Proceedings of 14th IOE Graduate Conference
Peer Reviewed
Year: 2023 Month: December Volume: 14
ISSN: 2350-8914 (Online), 2350-8906 (Print)

Security Analysis of Key Distribution using A Hybrid of Classical and Quantum Channels

Prakash Upadhyaya [a], Nanda Bikram Adhikari [b]

[a, b] *Department of Electronics and Computer Engineering, Pulchowk Campus, IOE, Tribhuwan University, Nepal*
[a] 078mscsk011.prakash@pcampus.edu.np, [b] adhikari@ioe.edu.np

Abstract
Quantum cryptography with its essential features' for enhancing the QKD application can promote the security to make information communication more reliable and trustworthy. Classical channel integrated with quantum channel can utilize both, the credentials of classical channel with principles of quantum physics maintained by quantum channels, can enrich the utilization of QKD. Principles of quantum physics such as quantum entanglement, teleportation of qubits, quantum measurement, principle of polarization, no-cloning theorem and Heisenberg uncertainty principle help for enriching the perception of a hybrid channel consisting of Classical and quantum channels. Such principles are proven to provide advantages on key distribution (also termed as QKD) through various phenomenal analysis provided in different literature followed through completion of this research work. Classical channel embedded with quantum channel can be utilized to achieve more secure communication in a noisy quantum channel using unitary operators, such as Pauli's operators from the given set I, X, Y, Z, in addition with H, Sw, Cx, Toffoli gates. While the research of this work BB84 protocol has been utilized, which uses four polarization states $\{\nwarrow, \nearrow, \uparrow, \rightarrow\}$ and two conjugate bases as shown in Figure 4. The rectilinear basis uses 0° for $|0\rangle$ state and 90° for $|1\rangle$ state. Similarly, diagonal basis uses 45° polarization for $|-\rangle$ state and 135° for $|+\rangle$ state; hence four possible quantum states are considered. The quantum circuits were all run in real quantum computing resources provided by IBM-Q. The analysis of the circuit shows tolerable error for the transmission channel without eavesdropper, but error surpasses the acceptable value while an eavesdropper is interfering in the channel. The proposed methodology utilizes the $|k_a\rangle$ and the $\langle k_b|$ states of GHZ unitary channel resulting in significant improvement in efficiency of key generation: for key length of 200 key generation efficiency is 55.5% for standard-BB84 protocol using the proposed methodology, but during the case for enhanced-BB84 protocol the key generation efficiency is 95%.

Keywords
quantum computing, quantum cryptography, quantum key distribution, hybrid channel, BB84 protocol

1. Quantum Cryptography and Quantum Channel

Quantum cryptography [1], also referred as post-quantum cryptography (PQC) [2], utilizes the properties of quantum mechanics like entanglement, polarization, teleportation, and most importantly superposition of qubits (Figure 1), utilizing unchanging principles of quantum mechanics (quantum physics) instead of depending only on the complexity of factoring large integers.

Quantum key distribution (QKD) uses the principle of quantum mechanics (quantum physics) to maintain the security mechanism for protecting the information. The Heisenberg's uncertainty principle($\Delta x \cdot \Delta P \geq \frac{h}{4\pi}$) [3], the no-cloning theorem [4], and the principle of photon polarization are the main principles of quantum mechanics which are harnessed by QKD protocols. QKD is an application for PQC that utilizes the principles of quantum physics that help to improve the availability, integrity, confidentiality and protect the messages from unauthorized and malicious intruders. Also, as described in [5], quantum public keys are more basic than classical public key and have more potential than private keys. Each measurement disrupts the quantum state of the qubit in the quantum system. Interestingly, sender and receiver, in an unexpected twist, don't rely solely on quantum channels. Instead, they employ an entirely classical approach. They utilize the quantum channel exclusively for transmitting a random sequence of bits, which is essentially a key, as opposed to sending the entire information through it. This is done to facilitate key agreement procedures through classical means. If, at any point, the key becomes compromised or unsettled, it is promptly discarded, and communication is re-established.

The difficulty associated with distributing keys through a combination of classical and quantum channels stems from a lack of security protocols and standardized guidelines for this procedure and the associated equipment. Despite the theoretically robust security features, there remains a requirement for a secure implementation of this technology. As highlighted in the citation [6], asymmetric encryption is notably slower than symmetric encryption. This is why many organizations have adopted a hybrid approach, effectively expediting the key exchange mechanism (KEM). This hybrid method offers a potential means of enhancing information security.

