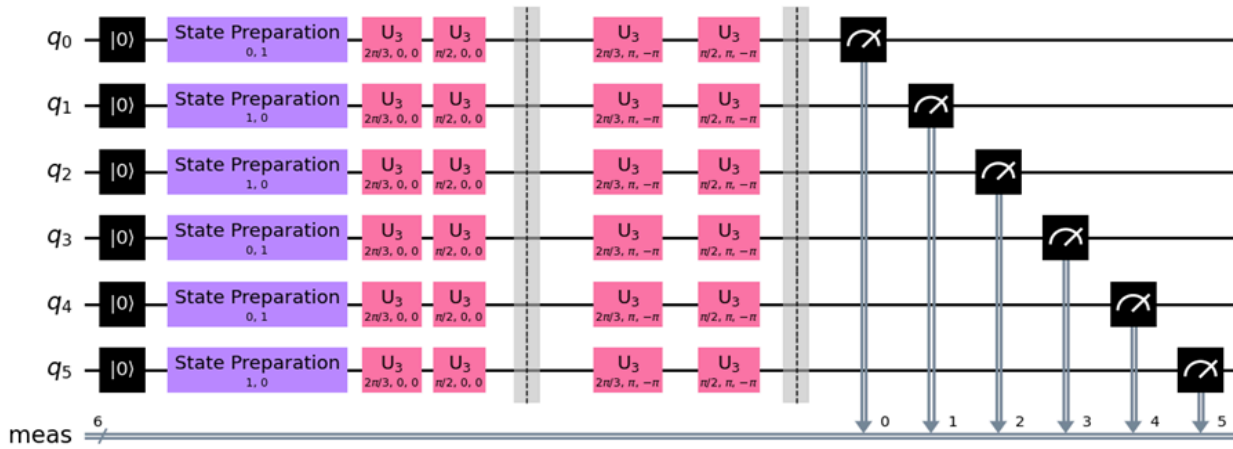


(d)

54

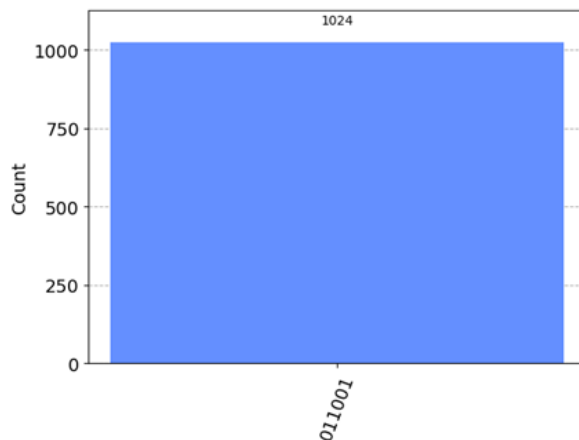
**Figure 4.7:** Fig represents the visualization of the qubits after the unitary rotational transformations applied by (a)  $\pi/3$ , (b) conjugate transpose of the  $\pi/3$ , (c)  $\pi/4$ , (d) conjugate transpose of the  $\pi/4$

## Implementation:



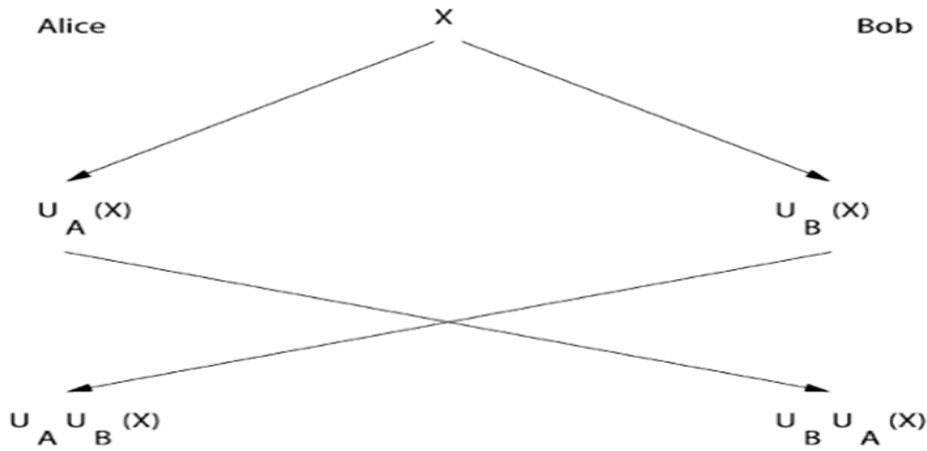
**Figure 4.8:** Three stage QKD protocol circuit

The three-stage quantum key distribution for the five qubits is implemented in the above figure. Here, the qubits have been initialized prior to the application of the Alice rotational operation. The qubit then be sent to the bob, who will then apply his own secret rotational operation and send it back to Alice through the same quantum channel. Once Alice receives the qubit from Bob, she applies the conjugate transpose of the rotational operator she previously used and sends it back to Bob. Bob will also apply the conjugate transpose of the rotational operator he previously employed after obtaining the qubit. He will then measure the qubit and decode the message that Alice encoded after this step. As can be seen from the measurement result in the image, Alice successfully deciphered the 100110 message that was stored in the qubits before passing it through via the three-stage QKD procedure.



**Figure 4.9:** Three stage QKD measurement result of 100110

#### 4.5 Proposed Entangled two stage QKD Protocol:

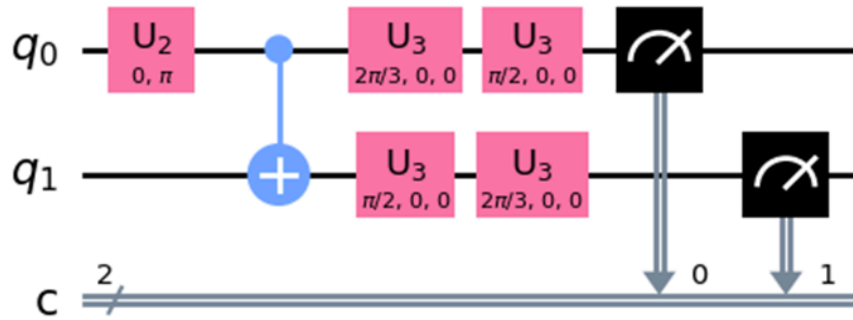


**Figure 4.10:** Proposed Entangled two stage QKD Protocol

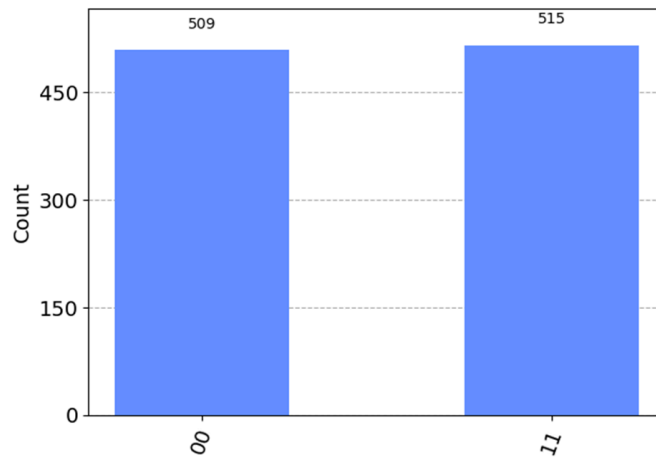
A related key distribution protocol shown in the fig ,  $X$  is a fixed public state, in contrast to the preceding example. The goal is to provide a key that depends on the transformations that are involved and isn't predetermined by either side. There are two steps to the protocol:

A key registration authority, Charlie, may provide Alice and Bob with two copies of the unknown quantum state  $X$  in a three-stage QKD protocol variation via the entanglement generation circuit, as seen in the figure. Following receipt of the entangled pair of qubits, Alice and Bob swap the qubits by applying the covert transformations  $U_A$  and  $U_B$  to them.

They each obtain  $U_A U_B(X)$  after applying the identical changes once again to the received qubits. given that  $U_A U_B = U_B U_A$  It is anticipated that the received qubits will be used as the input to a quantum register and that neither Alice nor Bob will measure them.

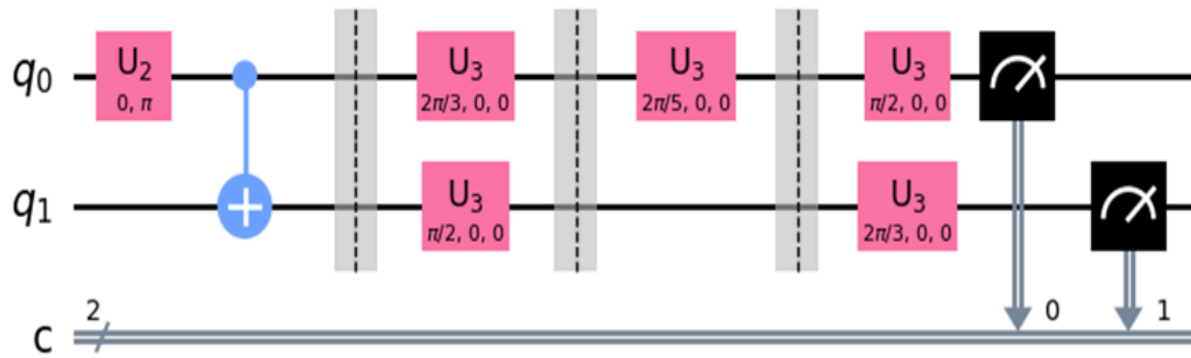


**Figure 4.11:** shows the implementation of the proposed Entangled two stage QKD Protocol circuit with  $U_A=60$  degree rotational operation by alice,  $U_B(X)=45$  degree rotational operation by bob

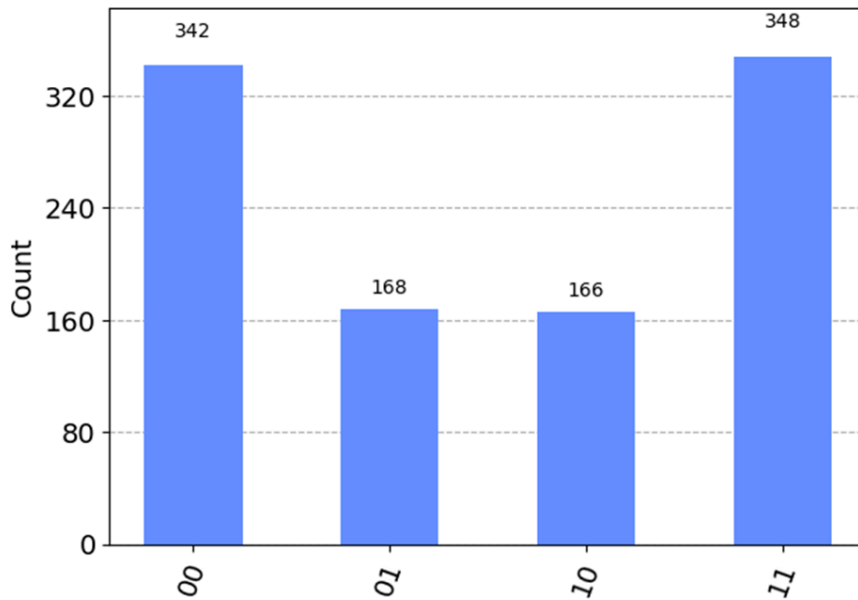


**Figure 4.12:** shows the measurement result of the Entangled two stage QKD Protocol circuit. Security analysis of the Entangled two stage QKD Protocol

Case 1: when the eavesdropper tries to apply his rotational operation for getting the key information. Here we have shown the simulation the same situation in the fig where the eavesdropper rotates one of the qubits with his random rotational operation. Here in this case the eavesdropper used  $\pi/5$  angle unitary transformation . and we can observe the measurement result of the simulation result which shows all possible cases of 00,01,10,11. By using the Appending parity bits, previously selected bit sequences—which can include the transmitting and destination addresses or their hashed values—or any other mutually agreed-upon sequence can be used to detect this .



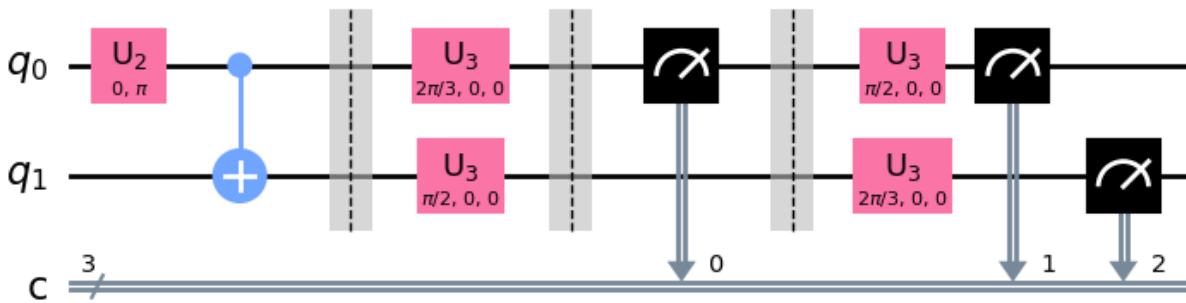
**Figure 4.13:** shows the interception by eavesdropper in between the quantum communication channel where the eavesdropper used the  $UE = 36$  degree rotational operation .