1.1 Classical Channels

In the field of quantum information science [7], a classical information channel, also known as a classical channel, refers to a means of communication that enables the transmission of conventional or classical information. This stands in

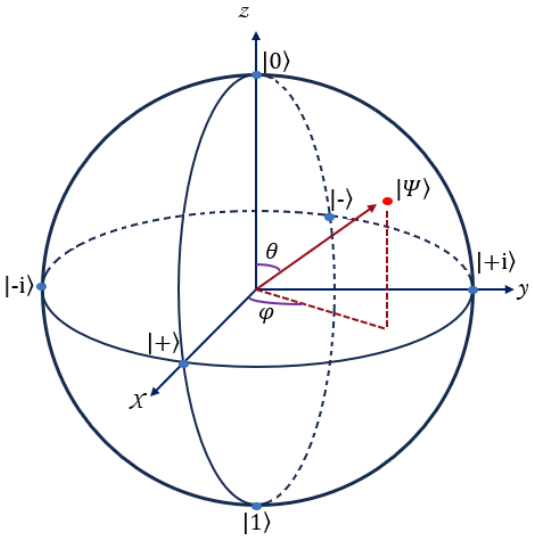

Figure 1: Representation of superposition for qubit in Bloch sphere.

contrast to a quantum channel, which facilitates the transmission of quantum information. One illustration could be the transmission of light through fiber optic lines or the conveyance of electricity across telephone lines.

While classical channels are unable to independently transmit quantum information, they can be advantageous when combined with quantum channels. Some of their applications are:

- In quantum teleportation, quantum information is transmitted between two parties through the combined utilization of a classical channel and a previously prepared entangled quantum state. It is important to note that neither the classical channel nor the previously prepared quantum state can perform this task independently.
- In quantum cryptography, protocols for quantum key exchange make use of both a classical channel and a quantum channel.
- In quantum communication, the utilization of a noise-free classical channel in conjunction with a noisy quantum channel can enhance the information rate of the overall communication system. Specifically, certain highly noisy quantum channels that are incapable of transmitting quantum information when used independently can effectively transmit such information when combined with a classical channel, despite the classical channel's inherent inability to transmit quantum information on its own.

1.2 Quantum Channels

In the realm of quantum information theory, a quantum channel refers to a communication channel that is capable of transmitting both quantum information and classical information. A qubit state serves as an illustration of quantum information, while a text document transmitted over the Internet serves as an example of classical information. Quantum channel is a fundamental concept in quantum communication and quantum computing.

Unlike classical channels that can only transmit classical information, quantum channels allow for the transmission of quantum states. Quantum states are the fundamental units of quantum information and include properties such as superposition and entanglement. A quantum channel can be implemented using various physical systems, such as photons, atoms, or solid-state devices. The specific properties and behavior of the chosen physical system determine the characteristics of the quantum channel. Quantum channels can exhibit different levels of noise and imperfections, leading to a loss or distortion of the transmitted quantum information. This can be caused by factors like decoherence, which refers to the interaction of the quantum system with its environment, leading to the loss of quantum coherence.

Quantum error correction codes and other techniques are used to mitigate the effects of noise and preserve the integrity of quantum information transmitted through quantum channels. These techniques aim to correct errors and protect the delicate quantum states from being destroyed or altered during transmission.

In general, quantum channels play a crucial role in advancing and executing quantum communication protocols, including but not limited to quantum teleportation, quantum key distribution, and post-quantum cryptography (PQC). They provide the means to transmit and manipulate quantum information, enabling advancements in quantum technologies and applications.

The main objective of this article is to present the performance analysis of standard BB84 protocol and the proposed methodology for enhanced-BB84 protocol.

2. Quantum Computing: Qubit!

The qubit, unlike the classical bits which is represented by 0 or 1, can be represented in superposition [8] of both 0 and 1. Thus, qubits impose the property which cannot be distinguished with certainty.

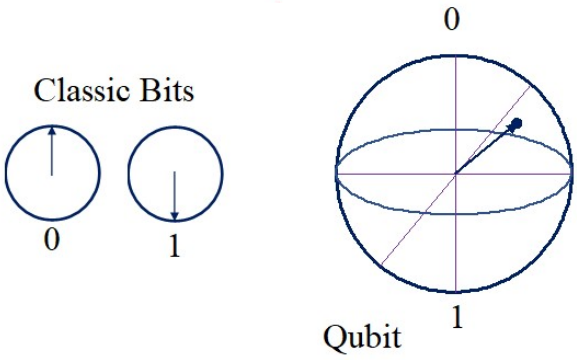

Figure 2: Representation of classical bits and qubit.

The qubits can be represented in the complex superposition

by ket vectors, $|0\rangle$ and $|1\rangle$, where

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} and \;\; |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Thus, a quantum state can be represented as

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

where, α and β satisfies $|\alpha|^2 + |\beta|^2 = 1$.
The state of a qubit can be represented using the Bloch sphere as shown in Figure 1. The symbol θ denotes the polar angle, measured with respect to the positive Z-axis, while ϕ represents the azimuth angle, measured with respect to the positive X-axis. $|\psi\rangle$ signifies any superposition state of the quantum system. The generic equation for the quantum state of a qubit is as follows:

$$|\psi\rangle = cos\theta|0\rangle + e^{i\phi} sin\theta|1\rangle \tag{2}$$

2.1 Quantum entanglement

Quantum entanglement is a phenomenon in quantum mechanics where two or more particles become correlated in such a way that their states are intimately connected, regardless of the distance between them. It is an attribute within quantum physics and quantum computing that, once established, maintains its integrity when influenced by any quantum circuit or quantum channel, expressed mathematically through a unitary operator. In other words, the quantum states of entangled particles are interdependent, and measuring the state of one particle instantly determines the state of the other(s), even if they are separated by vast distances.

When two particles are entangled, the individual states of the particles are no longer well-defined. Instead, the joint state encompasses all possible combinations of the particles' states. However, when a measurement is performed on one of the entangled particles, its state "collapses" into a definite value, instantaneously determining the state of the other particle, regardless of the distance between them.

For example, let's consider a specific entangled state called the Bell state [7]:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) \tag{3}$$

If we measure the state of the first particle and find it to be $|0\rangle$, then the state of the second particle immediately becomes $|1\rangle$. Similarly, if we measure the first particle to be $|1\rangle$, the state of the second particle becomes $|0\rangle$. This instantaneous correlation between the entangled particles is what makes quantum entanglement intriguing and has been experimentally verified in numerous experiments.

3. QKD and BB84 Protocol

The objective of Quantum Key Distribution (QKD) is to create a mutually shared secret key between two entities in a manner that allows the detection of any efforts to eavesdrop or intercept the key. QKD ensures the security of key distribution process, which can then be used for secure communication

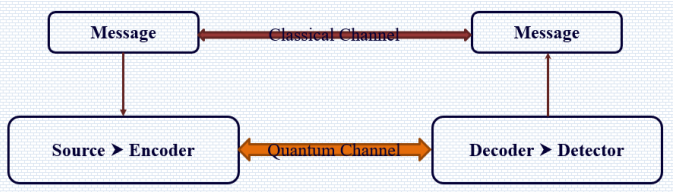

Figure 3: QKD uses the combination of both the classical channels and the quantum channels to establish proper communication channel for secure key transmission.

using traditional cryptographic algorithms. QKD is an application for PQC that utilizes the principles of quantum physics that help to improve the availability, integrity, confidentiality and protect the messages from unauthorized and malicious intruders. According to Heisenberg's uncertainty principle, it is not possible to measure the state of any quantum system without disturbing its state. This principle states that only either the position or the momentum can be measured precisely. While measuring one property, it can randomize another property. According to no-cloning theorem, the perfect copying of quantum state is not possible because the perfect quantum copy machines can't exist which makes the process more secure. The principle of photon polarization provides the mechanism to orient or polarize the light particle to a specific path or direction. A photon filter with correct polarization can detect the specific photons polarized according to the filter or the photon is destroyed.

3.1 BB84 Protocol

The BB84 protocol is the first QKD protocol, proposed by Charles H. Bennet and Gilles Brassard in 1984 [9] and is abbreviated after them. Sender wishes to send a private key to Receiver. She begins with two strings of bits a and b, each n bits long. She then encodes these two strings as a tensor product of n qubits.

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle, \tag{4}$$

where a_i and b_i are the i-th bits of a and b respectively. Together, $a_i b_i$ gives an index into the following four qubit states,
$|\psi_{00}\rangle = |0\rangle$,
$|\psi_{10}\rangle = |1\rangle$,
$|\psi_{01}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$,
$|\psi_{11}\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$,
b_i decides which basis a_i is encoded in: computational (rectilinear) or Hadamard (diagonal).

This protocol uses four polarization states $\{\nwarrow, \nearrow, \uparrow, \rightarrow\}$ and two conjugate bases as shown in Figure 4. The rectilinear basis uses 0° for $|0\rangle$ state and 90° for $|1\rangle$ state. Similarly, diagonal basis uses 45° polarization for $|-\rangle$ state and 135° for $|+\rangle$ state; hence four possible quantum states are considered. By performing comparative analysis between Figure 4 and Figure 5 we can notice, the $|0\rangle$ and $|-\rangle$ represent bit value '0'; similarly the $|1\rangle$ and $|+\rangle$ represent bit value '1'. The bit is encoded in either of these state and if the receiver uses same

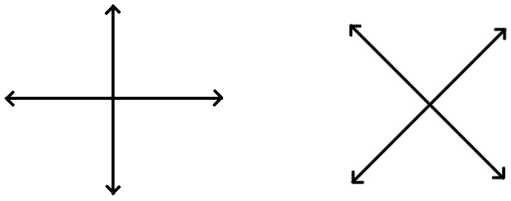

Figure 4: Conjugate bases for creation of polarization states in BB84 protocol.

Table 1: BB84 protocol [9] uses the polarization phenomenon to establish proper quantum state for transmitting the information through quantum channel.

S_x =Sender, R_x=Receiver	BB84 Qubit preparation scheme							
S_x's Bit	0	0	1	1	0	1	1	0
S_x's Base	X	Z	Z	X	Z	X	Z	X
S_x's Polarization Angle	45	0	90	135	0	135	90	45
R_x's Base	X	X	Z	Z	Z	X	X	Z
R_x's Measurement	0	-	1	-	0	1	-	-
Match	*		*		*	*		
Shared Key	0		1		0	1		

basis then a meaningful bit will be generated otherwise random message will be generated.