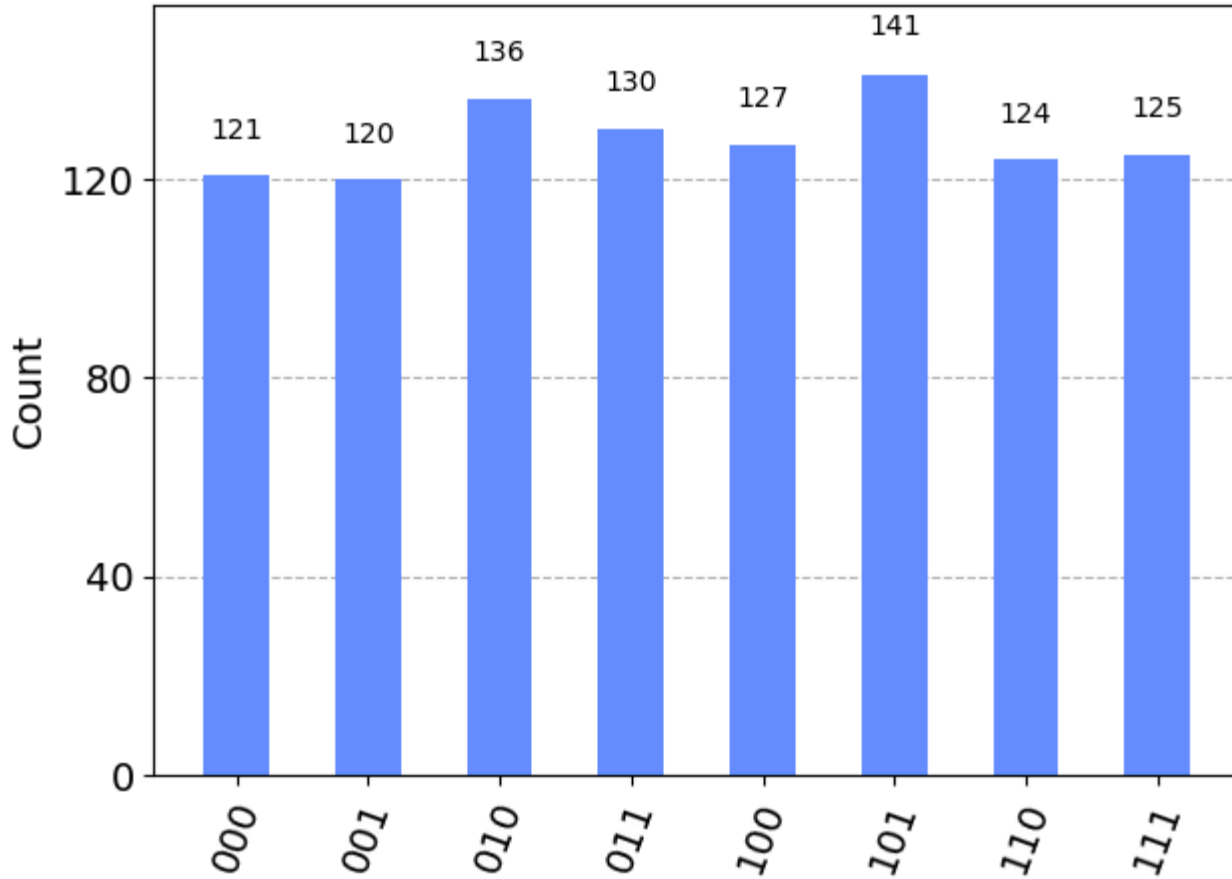
**Figure 4.14:** shows the measurement result of the Entangled two stage QKD Protocol circuit when an eavesdropper was intercepted by performing his own unitary transformation.

Case 2:

when the eavesdropper tries to measure the qubit for getting the key information. Here we have shown the simulation the same situation in the fig where the eavesdropper tries to measure one of the qubits. Here in this case the eavesdropper measured the qubit coming from the alice after she applied her unitary transformation. and after which he will destroy the entanglement of the qubits which we can observe in the measurement result of the simulation result which shows all possible cases of 00,01,10,11. By using the Appending parity bits, previously selected bit sequences—which can include the transmitting and destination addresses or their hashed values—or any other mutually agreed-upon sequence can be used to detect this .



**Figure 4.15:** shows the interception by eavesdropper by measuring in between the quantum communication channel which destroys the entanglement property of the qubits.



**Figure 4.16:** shows the measurement result of the Entangled two stage QKD Protocol circuit when an eavesdropper was intercepted by measuring the entangled qubits in between the quantum communication channel which destroys the entanglement property of the qubits.

Entangled two stage QKD Protocol can be thought of as a quantum double-lock encryption, where the locks are the unitary transformations  $U_A$  and  $U_B$ , which in this case are polarization rotations. Thus, the three-stage protocol's security depends on following things:

- (1) The transformation's capacity to safeguard the sent bit value.
- (2) Alice and Bob's conviction that they were the ones who actually applied the locks during the information transfer.

(3) quantum mechanics prevents the generation of identical clones of any given unknown quantum state, it leads to the no cloning theorem.

(4) Entanglement is a phenomenon where, even when the items are separated by a great distance, the quantum states of two or more objects become entangled to the point where the state of one object can no longer be represented independently of the states of the other objects. On the other hand, one of the entangled particles collapses into one of the potential states upon measurement. No matter how far apart they are, the other particle's state instantly reflects this collapse. Wave function collapse or quantum state collapse are terms used to describe this. The particles lose their entanglement after the measurement and are no longer entangled. Even if they might have been entangled before the measurement, they are no longer able to impact one another. This is commonly known as the quantum state's decoherence.

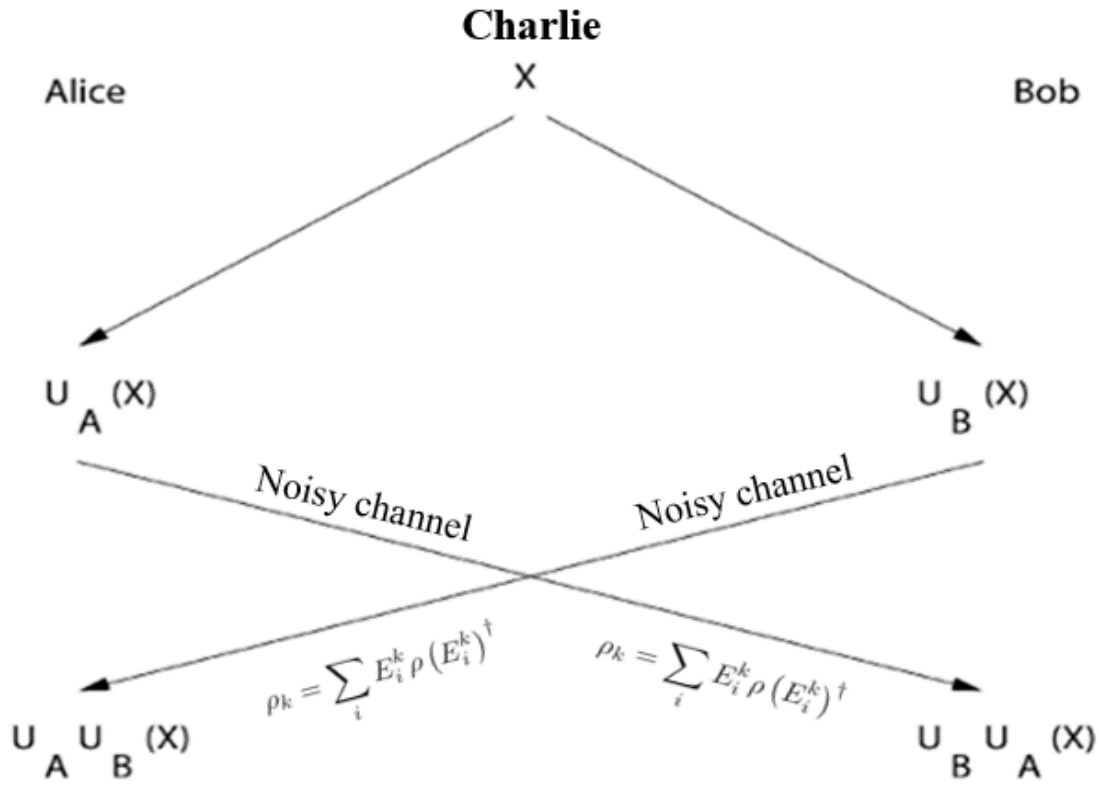
The second scenario is exploited by an invader Eve man-in-the-middle (MIM) attack. In what follows, we will address the two scenarios in further detail.

The Entangled two stage QKD Protocol core premise is that Bob only needs to discriminate between two distinct orthogonal polarization states—horizontal and vertical—in order to retrieve the key X. Conversely, an eavesdropper Eve must ascertain the arbitrary unknown polarization angles  $\phi_i$  of the quantum state transmitted in the quantum channel in order to receive meaningful information. The quantity of photons she can access from the channel determines how accurate her measurement will be. The polarization rotation angle that Bob and Alice decide to apply to the information bits is an independent, arbitrary parameter that ranges from 0 to 180 degrees.

It should be mentioned that in practice, one must also consider the challenges of preserving integrity and stability when noise is present. We shall disregard these conditions in the analysis that follows and make the assumption that Alice and Bob can continue to align perfectly in their basis for simplicity.



### Effect of noise:



**Figure 4.17:** Entangled two stage QKD protocol in noisy communication channel

Using the Kraus operator concept, a single qubit quantum physical state  $\rho$  in a noisy quantum communication channel can be characterized.

$$\rho_k = \sum_i E_i^k \rho (E_i^k)^\dagger$$

We take into consideration of some noise models, including the AD and PD noise channels as well as the CD and CR collective noise channels. The impact of amplitude damping (AD) noise is examined initially in relation to the quantum state  $\rho$ . A dissipative interaction between a system and its environment is taken into consideration in the AD noise. The environment is regarded as a vacuum

bath, meaning that there is no squeezing and it is at zero temperature. The interaction results in a loss of energy, specifically photons. The following Kraus operators describe such a noise:

$$E_0^A = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\eta_A} \end{bmatrix}, \quad E_1^A = \begin{bmatrix} 0 & \sqrt{\eta_A} \\ 0 & 0 \end{bmatrix}$$

where the probability error caused by the AD channel is described by  $\eta_A$  (where  $0 \leq \eta_A \leq 1$ ), the decoherence rate. Impact of Phase Damping (PD) noise the PD noise takes into account an energy-loss-free interaction between a system and its surroundings. In particular, the environment is thought to have the effect of making the density matrix's off-diagonal terms disappear, which causes the state to be mixed. The following Kraus operators describe the PD noise model.

$$E_0^P = \sqrt{1-\eta_P} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_1^P = \sqrt{\eta_P} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad E_2^P = \sqrt{\eta_P} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

where the PD channel decoherence rate is expressed as  $\eta_P$  ( $0 < \eta_P = 1$ ).

Impact of noise using collective dephasing (CD) Collective noise models are explored as a coherent impact of environment on all qubits passing through a quantum communication channel. The impact of CD noise is distinguished by

$$E^D |0\rangle = |0\rangle \quad E^D |1\rangle = \exp(i\Phi) |1\rangle$$

$$E^D = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\Phi) \end{bmatrix}$$

Impact of collective rotation (CR) noise: the model of CR noise, which is described as

$$E^R |0\rangle = \cos \Theta |0\rangle + \sin \Theta |1\rangle \quad E^R |1\rangle = -\sin \Theta |0\rangle + \cos \Theta |1\rangle$$

$$E^R = \begin{bmatrix} \cos \Theta & -\sin \Theta \\ \sin \Theta & \cos \Theta \end{bmatrix}$$

the three-stage Kak protocol's of a single qubit quantum state in a noisy channel is defined as

$$\rho_k = \sum_{i,j,l} \left( (R(\phi))^\dagger E_i^k R((\theta))^\dagger E_j^k R(\phi) E_l^k R(\theta) \right) \rho \left( (R(\phi))^\dagger E_i^k R((\theta))^\dagger E_j^k R(\phi) E_l^k R(\theta) \right)^\dagger$$

The sort of noise model being considered is denoted by  $k \in \{\text{AD}, \text{PD}\}$ , and Alice has prepared the single qubit initial state  $\rho$ . In Step 1, Alice's (Bob's) action rotates the single qubit state in the Bloch sphere by an angle  $\theta$  ( $\phi$ ). Furthermore, distinct  $i$ ,  $j$ , and  $l$  in the subscript stand for independent noise effects along the journeys of a single qubit from Alice to Bob, Bob to Alice, and Alice to Bob, respectively.

Upon initial observation, the commutativity of Alice and Bob's rotation operators can only be maintained if the rotation unitary operators commute with the Kraus operators for different noise models. To start, let's look at a straightforward scenario where Kak's protocol is implemented using an amplitude damping (AD) quantum communication channel. In this scenario, noise affects the qubit via  $E_A 0$  during the first two stages of the protocol (i.e., the journeys from Alice to Bob, Bob to Alice). As a result, Alice will receive  $|\psi'' = E_A 0 R(\phi) E_A 0 R(\theta) |\psi$  rather than  $|\psi'' = R(\phi) R(\theta) |\psi = R(\theta) R(\phi) |\psi$ . Recall that if and only if  $R(\delta)$  commutes with  $E_A 0$ , Alice would be able to encode her encryption,  $U_A = R(\theta)$ , by applying  $U_A^\dagger A = U^{-1}$ . Only if  $R(\theta)$  commutes with  $E_A 0$  (i.e., iff  $E_A 0, R(\theta) = 0$ ).

$$[E_0^A, R(\theta)] = E_0^A R(\theta) - R(\theta) E_0^A = \left(1 - \sqrt{1 - \eta}\right) \sin \theta \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$[E_1^A, R(\theta)] = E_1^A R(\theta) - R(\theta) E_1^A = -\sqrt{\eta} \sin \theta \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

It is necessary for either  $\eta = 0$  or  $\theta = 0$  for this commutator to vanish, that is,  $E_A 0, R(\theta) = 0$ . While the latter scenario corresponds to no rotation imposed by Alice in the protocol, meaning that  $R(\theta)$  becomes identity and the eavesdropper's ignorance becomes zero, the former case relates to a noiseless

environment. These are insignificant situations, and the study demonstrates that Kak's protocol does not function as intended in the scenario mentioned above. The observation can be reinforced even more by pointing out that

Therefore, it can be concluded that the three-stage quantum key distribution protocol fails in the presence of AD noise because the inverse operator of the identical rotation operator used in the protocol's fourth step does not cancel out the rotation operator of Alice that was operated in the second step. Studies of a similar nature can be conducted for various types of noise, such as PD noise. As a matter of fact, we find that the conclusions drawn from EP 0 and EP 1 are identical to those we reached for the AD noise channel.