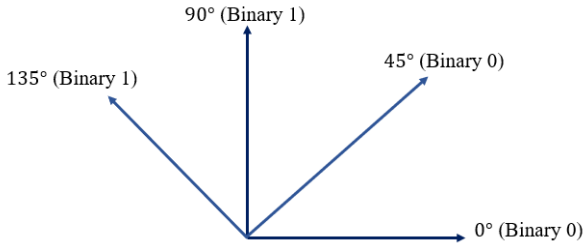

Figure 5: The polarization angle with bit values.

In the BB84 protocol, Sender randomly encodes each bit of the key using one of four possible quantum states(typically represented by two different orthogonal states, such as polarization of lights, or $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Sender then transmits these quantum states to Receiver over a quantum channel. The fundamental idea of the BB84 protocol is to encode every bit of the secret key by utilizing the polarization state of an individual photon. Because attempting to measure the polarization state of a single photon results in its destruction, this information becomes inherently delicate and remains beyond the reach of potential eavesdroppers. Any eavesdropper would be compelled to detect the photon, and in doing so, they would either reveal their presence or be forced to resend the photon. However, in the process of resending the photon, they would inevitably send one with an incorrect polarization state, leading to errors and once again exposing the eavesdropper.

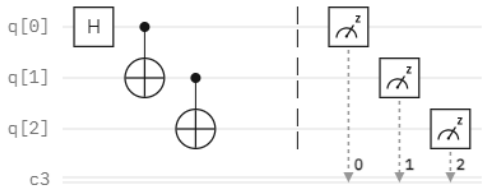

Figure 6: GHZ State is a quantum circuit to produce maximally entangled Bell's equation for $n \geq 3$ qubits.

3.2 GHZ State

A GHZ state is a type of entangled quantum state that involves at least three qubits [10]. The name GHZ is acronym of Daniel Greenberger, Michael Horne and Anton Zeilinger. It is hypothesized that GHZ states, when applied to a significant number of qubits, have the potential to offer superior performance in metrology compared to alternative qubit superposition. The quantum circuit to achieve 3-qubit GHZ state is as shown in Figure 6. The GHZ state for 3 qubits is given as

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

4. Research Methodology

4.1 Quantum Resources

Sending the prepared qubits through quantum channel requires a unitary operator as quantum circuit between sender and receiver. The GHZ state quantum circuit can be used to overcome that challenge and here, in this research it comprises that, $\langle GHZ|GHZ\rangle = I$. Thus, the proposed methodology is as shown in the Figure 7, for the case without any interception by the eavesdropper.

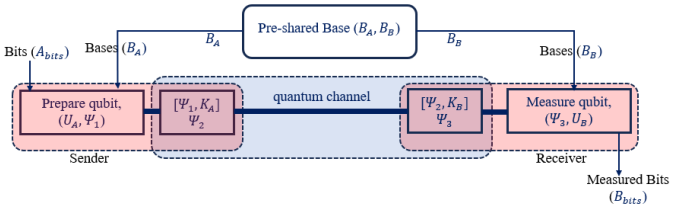

Figure 7: Proposed Methodology includes a combination of GHZ-state unitary circuit for dedicated quantum channel between sender and receiver: $K_A = |GHZ\rangle$ and $K_B = \langle GHZ|$.

While in the case where the eavesdropper is intervening the communication channel, the principles of quantum physics does not allow to replicate the initial quantum state. Later, the receiver yields a different result, as demonstrated in Figure 8. Thus making the presence known to both sender and receiver during key verification process.

4.2 Qubit Preparation

Sender initially prepares qubit (encode bits into photons) which is then sent to Receiver through the quantum channel.

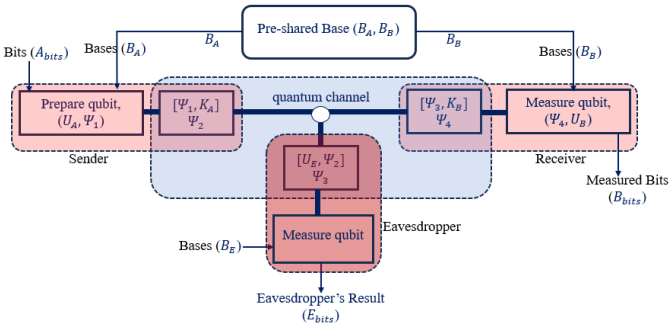

Figure 8: Here, the receiver intercepts a totally random measurement than the original, in presence of eavesdropper. Key verification process is done by utilizing the classical channel.