It is relatively simple to conduct similar research for both CD and CR noise because unitary operators are used in both cases to characterize the noise's influence. In particular, the rotation operator commutes exclusively under ideal conditions and in the noisy case for  $\Phi = 2n\pi$  with integer  $n$  (because the unitary for CD noise reduces to an identity).

This is the same conclusion that the rotation noise produces. Additionally, since two arbitrary rotation unitary operators always commute with one another, CR noise has no effect on the protocol. Thus, under CR noise, Kak's protocol would function.

Fidelity of the different noise parameters :

$$F = \langle \psi | \rho_k | \psi \rangle, \quad F_k^{\text{av}} = \frac{1}{2\pi} \int_0^{2\pi} F_k d\theta.$$

The fidelity of the above quantum channel noises are calculated by using the below formula and Kraus operators of the AD noise that are E(AD).

$$F_{AD} = \frac{1}{16} \left[ -\eta (\eta^2 - 3 (\sqrt{1-\eta} + 2) \eta + 7\sqrt{1-\eta} + 9) + 4 (\sqrt{1-\eta} + 3) \right. \\ \left. - (\eta - 1) (\eta (\eta + 3\sqrt{1-\eta} - 5) - 4\sqrt{1-\eta} + 4) \cos(4\xi) \right]$$

The average of the fidelity of the AD noise is calculated by the

$$F_{AD}^{\text{av}} = \frac{1}{16} \left( 4 \left( \sqrt{1-\eta} + 3 \right) - \eta \left( \eta^2 - 3 \left( \sqrt{1-\eta} + 2 \right) \eta + 7\sqrt{1-\eta} + 9 \right) \right)$$

Similarly the fidelity of the Phase damping(PD)noise quantum channel noises are calculated by using the below formula .

$$F_{PD} = \frac{1}{8} \left( \left( -\sqrt{1-\eta}\eta + 3\eta + 4\sqrt{1-\eta} - 4 \right) \sin^2(2\xi) - 3\eta + 8 \right)$$

The average of the fidelity of the PD noise is calculated by the

$$F_{PD}^{\text{av}} = \frac{1}{16} \left( \sqrt{1-\eta} + 3 \right) (4 - \eta)$$

The fidelity of the collective damping(CD) noise quantum channel noises are calculated by using the below formula .

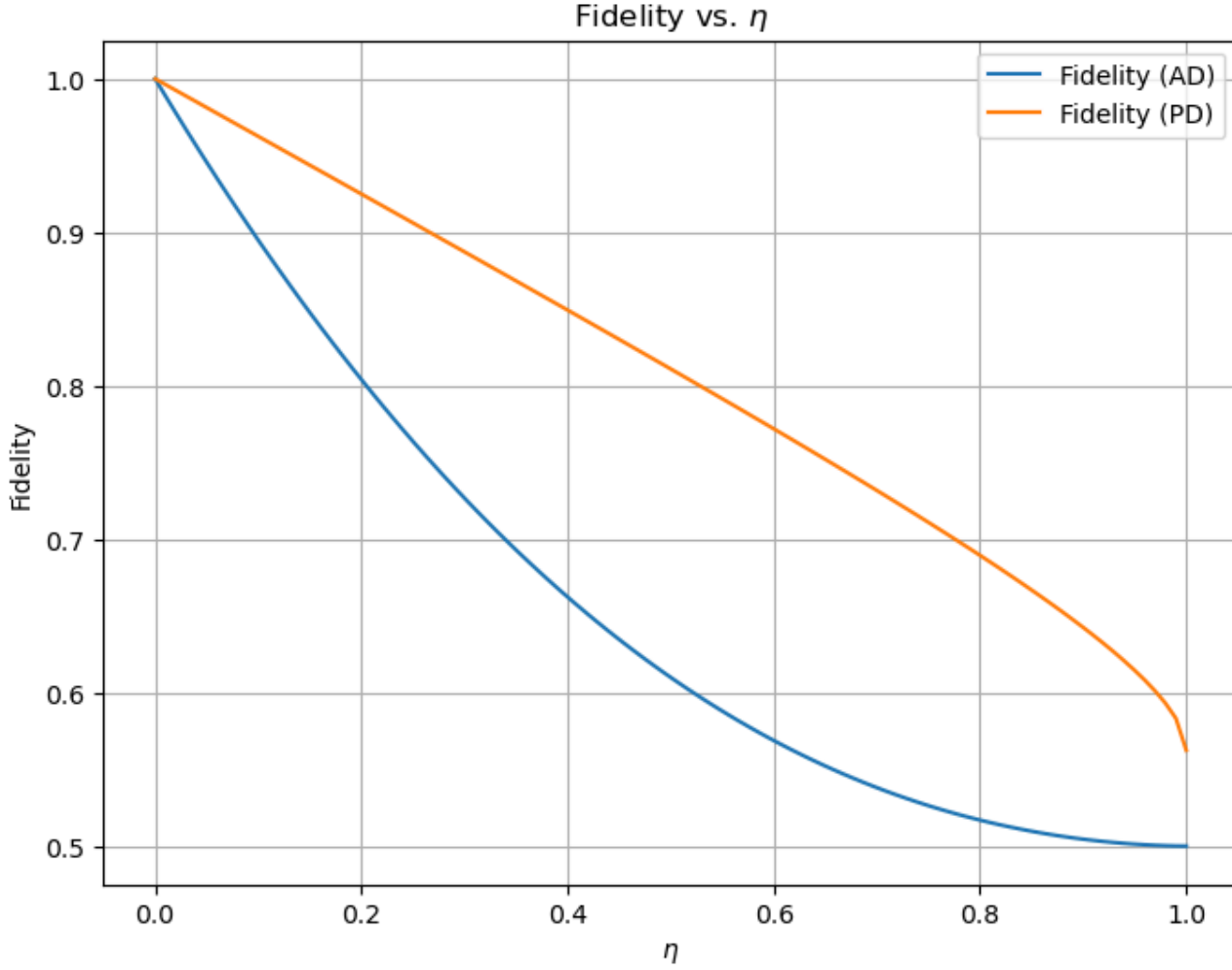
$$F_{CD} = \frac{1}{32} \left( 6 \cos^2(2\theta) \cos(2\Phi) + \sin^2(2\theta)(15 \cos(\Phi) + \cos(3\Phi)) + 5 \cos(4\theta) + 21 \right)$$

The average of the fidelity of the CD noise is calculated by the

$$F_{CD}^{\text{av}} = \frac{1}{64} (15 \cos(\phi) + 6 \cos(2\phi) + \cos(3\phi) + 42)$$

The fidelity of the collective rotation (CR)noise quantum channel noises are calculated by using the below formula and average of the fidelity of the CR noise is calculated by the same formula given by

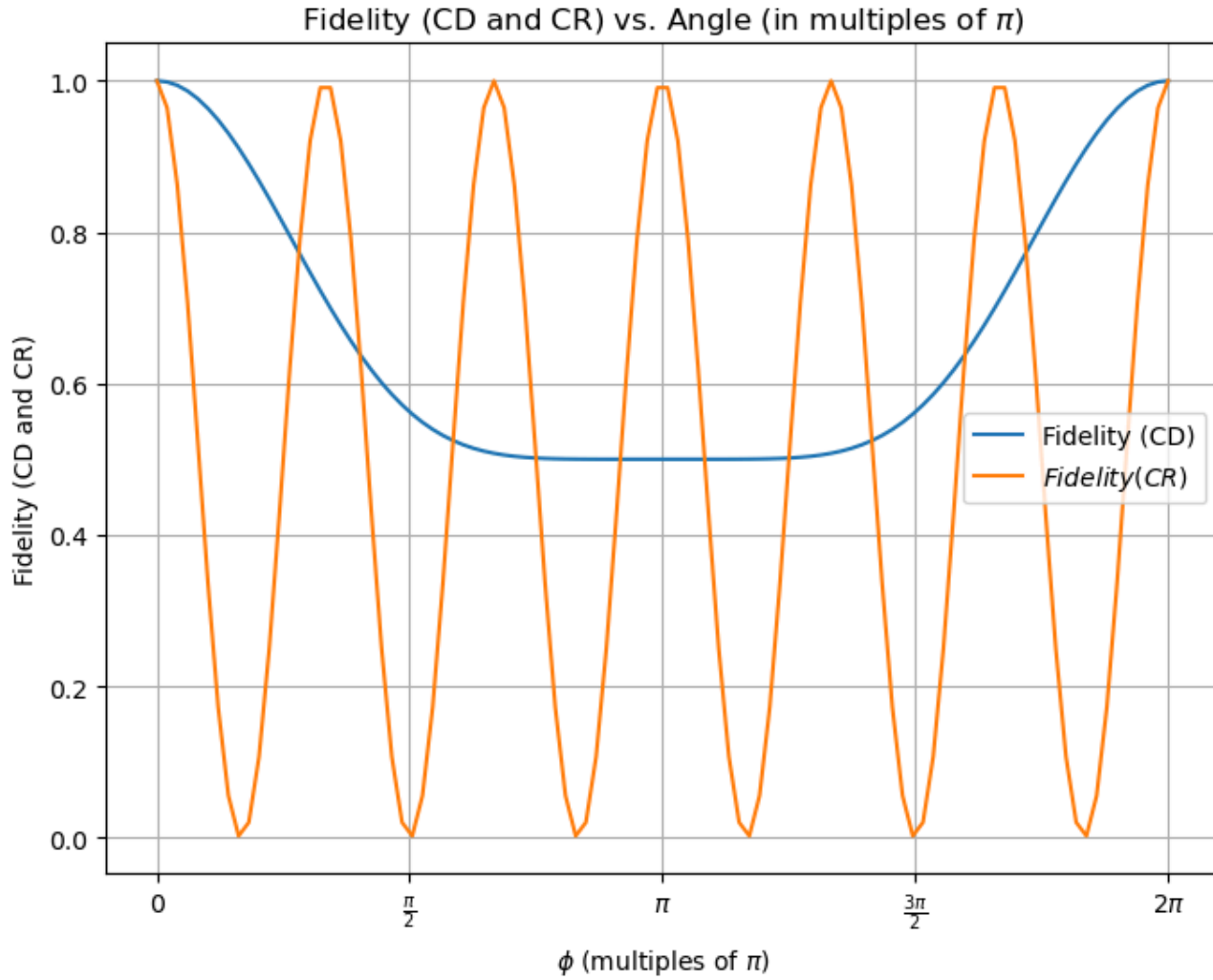
$$F_{CR} = \cos^2(3\Theta)$$



**Fig 4.18:** average fidelity of AD and PD noise parameters is shown in this graph with the decoherence rate .

The average and achieved fidelity over a PD noise channel is superior to that over an AD channel. We can observe in figure 4.18 that the fidelity in case of AD noise is parabolically decreasing faster than the fidelity in case of PD noise channel with the increasing decoherence rate . similarly a related work on CR noise demonstrates that fidelity for CR noise is a periodic function of the noise parameter  $\Theta$  with period  $\pi/3$  and is independent of state characteristics as shown in the figure 4.19. Consequently, the state becomes unaffected for a certain range of values of the noise parameter. Two arbitrary rotation operators commute with one another, which accounts for this characteristic. As might be predicted, the CD fidelity's average value tends towards its lowest value of 0.5 as the  $\Phi$

values increases from 0 to  $2\pi$  the fidelity flattens to 0.5 and then increases to the 1 value in case of the CD noise .

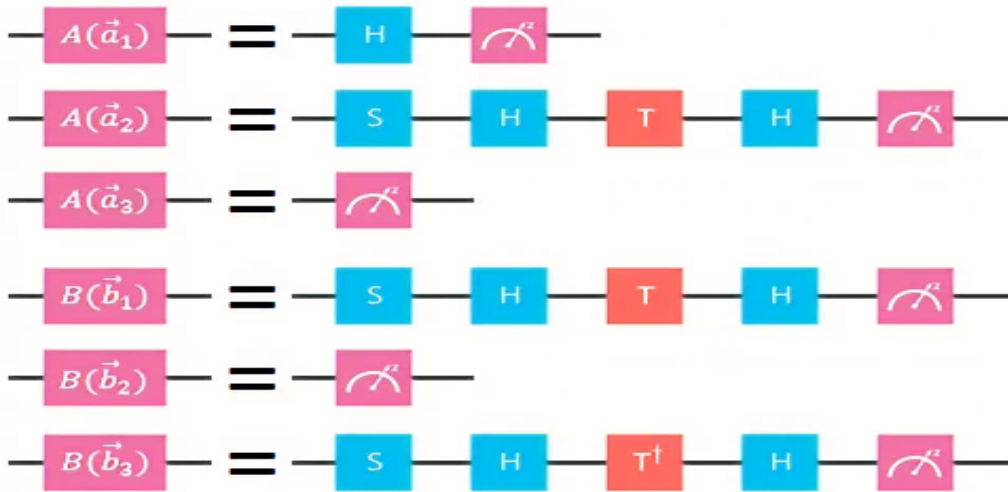


**Fig 4.19:** average fidelity of CD and CR noise parameters , when the quantum state of the qubit is subjected to collective noises.

Based on the analysis of three stage QKD protocol effectiveness across a variety of noise models, it can be concluded that the commutation between the rotation and noise operators, which is the most crucial step in the three-stage protocol, perfectly captures the overall situation.

## 4.6 generation of Bk

The process of generating entangled qubits continues till it completes generating a large number of entangled qubit pairs. One of each entangled qubit pairs are then sent to Alice and Bob respectively. These are then used by the sender and receiver to select the basis for measurement. For each time, both Alice and Bob measure their entangled qubits with any random basis. They then communicate with each other about the basis of measurement used through a classical channel.



**Fig 4.20:** Random measurement basis used by Alice and Bob

Figure 4.6 shows the Random measurement basis used by Alice and Bob . The S gate, sometimes referred to as the phase gate or Z90 gate, performs a rotation of 90 degrees around the z-axis. This gate is named after the angle it rotates the quantum state. Similarly, the T gate, also known as the phase gate or Z45 gate, performs a rotation of 45 degrees around the z-axis. It is named after the angle of rotation it applies to the quantum state. The T dagger gate is the conjugate transpose of the T gate. It is a gate that essentially reverses the effect of the T gate operation on the quantum state.



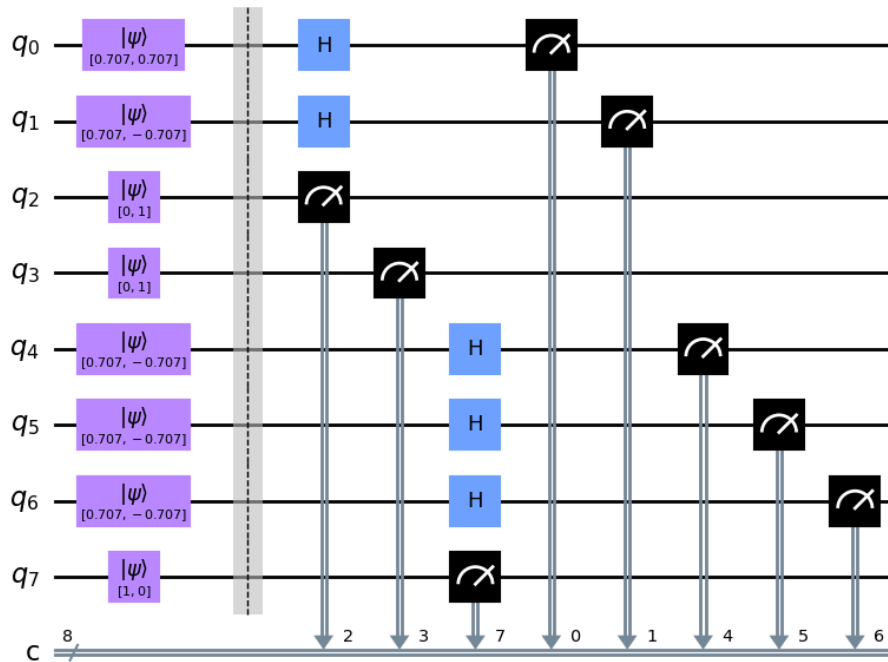


(along the X axis) based on the corresponding values of the Bk bit string, which represents the binary string of the measurement results obtained from the entangled qubits.

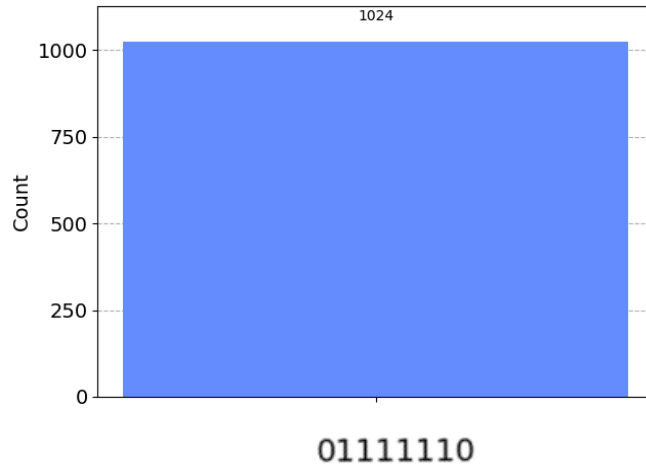
Following the measurement, the obtained results are stored in classical registers for further analysis and processing of the received data. These registers serve the purpose of error checking and facilitate the subsequent decoding of the transmitted message.

```
['01111110', '1101011101001101', '0011010101110011', '1010011011101110', '1100011000110110', '1011011011110110', '10100110', '000101', '01111110']
```

The above image shows the result obtained by Bob after measuring the received qubits.



**Figure 5.1:** Quantum measurement circuit for Start Flag



**Figure 5.2:** Quantum measurement result for Start Flag

In figure 5.1 and figure 5.2, the qubits labeled as q0 to q7 represent the states of the qubits. The specific states of the qubits are determined based on the values of  $A_k[i]$  and  $B_k[j]$ , where  $i$  and  $j$  range from 0 to 7.

Let's break down the initialization of qubit states based on the values of  $A_k[i]$  and  $B_k[j]$ :

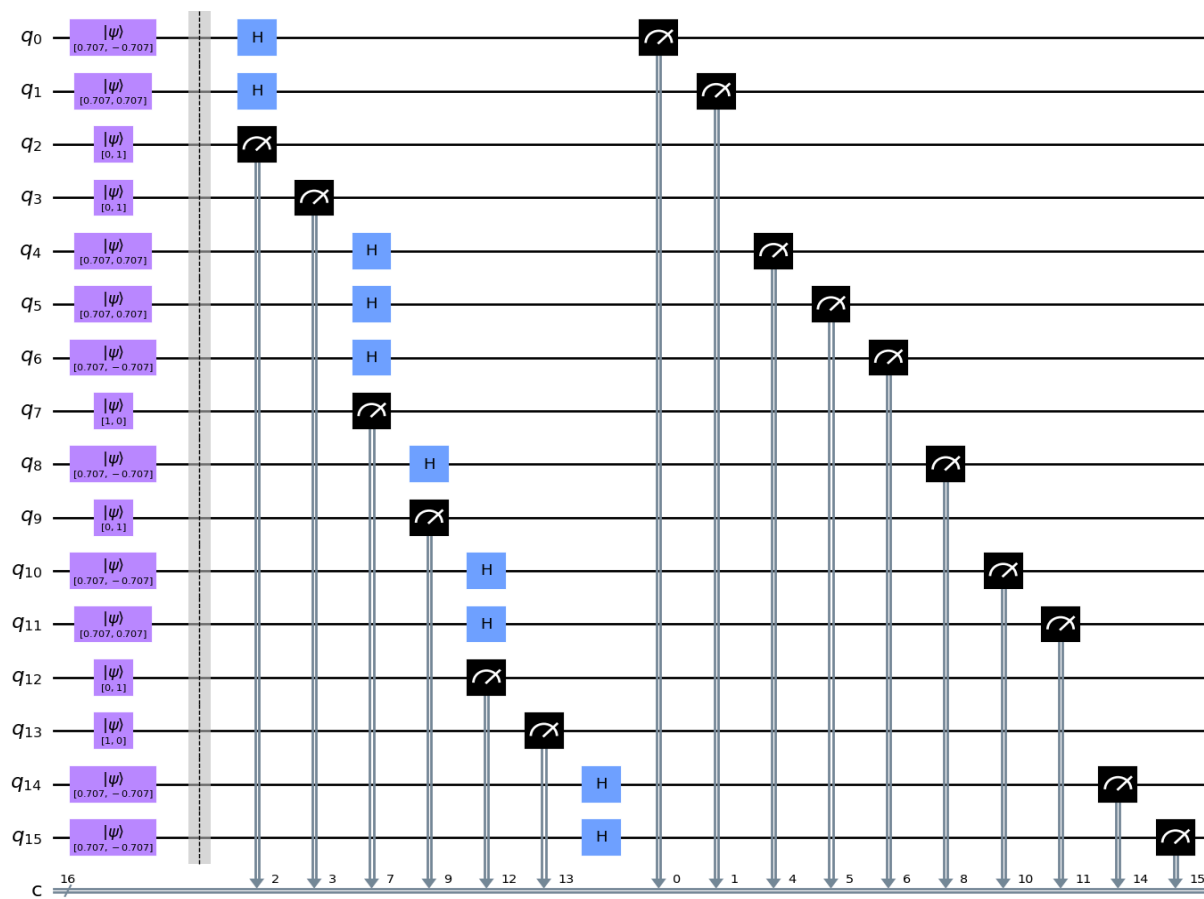
- If  $A_k[i]$  is 0 and  $B_k[j]$  is 0, the qubits are encoded in the '0' state, which can be represented as  $[1, 0]$ .
- If  $A_k[i]$  is 1 and  $B_k[j]$  is 0, the qubits are encoded in the '1' state, which can be represented as  $[0, 1]$ .
- If  $A_k[i]$  is 0 and  $B_k[j]$  is 1, the qubits are encoded in the '+' state, which can be represented as  $[0.707, 0.707]$ .
- If  $A_k[i]$  is 1 and  $B_k[j]$  is 1, the qubits are encoded in the '-' state, which can be represented as  $[0.707, -0.707]$ .

Additionally, if  $B_k[j]$  is 1, the qubits are measured in the X-basis (along the X-axis) using the Hadamard gate and z-basis measurement. On the other hand, if  $B_k[j]$  is 0, the qubits are measured on the Z-basis (along the Z-axis) using a z-basis measurement.

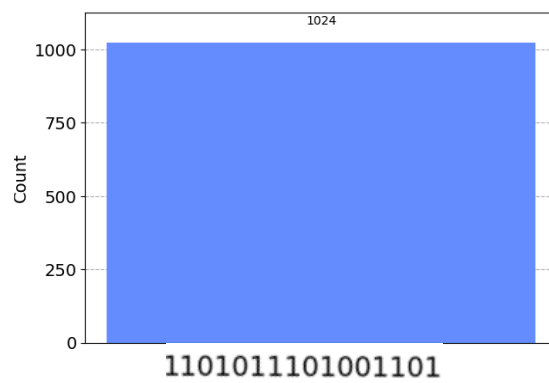
In summary, the qubit states in the circuit are determined by the values of  $A_k[i]$  and  $B_k[j]$ . They are initialized to specific states such as '0', '1', '+', or '-' based on these values. The measurement of the qubits is performed either in the X-basis or the Z-basis, depending on the value of  $B_k[j]$ .

Let's break down the information regarding the states and measurements of qubits in a clearer manner: Firstly,  $A_k[0]$  is 0 and  $B_k[0]$  is 1. As a result, qubit  $q_0$  is in the '+' state, represented as  $[0.707, 0.707]$ . Since  $B_k[0]$  is 1, qubit  $q_0$  is measured in the X-basis (along the X-axis) using the Hadamard gate and z-basis measurement. Moving on,  $A_k[1]$  is 1 and  $B_k[1]$  is 1. This means qubit  $q_1$  is in the '-' state, denoted by  $[0.707, -0.707]$ . Since  $B_k[1]$  is 1, qubit  $q_1$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Next,  $A_k[2]$  is 1 and  $B_k[2]$  is 0. Consequently, qubit  $q_2$  is in the '1' state, which can be represented as  $[0, 1]$ . As  $B_k[2]$  is 0, qubit  $q_2$  is measured in the z-basis measurement.

This process continues for  $A_k[3]$  through  $A_k[7]$  and  $B_k[3]$  through  $B_k[7]$ , determining the states and measurements of the respective qubits.



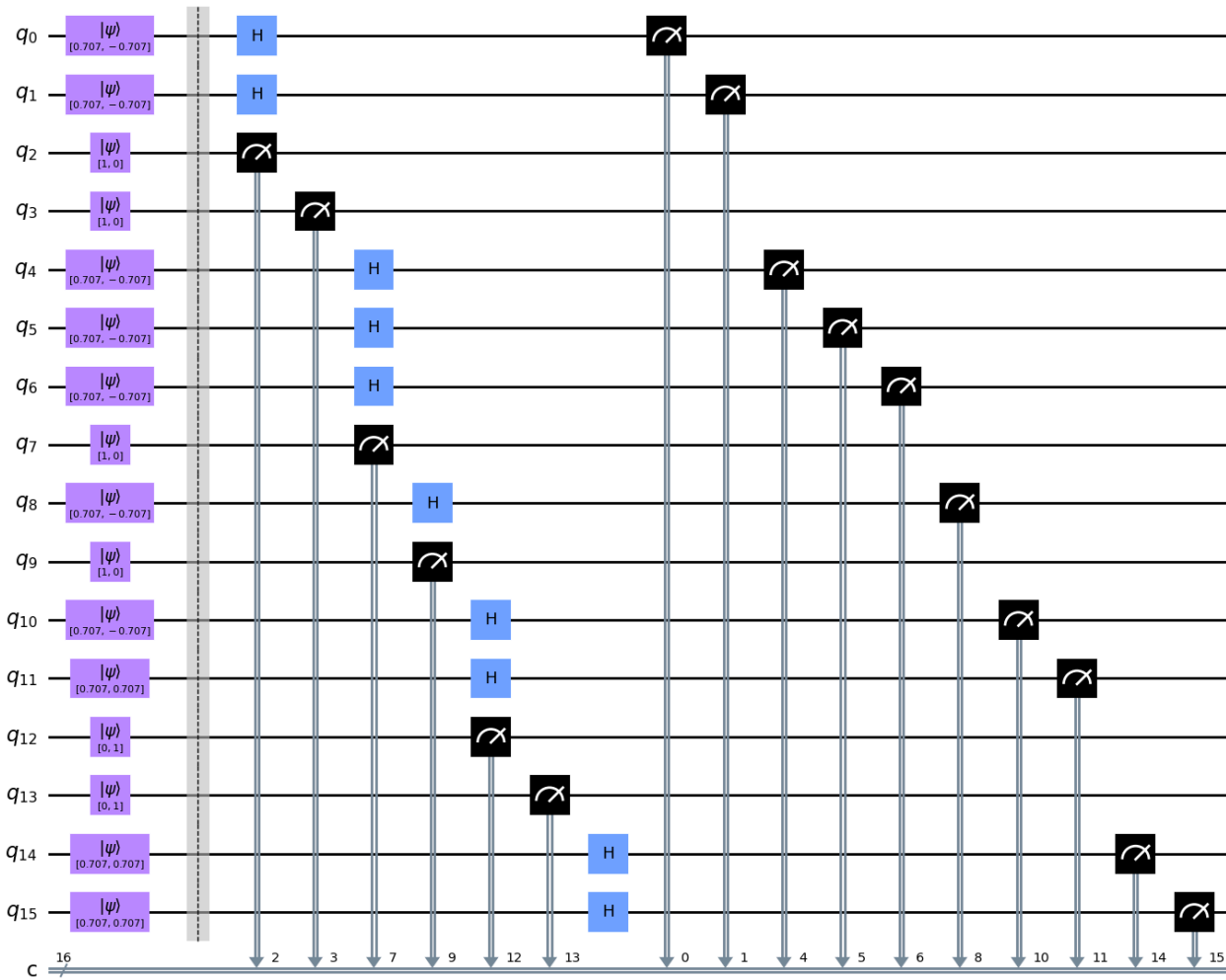
**Figure 5.3:** Quantum measurement circuit for Source IP Address



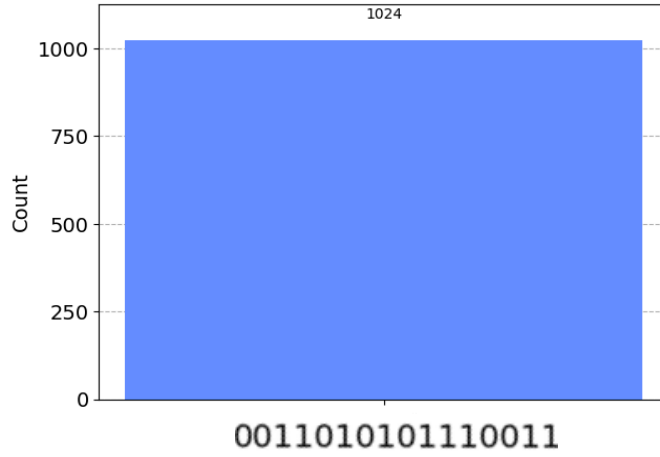
**Figure 5.4:** Quantum measurement result for Source IP Address

In figure 5.3 and figure 5.4 for  $A_k[0]=0$  and  $B_k[0]=1$ , qubit  $q_0$  is in the '+' state represented by  $[0.707, 0.707]$ . Since  $B_k[0]=1$ , qubit  $q_0$  is measured in the X-basis (along the X-axis) using the Hadamard gate and z-basis measurement. Moving on, with  $A_k[1]=1$  and  $B_k[1]=1$ , qubit  $q_1$  is in the '-' state denoted by  $[0.707, -0.707]$ . As  $B_k[1]=1$ , qubit  $q_1$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Similarly, for  $A_k[2]=1$  and  $B_k[2]=0$ , qubit  $q_2$  is in the '1' state, represented as  $[0, 1]$ . Since  $B_k[2]=0$ , qubit  $q_2$  is measured in the z-basis.