As already mentioned, the secure quantum channel between Sender and Receiver includes the unitary operator of GHZ state as mentioned in Figure 10. Sender prepares qubit in either of two basis: rectilinear basis (Z) and diagonal basis (X). Further, in rectilinear basis (Z) bit 0s are encoded into H-polarized photon (0°) while the bit 1s are encoded into V-polarized photon (90°). Similarly, in diagonal basis (X), bit 0s are encoded into D-polarized photon (45°), and bits 1s are encoded into A-polarization (135°), as shown in Table 1. In our work, the proposed enhanced-BB84 protocol works accordingly as mentioned below:

1. Initially, Sender and Receiver agree to share a small sequence of polarization bases.
2. The factor for meeting the key length is defined.
3. Sender randomly generates the bits for required key length, and the bases using the pre-shared bases and factor.
4. Sender prepare qubit in one of two mutually unbiased bases: the rectilinear basis (in the states $|0\rangle$ and $|1\rangle$) and the diagonal basis (in the states $|+\rangle$ and $|-\rangle$).
5. Sender embeds its portion of GHZ channel, i.e. K_A in the prepared qubits, and then sends it to Receiver.
6. Receiver in its side embeds its portion of GHZ channel, i.e. K_B.
7. Receiver generates the required measurement basis, using pre-shared basis and factor for meeting key length, and for each qubit.
8. Receiver measures the qubits using the generated basis: rectilinear or diagonal.
9. Sender and Receiver publicly announce the bases they used for each qubit.
10. Receiver discard the qubits measured in the wrong basis.
11. Sender and Receiver performs error correction and privacy amplification procedures to remove errors and ensure secrecy of the final key.

4.3 Quantum Teleportation

The quantum circuits for the proposed methodology for quantum transmission without any eavesdropper can be observed, and are similar as shown in Figure 10. And the quantum circuits for quantum transmission with presence of an eavesdropper can be observed, and are similar as shown in Figure 11. The quantum circuit for other basis and bits (to be transferred) have differing circuit elements for different polarization angles while qubit preparation.

Similar as in the quantum circuits for communication between sender and receiver in presence of eavesdropper, likewise analysis can be done for checking the accuracy of result measured by eavesdropper only. In such case, the receiver's end is discarded and the circuit looks like Figure 14.

5. Result Analysis

Various observations were run in IBM Q quantum resources to analyze the performance of the QKD protocol proposed in this research work. In this research work, there is prepared a unitary operator using the circuit of GHZ-state to create a unitary quantum channel between Sender and Receiver. The

Name	Qubits	EPLG	CLOPS	Status
ibm_brisbane	127	1.9%	5K	Online
ibm_osaka	127	2.8%	5K	Online
ibm_kyoto	127	3.6%	5K	Online

Figure 9: The list of backend real quantum computer each from IBMQ(hub='ibm-q', group='open', project='main') available to access for created account. Source: https://quantum-computing.ibm.com/services/resources?view=table.

use of enhanced-BB84 protocol is done for preparing qubit whereas unitary 3-GHZ state $|GHZ\rangle$ is used for establishing quantum channel. The QKD protocol we are analyzing is as mentioned in the proposed framework (Figure 7) for a hybrid of classical and quantum channels.

Initial state (bit 0):

$$|\psi\rangle = |000\rangle \tag{5}$$

Qubit Preparation:
If base is rectilinear basis (Z) U_{Bz} and bit is 0:

$$|\psi_1\rangle = U_{Bz}|\psi\rangle$$

If base is Z and bit is 1:

$$|\psi_1\rangle = U_{Bz}X|\psi\rangle$$

If base is diagonal basis (X) U_{Bx} and bit is 0:

$$|\psi_1\rangle = U_{Bx}H|\psi\rangle$$

If base is X and bit is 1:

$$|\psi_1\rangle = U_{Bx}XH|\psi\rangle$$

Channel Entanglement:
$|GHZ\rangle$ embedding is done with $|\psi_1\rangle$ by the sender for quantum teleportation:
The new state becomes:

$$|\psi_2\rangle = |GHZ\rangle|\psi_1\rangle \tag{6}$$

Note that $\langle GHZ|GHZ\rangle = I$ is only known to sender and receiver.

Measurement Without Eavesdropper:
Receiver prepares embedded $|GHZ\rangle$ with $\langle GHZ|$ that gives:

$$\begin{aligned} |\psi_3\rangle &= \langle GHZ||\psi_2\rangle \\ &= \langle GHZ|GHZ\rangle|\psi_1\rangle \\ &= |\psi_1\rangle \end{aligned} \tag{7}$$

$|\psi_1\rangle$ state can be observed as the measurement basis used by receiver: If base is rectilinear U_{Bz}, receiver measures:
For bit 0:

$$|\psi_{receiver}\rangle = U_{Bz}|\psi\rangle = |\psi\rangle$$

For bit 1:

$$|\psi_{receiver}\rangle = U_{Bz}X|\psi\rangle = X|\psi\rangle$$

If base is diagonal U_{Bx}, receiver initially applies H-gate, i.e.:

$$|\psi_4\rangle = H|\psi_3\rangle = H|\psi_1\rangle$$

Then receiver measures:
For bit 0:

$$|\psi_{receiver}\rangle = U_{Bx}|\psi_1\rangle = H|\psi\rangle$$

For bit 1:

$$|\psi_{receiver}\rangle = U_{Bx}X|\psi_1\rangle = XH|\psi\rangle$$

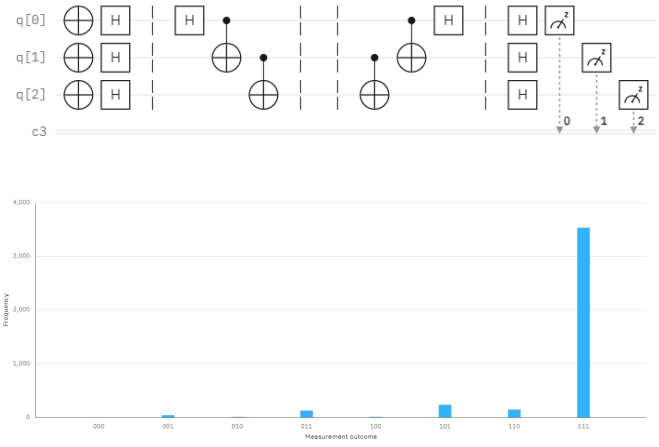

Figure 10: Quantum circuit for communication between Sender and Receiver for transmitting bit 1 with diagonal basis, without any intervention of eavesdropper.

Measurement With Eavesdropper:
Illustration of different measurement of receiver when the eavesdropper is present has been illustrated. Let's assume that

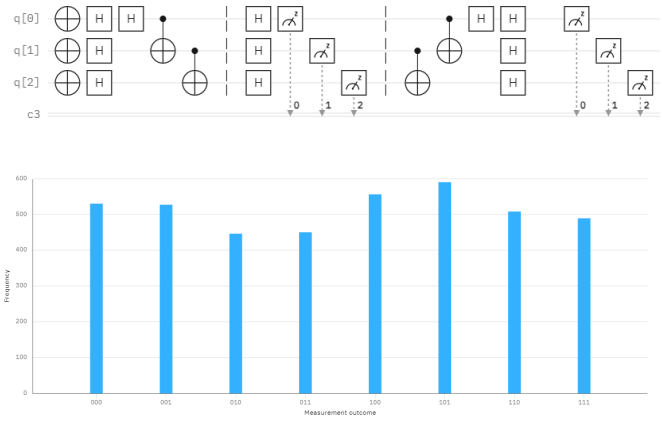

Figure 11: At the receiver end measures a completely different outcomes due to the presence of eavesdropper. Here the circuit is supposed to transport bit 1 in diagonal basis.

eavesdropper uses same bases as the sender and receiver does. In spite of that intruder measures a totally different outcomes due to presence of $|GHZ\rangle$ in equation 6, i.e.

$$|\psi_2\rangle = |GHZ\rangle|\psi_1\rangle$$

Unknown of this eavesdropper will apply its base $U_{intruder}$ while measurement as

$$\begin{aligned} |\psi_{intruder}\rangle &= U_{intruder}|\psi_2\rangle \\ &= U_{intruder}|\psi_1\rangle|GHZ\rangle \\ &\neq |\psi_1\rangle \end{aligned} \tag{8}$$

Thus eavesdropper won't have access to any information encoded in the photon.

In other hand receiver yields different results while the eavesdropper has changed the state of photon with its measurement operator $U_{intruder}$. Receiver during measurement applies its $\langle GHZ|$ to the $|\psi_{intruder}\rangle$ to obtain:

$$\begin{aligned} |\psi_{receiver}\rangle &= \langle GHZ||\psi_{intruder}\rangle \\ &= \langle GHZ|U_{intruder}|\psi_1\rangle|GHZ\rangle \\ &= U_{intruder}|\psi_1\rangle \\ &\neq |\psi_1\rangle \end{aligned} \tag{9}$$

Hence the receiver can easily know the presence of eavesdropper $U_{intruder}$ in the communication channel between sender and receiver.

5.1 Transmission without presence of Eavesdropper

The quantum transmission circuit without interference is shown in Figure 10. While measurement in such channel, i.e. without eavesdropper, maximum error rate of around 15% is obtained as shown in Table **??** and corresponding bar graph is shown in Figure 12. The presence of error is mostly due to noise in quantum hardware which are tolerable errors, and is mostly due to use of H, X, C_x gates. One major criteria is that the encoded bit can be measured successfully once we set the acceptable error rate and that depends upon the quantum computing resources in which the task is being performed. Hence, it can be concluded that there is not any kind of interference.

Table 2: Averaged sample observation of receiver measurements, without any presence of eavesdropper.

Base	Bit	0_counts	1_counts	error(%)
0	0	3851.25	244.75	5.975341797
0	1	611.5	3484.5	14.92919922
1	0	3906.75	189.25	4.620361328
1	1	569.25	3526.75	13.89770508

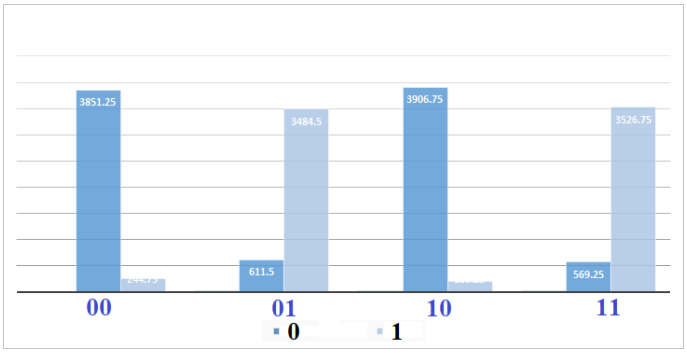

Figure 12: Bar graph to represent data in Table **??**.