This process continues for  $A_k[3]$  through  $A_k[7]$  and  $B_k[3]$  through  $B_k[7]$ , determining the states and measurements of the corresponding qubits.

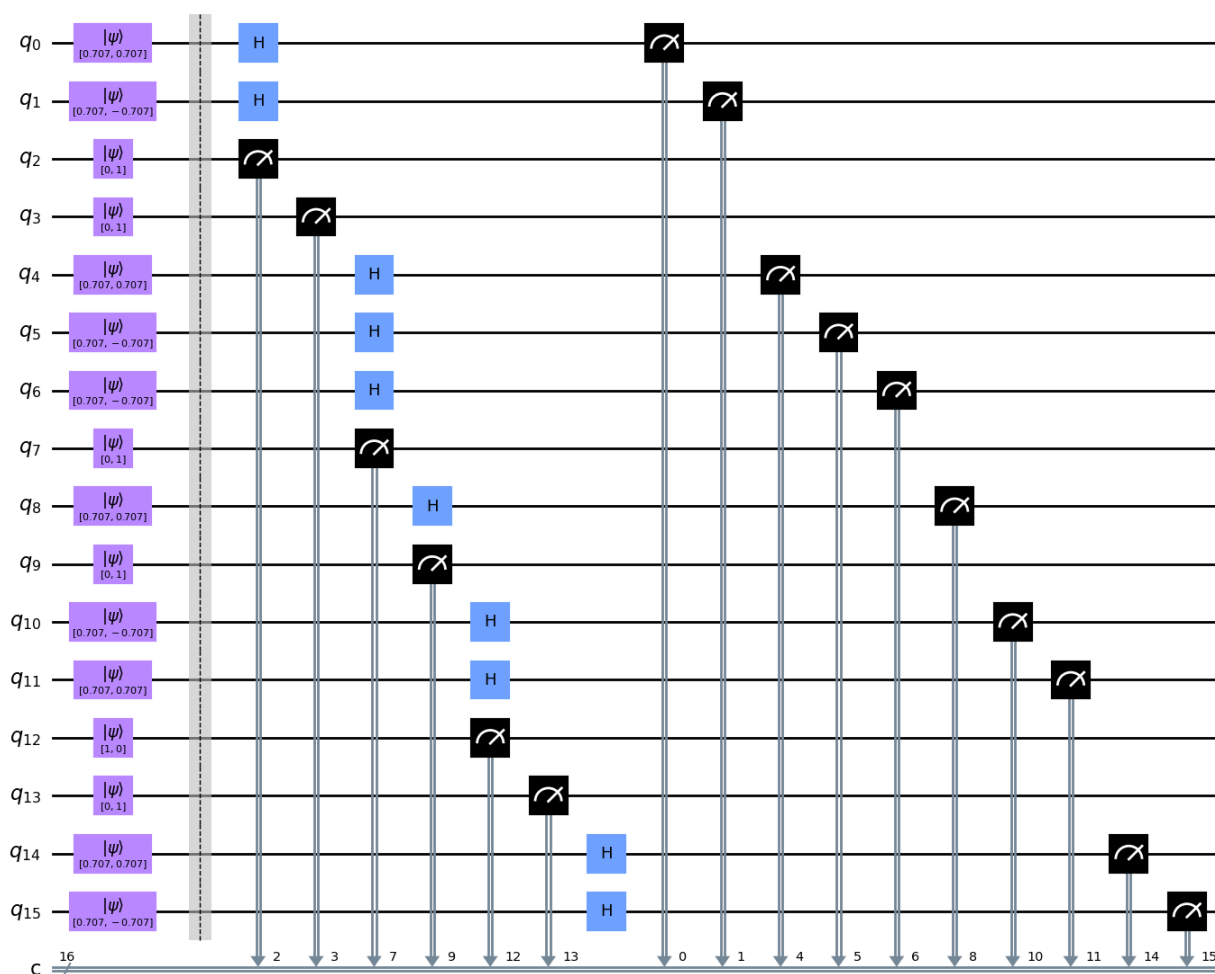


**Figure 5.5:** Quantum measurement circuit for Destination IP Address

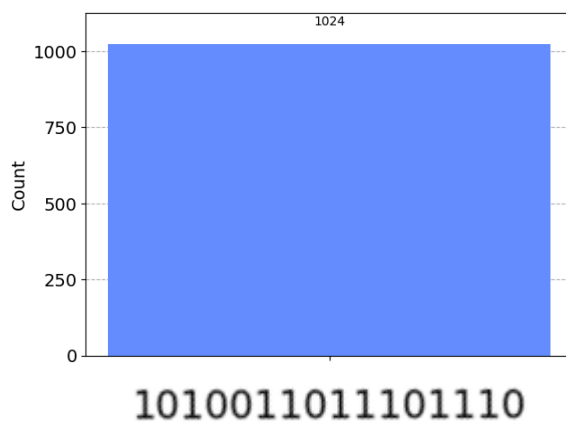


**Figure 5.6:** Quantum measurement result for Destination IP Address

In figure 5.5 and figure 5.6, with  $A_k[8]=1$  and  $B_k[8]=1$ , qubit  $q_0$  is in the '-' state represented by  $[0.707, -0.707]$ . Since  $B_k[8]=1$ , qubit  $q_0$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Moving on to  $A_k[9]=0$  and  $B_k[9]=1$ , qubit  $q_1$  is initialized in the '-' state denoted as  $[0.707, 0.707]$ . As  $B_k[9]=1$ , qubit  $q_1$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Similarly, for  $A_k[10]=1$  and  $B_k[10]=0$ , qubit  $q_2$  is initialized in the '1' state represented by  $[0, 1]$ . As  $B_k[10]=0$ , qubit  $q_2$  is measured using the z-basis measurement. This process continues for  $A_k[11]$  through  $A_k[7]$  and  $B_k[11]$  through  $B_k[7]$ , determining the initialization and measurement of the respective qubits.



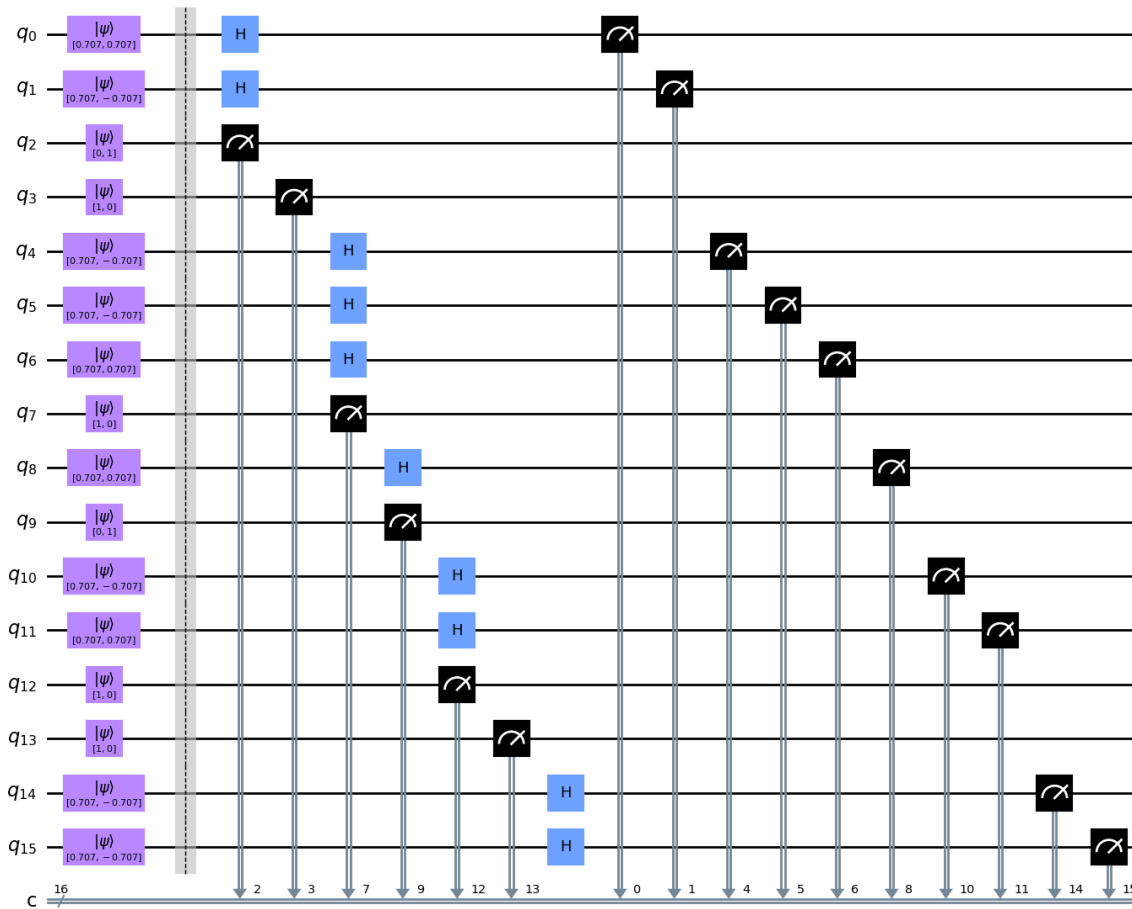
**Figure 5.7:** Quantum measurement circuit for Data Bits (1st and 2nd Character)



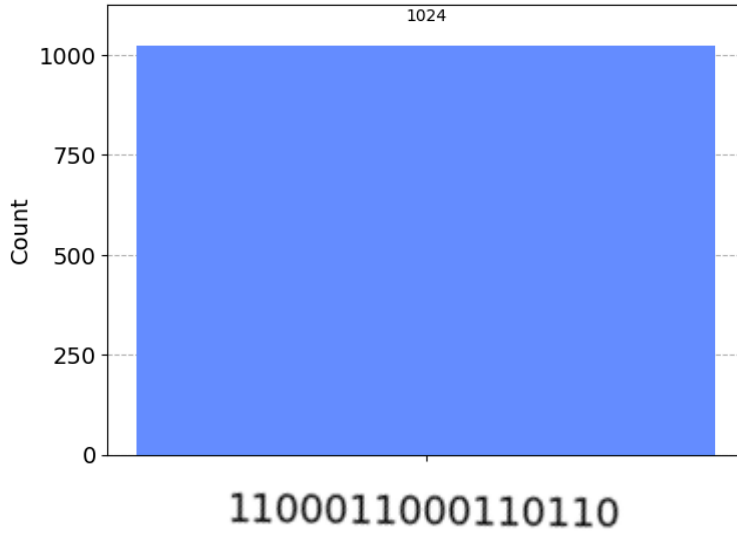
**Figure 5.8:** Quantum measurement result for Data Bits (1st and 2nd Characters)



In figure 5.7 and figure 5.8, for  $A_k[40]=0$  and  $B_k[40]=1$ , qubit  $q_0$  is initialized in the '+' state, denoted as  $[0.707, 0.707]$ . Since  $B_k[40]=1$ , qubit  $q_0$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Moving on to  $A_k[41]=1$  and  $B_k[41]=1$ , qubit  $q_1$  is initialized in the '-' state, represented by  $[0.707, -0.707]$ . As  $B_k[41]=1$ , qubit  $q_1$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Similarly, for  $A_k[42]=1$  and  $B_k[42]=0$ , qubit  $q_2$  is initialized in the '1' state, denoted as  $[0, 1]$ . As  $B_k[42]=0$ , qubit  $q_2$  is measured using the z-basis measurement. This process continues for  $A_k[43]$  through  $A_k[7]$  and  $B_k[43]$  through  $B_k[7]$ , determining the initialization and measurement of the respective qubits.