5.2 Transmission with presence of Eavesdropper

The quantum transmission circuit with presence of eavesdropper is shown in Figure 11.

While measurement in such channel, i.e. with presence of eavesdropper, high error rate can be observed, with minimum error rate of around 55% is obtained as shown in Table **??** and corresponding bar graph is shown in Figure 13.

Although the error due to noise in quantum hardware are tolerable errors, there is high error rate during presence of eavesdropper due to the disturbance made by the eavesdropper in the channel. the errors are beyond acceptable range and it can be concluded that there is presence of eavesdropper in the channel.

5.3 Measurements for Eavesdropper

While measuring the probable outcomes, even when the eavesdropper uses same basis for measurement, it can be seen that the error rate is higher than the threshold value for the tolerable error as observed in Table **??**.

The errors are because of the addition of GHZ unitary channel handler for sender ($\langle GHZ|GHZ\rangle = I$, unitary operator) through the communication channel.

Table 3: Averaged sample observation of receiver measurements, in presence of eavesdropper.

Base	Bit	0_counts	1_counts	error(%)
0	0	1856.5	2239.5	54.67529297
0	1	2281.25	1814.75	55.69458008
1	0	507	3589	87.62207031
1	1	3603.25	492.75	87.9699707

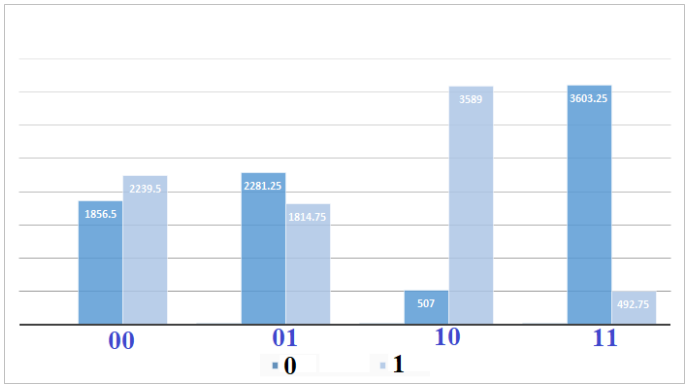

Figure 13: Bar graph to represent data in Table **??**.

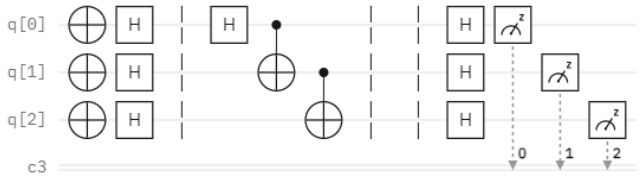

Figure 14: Qubit transmission circuit for bit 1 encoded with diagonal basis, while observing the measurement of the eavesdropper.

5.4 Key Agreement and Efficiency

There can be seen a significant improvement in efficiency for key generation while using the unitary GHZ-State operator as preferred quantum channel for qubit transmission. The efficiency of proposed methodology using BB84 and modified BB84 protocols are obtained and their statistics are presented as shown in Figure 16. For different length of key being generated, the efficiency is different. For key length of 200 while key generation, the efficiency is 55.5% for BB84 protocol using the proposed methodology, but in the same case the efficiency is 95% for modified BB84 protocol. It can be also seen that in case of modified BB84 protocol the efficiency of proposed methodology for key generation increases with increase in key length.

6. Conclusion and Future Works

Quantum cryptography with its essential features' for enhancing the QKD application can promote the security to

Table 4: Counts and error rate while observing the measurements for eavesdropper even if she uses same basis for measuring the qubits while interfering the communication channel. Eavesdropper unknown of $|GHZ\rangle$ applies measurement yielding different results as shown in Figure 15.

Base	Bit	0_counts	1_counts	error(%)
0	0	1984.25	2111.75	51.55639648
0	1	4089.25	6.75	99.83520508
1	0	1999.5	2096.5	51.18408203
1	1	4056.75	39.25	99.04174805

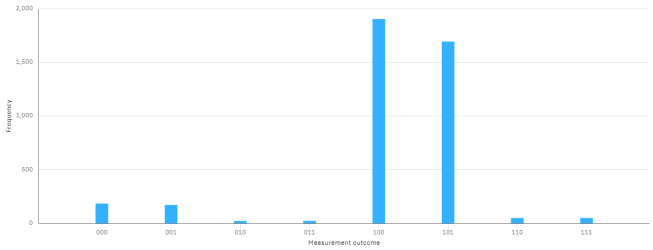

Figure 15: The measurement by eavesdropper yields totally different results. Here, the histogram plot is for quantum circuit in Figure 14.

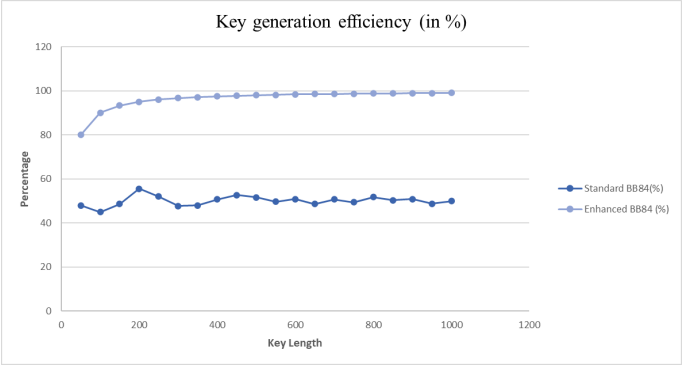

Figure 16: Comparision of the efficiency key generation from standard-BB84 protocol and Enhanced-BB84 protocol.

make information communication more reliable and trustworthy. Classical channel integrated with quantum channel can utilize both, the credentials of classical channel with principles of quantum physics maintained by quantum channels, can enrich the utilization of QKD. Principles of quantum physics such as quantum entanglement, teleportation of qubits, quantum measurement, principle of polarization, no-cloning theorem and Heisenberg uncertainty principle help for enriching the perception of a hybrid channel consisting of Classical and Quantum channels. Such principles are proven to provide advantages on key distribution (also termed as QKD) through various phenomenal analysis provided in different literature followed through completion of this research work. Classical channel embedded with quantum channel can be utilized to achieve more secure communication in a noisy quantum channel. The quantum circuits were all run in real quantum computing resources provided by IBM-Q. The analysis of the circuit shows tolerable error for the transmission channel without eavesdropper, but error surpasses the acceptable value while an eavesdropper is interfering in the channel. In addition, the efficiency of key generation for the proposed methodology is seen to be improved.

Nevertheless, availability of quantum computing resources is yet another challenge for conducting more research in quantum information science and presenting it to more mathematical theories regarding improvement of scientific discoveries. There are still much work to achieve a successful quantum computing resource because of the fact that generating a perfect qubit is still lagging perfect technological advancements. In other hand, many approaches has been made to establish a proper standard for a hybrid approach

Table 5: Tabulation of PQC Schemes that are competing in the NIST (National Institute of Standards and Technology) standardization process [12]. The italic scheme are the fourth round finalists [13]: *Classic McEliece, BIKE, HQC, SIKE.*

Cryptography	Type of scheme	Scheme
Lattice-based	Key Exchange	Kyber, SABER, NTRU, FrodoKEM, NTRU Prime
	Digital Signature	Dilithium, FALCON
Code-based	Key Exchange	*Classic McEliece, BIKE,* NIKE, *HQC*
MQ-based	Digital Signatures	RainBow, GeMSS
Hash-based	Digital Signatures	Picnic, SPHINCS+
Supersingular Isogeny-based	Key Exchange	*SIKE*

regarding key distribution and enabling faster symmetric cryptographic processes. Still not much progress has been made in either of scenario demanding more research in such integrated approach.

Quantum information science provides a very broad concept for scientific research and development of scientific achievements [11]. Although, with advent of quantum computers, the information of the post-quantum era is vulnerable to various threats. The threats are making the classical cryptography obsolete, probing attacks by the quantum computer in the post-quantum world. Although, many research is being carried out to improve the present state of PQC and to carry out the standardization process of PQC algorithms, refer Table **??**. However, the QKD components can also be used for implementation of quantum digital signatures (QDS).

Acknowledgments

The authors are thankful to DOECE, Pulchowk Campus, Institute of Engineering, Tribhuwan University, Nepal.

References

[1] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, 2002.

[2] Daniel J. Bernstein. *Introduction to Post-Quantum Cryptography*. 2009.

[3] Werner Heisenberg. The actual content of quantum theoretical kinematics and mechanics. 43(3-4):172–198, 1927.

[4] William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[5] Daniel Gottesman and Isaac L. Chuang. Quantum digital signatures. *arXiv:quant-ph/0105032v2*, November 2001.

[6] M. A. Panhwar, S. A. Khuhro, T. Mazhar, D. ZhongLiang, and N. Qadir. Quantum cryptography: A way of improving security of information. 16(1):9–21, 2021.

[7] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10th anniversary edition edition, 2010.

[8] P.A.M. Dirac. *The Principles of Quantum Mechanics*. Clarendon Press, 2nd edition, 1947.

[9] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. pages 175–179, 1984.

[10] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Going Beyond Bell's Theorem. *arXiv e-prints*, page arXiv:0712.0921, December 2007.

[11] The Nobel Prize Committee for Physics. *For Experiments with Entangled Photons, Establishing the Violation of Bell Inequalities and Pioneering Quantum Information Science*. The Royal Swedish Academy of Sciences, October 4 2022.

[12] P. Ravi, A. Chattopadhyay, and S. Bhasin. Security and quantum computing: A perspective. 2022.

[13] NIST. Post-quantum cryptography: Digital signature schemes, 2023.