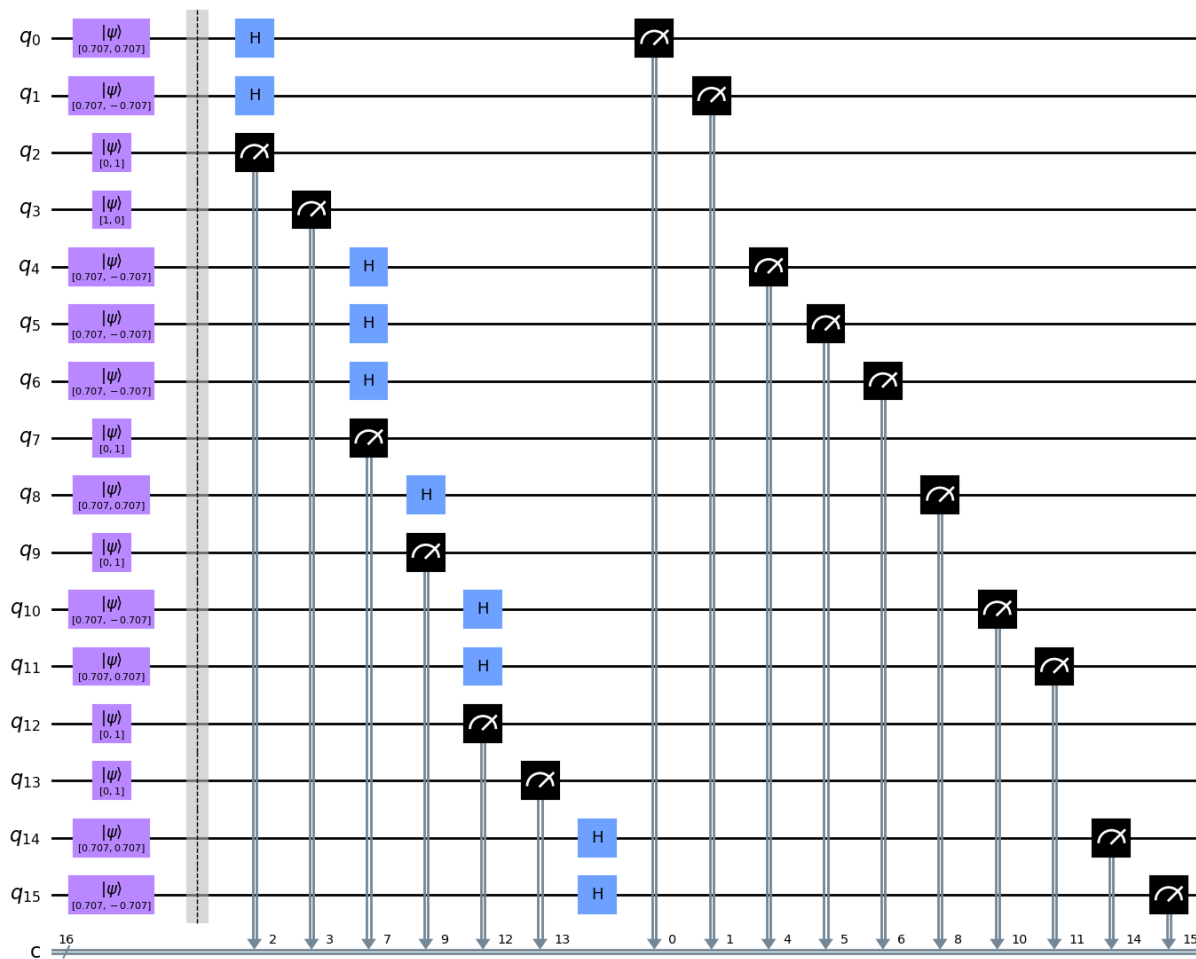


**Figure 5.9:** Quantum measurement circuit for Data Bits (3rd and 4th Characters)

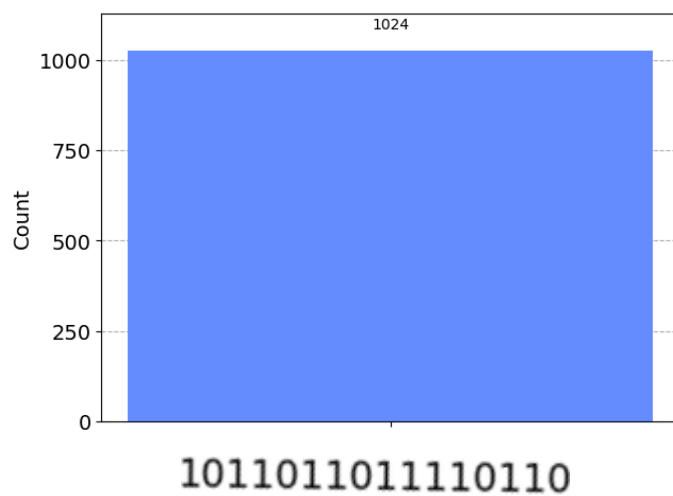


**Figure 5.10:** Quantum measurement result for Data Bits (3rd and 4th Character)

In figure 5.9 and figure 5.10, with  $A_k[56]=0$  and  $B_k[56]=1$ , qubit  $q_0$  is initialized in the '+' state, denoted as  $[0.707, 0.707]$ . Since  $B_k[56]=1$ , qubit  $q_0$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Moving on to  $A_k[57]=1$  and  $B_k[57]=1$ , qubit  $q_1$  is initialized in the '-' state, represented by  $[0.707, -0.707]$ . As  $B_k[57]=1$ , qubit  $q_1$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Similarly, for  $A_k[58]=1$  and  $B_k[58]=0$ , qubit  $q_2$  is initialized in the '1' state, denoted as  $[0, 1]$ . As  $B_k[58]=0$ , qubit  $q_2$  is measured using the z-basis measurement. This process continues for  $A_k[59]$  through  $A_k[7]$  and  $B_k[59]$  through  $B_k[7]$ , determining the initialization and measurement of the respective qubits.

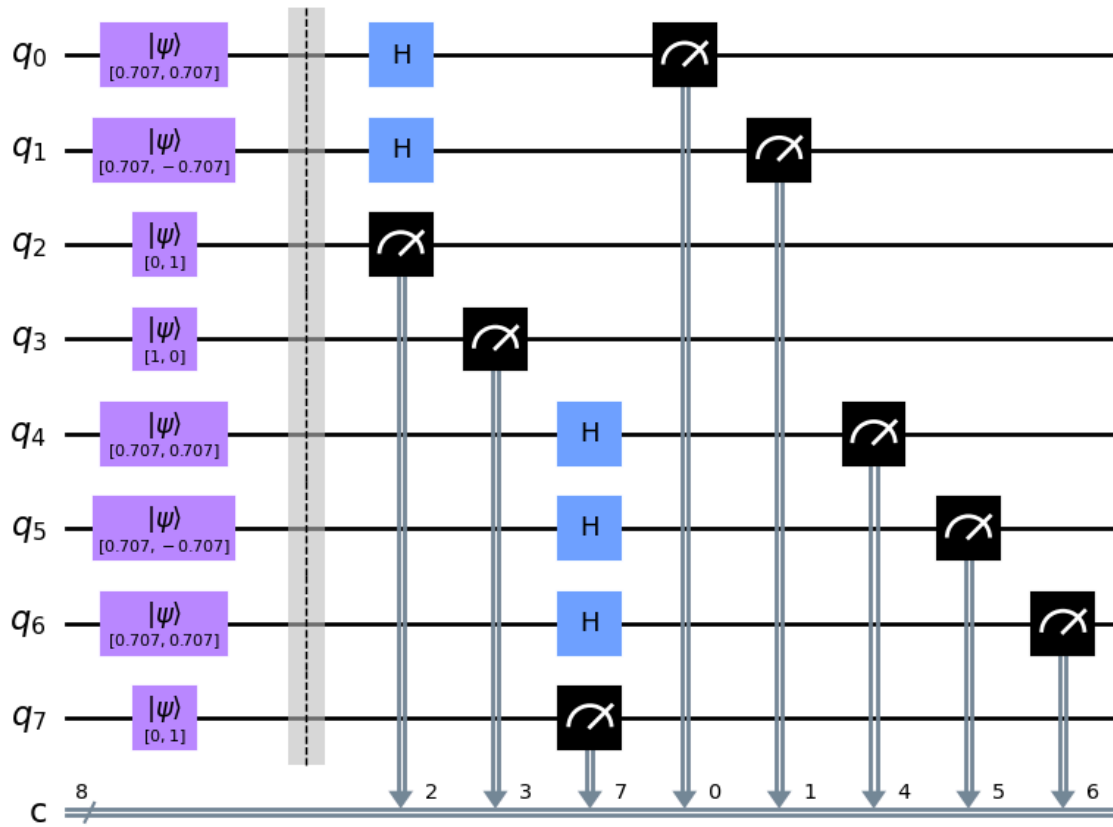


**Figure 5.11:** Quantum measurement circuit for Data Bits (5th and 6th Character)

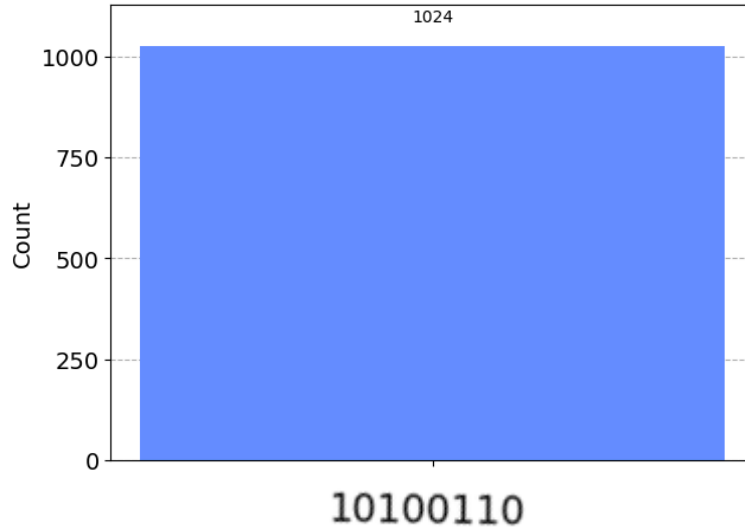


**Figure 5.12:** Quantum measurement result for Data Bits (5th and 6th Character )

In figure 5.11 and figure 5.12, for  $A_k[72]=0$  and  $B_k[72]=1$ , qubit  $q_0$  is initialized in the '+' state, denoted as  $[0.707, 0.707]$ . Since  $B_k[72]=1$ , qubit  $q_0$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Moving on to  $A_k[73]=1$  and  $B_k[73]=1$ , qubit  $q_1$  is initialized in the '-' state, represented by  $[0.707, -0.707]$ . As  $B_k[73]=1$ , qubit  $q_1$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Similarly, for  $A_k[74]=1$  and  $B_k[74]=0$ , qubit  $q_2$  is initialized in the '1' state, denoted as  $[0, 1]$ . As  $B_k[74]=0$ , qubit  $q_2$  is measured using the z-basis measurement. This process continues for  $A_k[75]$  through  $A_k[7]$  and  $B_k[75]$  through  $B_k[7]$ , determining the initialization and measurement of the respective qubits.



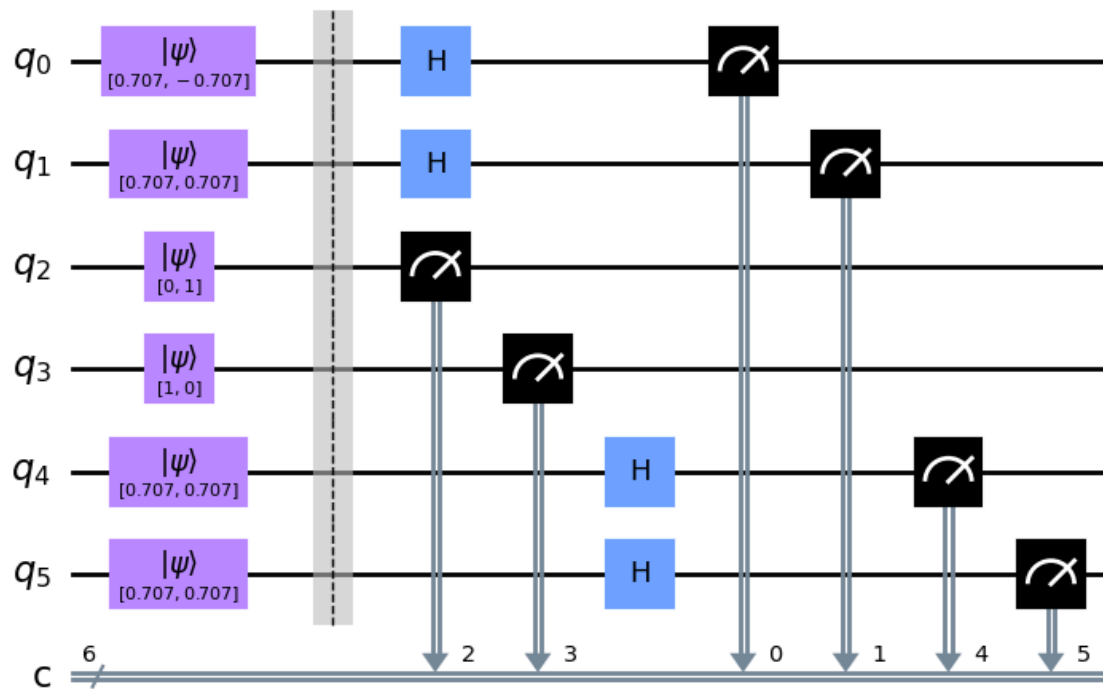
**Figure 5.13:** Quantum measurement circuit for Data Bits (Last Character)



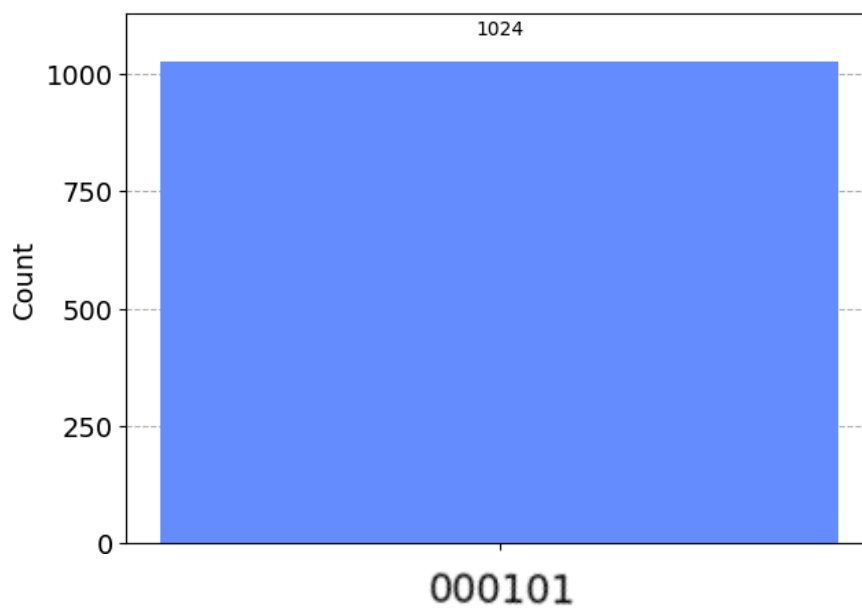
**Figure 5.14:** Quantum measurement result for Data Bits (Last Character)

In figure 5.13 and figure 5.14, for  $A_k[90]=0$  and  $B_k[90]=1$ , qubit  $q_0$  is initialized in the '+' state, represented by  $[0.707, 0.707]$ . Since  $B_k[90]=1$ , qubit  $q_0$  is measured in the X-basis (along the X-axis) using the Hadamard gate and z-basis measurement. Moving on to  $A_k[91]=1$  and  $B_k[91]=1$ , qubit  $q_1$  is initialized in the '-' state, denoted as  $[0.707, -0.707]$ . As  $B_k[91]=1$ , qubit  $q_1$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Similarly, for  $A_k[92]=1$  and  $B_k[92]=0$ , qubit  $q_2$  is initialized in the '1' state, which can be written as  $[0,1]$ . As  $B_k[92]=0$ , qubit  $q_2$  is measured using the z-basis measurement.

This process continues for  $A_k[93]$  through  $A_k[7]$  and  $B_k[93]$  through  $B_k[7]$ , determining the initialization and measurement of the respective qubits.



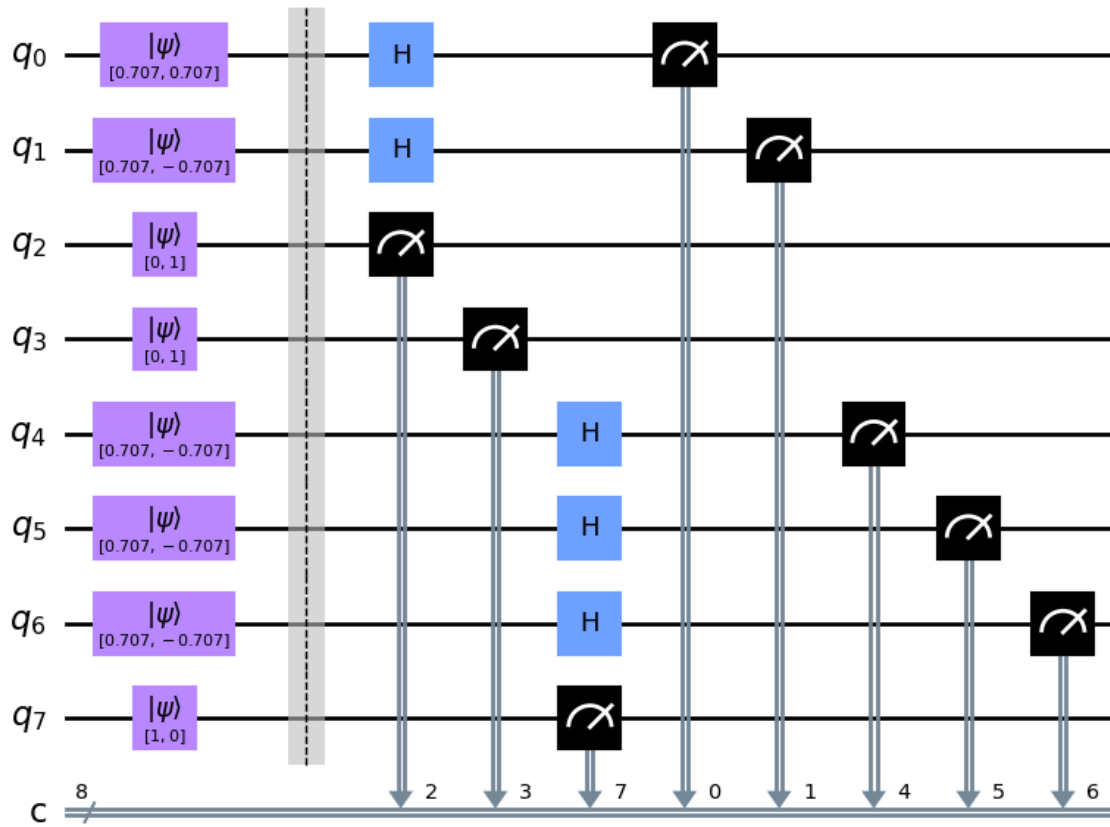
**Figure 5.15:** Quantum measurement circuit for FCS



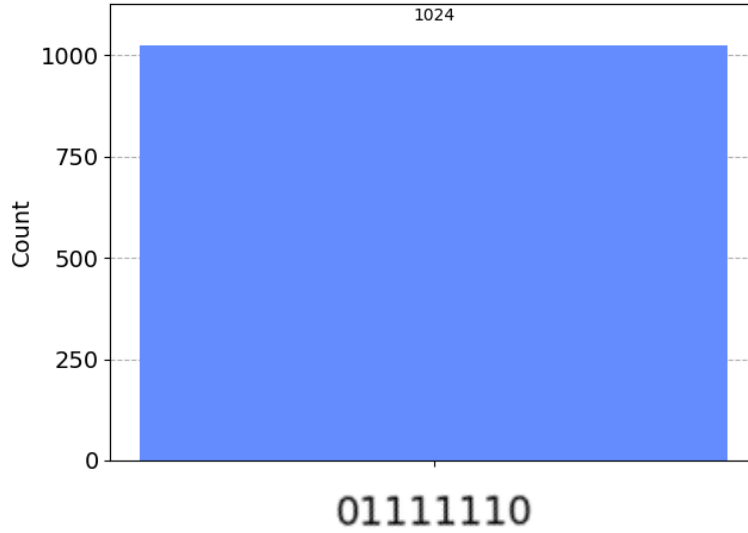
**Figure 5.16:** Quantum measurement result for FCS

In figure 5.15 and figure 5.16, for  $A_k[98]=1$  and  $B_k[98]=1$ , qubit  $q_0$  is initialized in the '+' state, represented by  $[0.707, -0.707]$ . Since  $B_k[98]=1$ , qubit  $q_0$  is measured in the X-basis (along the X-axis) using the Hadamard gate and z-basis measurement. Moving on to  $A_k[99]=0$  and  $B_k[99]=1$ , qubit  $q_1$  is initialized in the '-' state, denoted as  $[0.707, 0.707]$ . As  $B_k[99]=1$ , qubit  $q_1$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Similarly, for  $A_k[100]=1$  and  $B_k[100]=0$ , qubit  $q_2$  is initialized in the '1' state, which can be written as  $[0, 1]$ . As  $B_k[100]=0$ , qubit  $q_2$  is measured using the z-basis measurement.

This process continues for  $A_k[101]$  through  $A_k[7]$  and  $B_k[101]$  through  $B_k[7]$ , determining the initialization and measurement of the respective qubits.



**Figure 5.17:** Quantum measurement circuit for End Flag



**Figure 5.18:** Quantum measurement result for End Flag

In figure 5.17 and figure 5.18, for  $A_k[104]=0$  and  $B_k[104]=1$ , qubit  $q_0$  is initialized in the '+' state, represented by  $[0.707, 0.707]$ . Since  $B_k[104]=1$ , qubit  $q_0$  is measured in the X-basis (along the X-axis) using the Hadamard gate and z-basis measurement. Moving on to  $A_k[105]=1$  and  $B_k[105]=1$ , qubit  $q_1$  is initialized in the '-' state, denoted as  $[0.707, -0.707]$ . As  $B_k[105]=1$ , qubit  $q_1$  is measured in the X-basis using the Hadamard gate and z-basis measurement. Similarly, for  $A_k[106]=1$  and  $B_k[106]=0$ , qubit  $q_2$  is initialized in the '1' state, which can be written as  $[0,1]$ . As  $B_k[106]=0$ , qubit  $q_2$  is measured using the z-basis measurement.

This process continues for  $A_k[107]$  through  $A_k[7]$  and  $B_k[107]$  through  $B_k[7]$ , determining the initialization and measurement of the respective qubits.

## 5.2 CRC Error Checking and Final Message Generation

Upon receiving the qubits through the quantum communication channel and then decrypting it, Bob will employ the cyclic redundancy check (CRC) technique to verify the integrity of the message data. This involves dividing the received data by a predetermined key. If the remainder is zero for all divisions, it confirms that our received data is error-free. Conversely, if the remainder is non-zero, it indicates the presence of errors in the received data.



```
Reminder after division with the data is :['000000']
```

The above image shows the generated reminder after division. The remainder '000000' tells us that the data received by Bob is free of error.

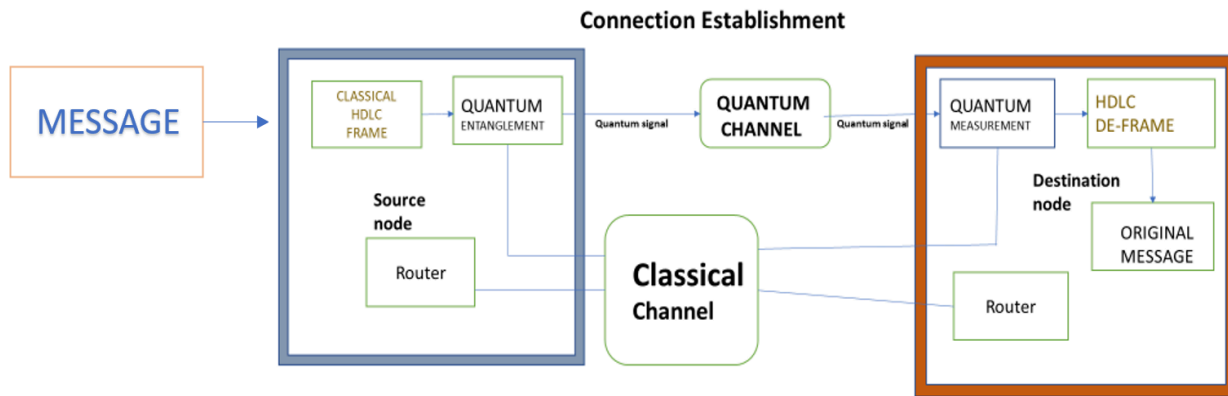
Bob will then employ an ASCII decoder to meticulously transform the binary bit pattern into their respective characters, thus culminating in the retrieval of the message in a coherent and easily understandable form. This crucial step ensures that the transmitted information is effectively decoded and made accessible for further analysis and interpretation.

```
['01110111', '01100101', '01101100', '01100011', '01101111', '01101101', '01100101']  
message received from the sender is : welcome
```

The above image shows the final message that is generated after the binary bits conversion into the ASCII characters.

## **6. CONNECTION DATA COMMUNICATION THROUGH NETWORK**

The successful implementation of quantum data communication in practical scenarios requires the establishment of essential connections between the sender and receiver, as well as necessary connections to obtain entangled qubits. It is crucial to ensure the precise establishment of these connections, as they play a vital role in facilitating seamless and effective data communication in the quantum realm.



**Figure 6.1:** Connection Establishment for Quantum Communication

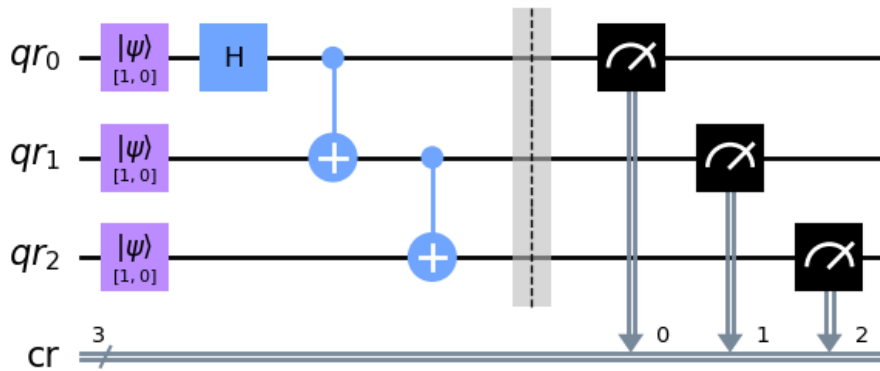
In Figure 6.1 To initiate the process of quantum data transmission, both Alice and Bob begin by sending individual requests for a data path connection link to the Router. These requests are transmitted through a classical channel, which serves as the medium for conventional communication.

Subsequently, Alice and Bob proceed to send their respective requests to Charlie, who possesses the capability to generate entangled pairs of qubits. These entangled qubits are essential for the generation of  $B_k$  bit patterns.

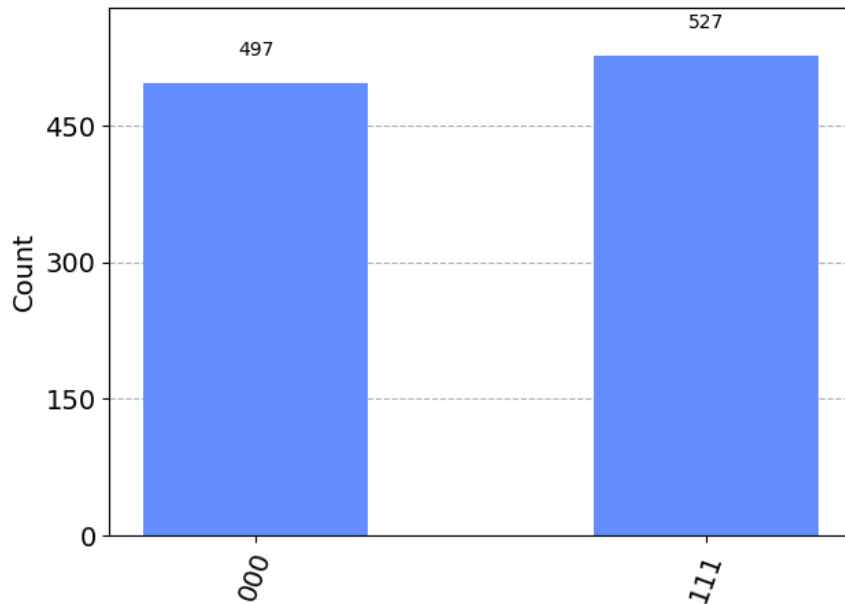
Once Charlie receives the requests from Alice and Bob, he prepares the entangled pairs of qubits and distributes them to both parties. This enables Alice and Bob to establish a synchronized quantum state, facilitating the subsequent transmission of message qubits. For this purpose, a dedicated cable link is employed to ensure a direct, one-to-one communication channel between the two participants.

By following this comprehensive procedure, involving request exchanges and the distribution of entangled qubits, Alice and Bob can establish a robust and reliable quantum data communication pathway. This systematic approach ensures the integrity and efficiency of their quantum communication endeavors.

## 7. DATA COMMUNICATION USING GHZ ENTANGLED QUBITS



**Figure 7.1:** Three Qubit Entanglement Generation Circuit (GHZ).



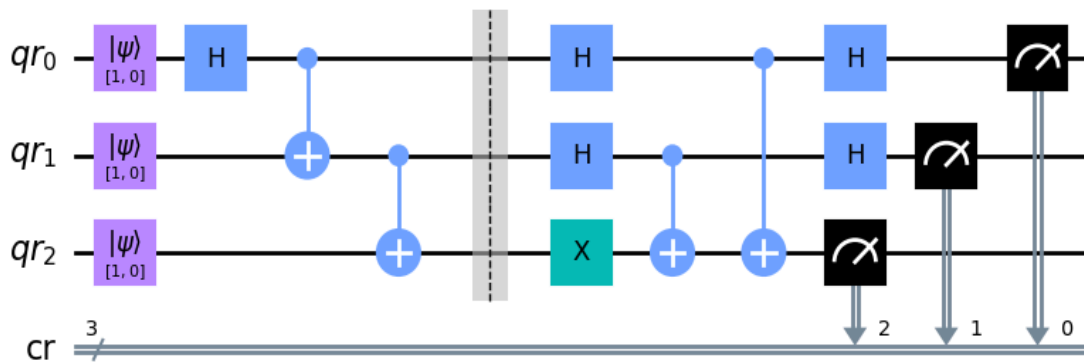
**Figure 7.2:** Three qubit Entanglement Generation circuit measurement result.

In order to generate a state of entanglement among three qubits, we employ the GHZ entanglement circuit. Initially, all three qubits are prepared in the state of zero. To create the entanglement, we apply a series of quantum operations.

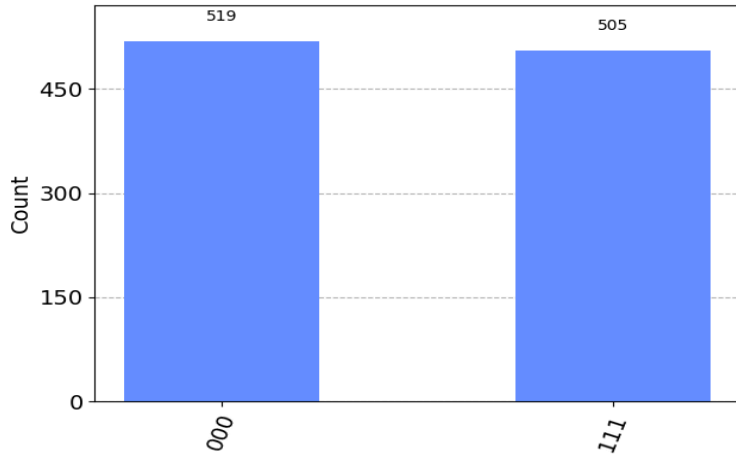
First, a Hadamard gate is applied to the first qubit (qr0), which prepares it in a superposition state. Then, we apply the first controlled-NOT (CNOT) gate, where qr0 serves as the control qubit and qr1 as the target qubit. This gate entangles the first and second qubits together.

Next, we proceed to apply the second CNOT gate. This time, qr1 acts as the control qubit, while qr2 is the target qubit. By doing so, the second and third qubits become entangled as well.

After these operations, all three qubits are entangled together and form an interconnected quantum state. This entangled state is then sent to a sender (S) and two receivers (R1 and R2) for further measurements and observations.



**Figure 7.3:** Three Qubit Entanglement Measurement Circuit (GHZ).



**Figure 7.4:** Three Qubit Entanglement Measurement Result

The process of measurements on a system of three entangled qubits involves the utilization of four Hadamard gates, a Pauli X gate (also known as a NOT gate), and two CNOT gates.

To begin, we apply a Hadamard gate to each of the qubits qr0 and qr1, and a Pauli X gate is applied to the third qubit qr3, effectively flipping its state to establish the desired entanglement pattern. Following that we apply two CNOT gates. The first CNOT gate employs qr1 as the control qubit and qr2 as the target qubit, establishing a correlation between their states. Subsequently, the second CNOT gate is applied with qr0 as the control qubit and qr2 as the target qubit, further enhancing the entanglement between qr0 and qr2.

After the entanglement operations, the qubits qr0 and qr1 undergo another Hadamard gate to further manipulate their states. Subsequently, the final step involves measuring all three qubits in the Z basis. The measurement outcomes provide definitive values that can be interpreted as classical information. Once the measurements are performed, the results obtained by the sender (S) and the two receivers (R1 and R2) exhibit an intriguing property of entanglement. Remarkably, all three parties—S, R1, and R2—obtain identical measurement outcomes. This intrinsic correlation ensures the secure transmission of data utilizing the entangled state of the three qubits. The resulting measurements yield consistent and correlated results for the sender and the two receivers, establishing a robust foundation for secure quantum communication.

## **8. CONCLUSION**

This project demonstrated the integration of classical and quantum techniques in a communication system. By leveraging the properties of entanglement and quantum superposition, secure transmission and efficient data encoding can be achieved. The combination of quantum and classical approaches opens up new possibilities for enhancing communication systems in terms of speed, security, and reliability.

In conclusion, it is important to highlight the significance of data encryption and quantum entanglement in securing communication systems.

The combination of data encryption and quantum entanglement provides a powerful framework for enhancing the security of communication networks. It offers the possibility of secure and reliable data transmission, resistant to eavesdropping and hacking attempts. As quantum technologies continue to advance, the integration of encryption and entanglement will play an increasingly vital role in ensuring the confidentiality and integrity of sensitive information in our interconnected world.

Overall, the project underscores the importance of data encryption and quantum entanglement as key components in the development of secure communication systems, paving the way for advanced encryption techniques and quantum-enabled technologies in the field of data security.

## **9. REFERENCES**

[1] G Arun and Vivekanand Mishra, “A review on quantum computing and communication”

Available: <https://ieeexplore.ieee.org/document/7044953>

[2] Leilei Li, Hengji Li, Chaoyang Li, Xiubo Chen, Yan Chang, Yuguang Yang, and Jian Li, “ The security analysis of E91 protocol in collective-rotation noise channel”

Available: <https://journals.sagepub.com/doi/full/10.1177/1550147718778192>

[3] Martin Giles, “Explainer: What is quantum communication?”

Available: <https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/>

[4] Nicolas Gisin and Rob Thew, “Quantum Communication”

Available: <https://www.nature.com/articles/nphoton.2007.22>

[5] Dimitris Giampouris, “Short Review on Quantum Key Distribution Protocols”

Available: [https://link.springer.com/chapter/10.1007/978-3-319-56246-9\\_12](https://link.springer.com/chapter/10.1007/978-3-319-56246-9_12)

[6] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling, “ Progress in satellite quantum key distribution”

Available: <https://www.nature.com/articles/s41534-017-0031-5>

[7] Anirban Pathak, “Elements of Quantum Computing and Quantum Communication”

[8] Edo Waks, Assaf Zeevi, and Yoshihisa Yamamoto, “ Security of Quantum Key Distribution with Entangled Photons Against Individual Attacks”

Available:

[https://www.researchgate.net/publication/2185340\\_Security\\_of\\_Quantum\\_Key\\_Distribution\\_with\\_Entangled\\_Photons\\_Against\\_Individual\\_Attacks](https://www.researchgate.net/publication/2185340_Security_of_Quantum_Key_Distribution_with_Entangled_Photons_Against_Individual_Attacks)



[9] Taofiq K. Paraiso, Robert I, Woodward, Davide G, Marangon, Victor Lovic, Zhiliang Yuan, and Andrew J. Shields, “ Advanced Laser Technology for Quantum Communication”

Available: <https://onlinelibrary.wiley.com/doi/full/10.1002/qute.202100062>

[10] Siddhartha Roy, and Anushka Ghosh, “ Securing Medical Images Using Quantum Key Distribution Scheme BB84”

Available:

[https://www.researchgate.net/publication/371182928\\_Securing\\_Medical\\_Images\\_Using\\_Quantum\\_Key\\_Distribution\\_Scheme\\_BB84](https://www.researchgate.net/publication/371182928_Securing_Medical_Images_Using_Quantum_Key_Distribution_Scheme_BB84)

### Submission Information

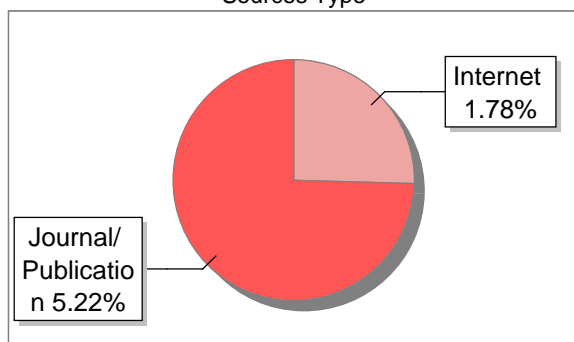
Author Name	Kale Vinay
Title	Entangled two stage QKD project
Paper/Submission ID	1897331
Submitted by	rewa325@tezu.ernet.in
Submission Date	2024-05-29 17:18:31
Total Pages, Total Words	52, 8080
Document type	Dissertation

### Result Information

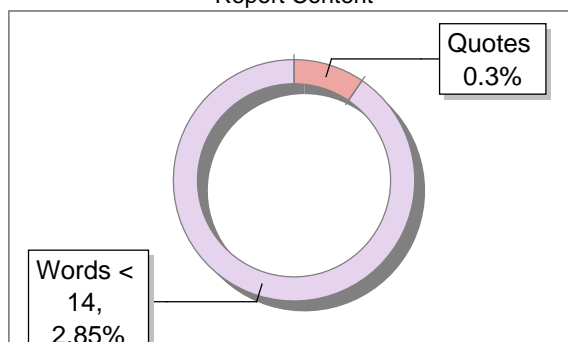
Similarity **7 %**



Sources Type



Report Content



### Exclude Information

Quotes	Not Excluded
References/Bibliography	Excluded
Source: Excluded < 14 Words	Not Excluded
Excluded Source	<b>0 %</b>
Excluded Phrases	Not Excluded

### Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

A Unique QR Code use to View/Download/Share Pdf File



## DrillBit Similarity Report

7

SIMILARITY %

30

MATCHED SOURCES

A

GRADE

A-Satisfactory (0-10%)

B-Upgrade (11-40%)

C-Poor (41-60%)

D-Unacceptable (61-100%)

LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1	<a href="http://www.wireilla.com">www.wireilla.com</a>	2	Publication
2	<a href="http://citeseerx.ist.psu.edu">citeseerx.ist.psu.edu</a>	1	Publication
3	Controlled deterministic secure quantum communication using five-qubit entangled by Xiao-Min-2009	1	Publication
4	Design Steps Toward a 40-kVA SiC JFET Inverter With Natural-Convection by Rabkowski-2013	<1	Publication
5	<a href="http://www.arxiv.org">www.arxiv.org</a>	<1	Publication
6	<a href="http://acm.org">acm.org</a>	<1	Internet Data
7	Green two-tiered wireless multimedia sensor systems an energy, bandwidth, and q by Canberk-2016	<1	Publication
8	<a href="http://moam.info">moam.info</a>	<1	Internet Data
9	<a href="http://images.collegedunia.com">images.collegedunia.com</a>	<1	Publication
10	<a href="http://ca-c.org">ca-c.org</a>	<1	Internet Data
11	<a href="http://eprints.umm.ac.id">eprints.umm.ac.id</a>	<1	Internet Data
12	Dynamics of photoluminescence in medium-size CdSe quantum crystallites, by Lefebvre, P Mathie- 1997	<1	Publication

13	Entanglement Generation Between Two Mechanical Resonators in Two Optomechanical by Rehaily-2017	<1	Publication
14	Quantum Genetic Terrain Algorithm (Q-GTA) A Technique to Study the Evolution of by Sharma-2019	<1	Publication
15	mapyourtech.com	<1	Internet Data
16	www.arxiv.org	<1	Publication
17	A provably secure pairing-free anonymous handover authentication protocol for mo by Ogundoyin-2020	<1	Publication
18	www.arxiv.org	<1	Publication
19	acm.org	<1	Internet Data
20	Automatic TEM image alignment by trifocal geometry by S-2006	<1	Publication
21	Thesis Submitted to Shodhganga Repository	<1	Publication
22	docplayer.gr	<1	Internet Data
23	docplayer.net	<1	Internet Data
24	Limb-girdle muscular dystrophies international collaborations for tr by Thompson-2016	<1	Publication
25	Rapid Detection and Subsequent Isolation of Bioactive Constituents of Crude Plan by Hostettmann-1997	<1	Publication
26	signal.org	<1	Internet Data
27	theoldreader.com	<1	Internet Data
28	Thesis submitted to shodhganga - shodhganga.inflibnet.ac.in	<1	Publication
29	Tribochemistry of bearing steels A new AFM method to study the material - tribo by Jelit-2016	<1	Publication

