Quantum Computing Protocol Comparison and Proposed a Hybrid Secure Protocol Model

[1]*J. Sebastian Nixon*
Department of CSE, SoE
Dayananda Sagar University
Bangalore, India.

[2]*J. Jeya A Celin*
Department of Information Technology
Kalasalingam Academy of Research and Education,
Krishnankovil, India.

[3]*C. Ganesh*
Department of BCA
IZEE Business School
Bangalore, India

[4]*Priyanka S Marellavar*
Department of CSE, SoE
Dayananda Sagar University
Bangalore, India.

Abstract:

Quantum computing is an emerging technology with the ability to solve critical problems which are traditional computers can't. There are many protocols for quantum computing, such as Quantum Teleportation (QT), Quantum Error Correction (QEC) and Quantum Key Distribution (QKD), have been developed to exploit quantum mechanics' principles. In this paper we did a comparison of these quantum protocols, highlighting their strengths and limitations. Additionally, we propose an optimized quantum protocol that combines features from existing protocols to improve efficiency and robustness in quantum communications.

Keywords: Quantum Computing, Quantum Key Distribution, QKD, QT, QEC, Quantum Protocols.

I. INTRODUCTION

Quantum computing uses the quantum mechanics standards, such as entanglement and superposition, to do operations which are impossible / difficult for traditional computers. Quantum protocols are essential for secure communication, error correction, and efficient computation in quantum

networks. Despite the great progress, each protocol has limitations that require the development of new or updated.

A. Properties of Quantum Computing

Quantum States: A bit is the smallest unit in traditional digital computers to represent and store data. In quantum computing, the basic unit is a quantum bit (qubit), which can be represented by photons and electrons as shown in Figure 1.

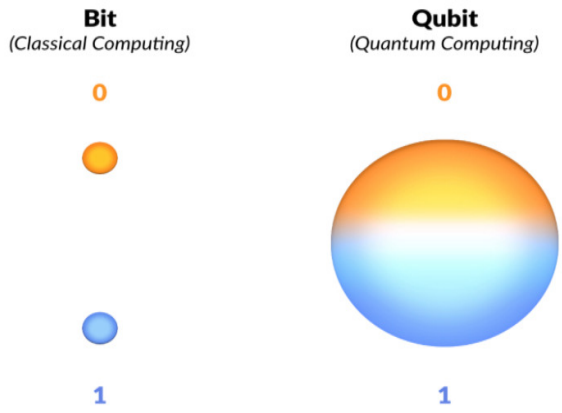

Figure 1 : Classical bit Vs. Quantum bit

In the free space, polarization of the photon defines the states of 0 and 1, can be written as $|0\rangle$ and $|1\rangle$.
These states can be thought as the states 0 and 1 states of a classical bit. However, a quantum bit can have an infinite number of states in arbitrary superposition's of 0 and 1.

In general, a qubit system can be defined as a linear combination of these t states and can be expressed as:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{(i)}$$

where $|\alpha|^2+|\beta|^2 = 1$ and α and β are complex numbers, , which means that the qubit can be embedded in $|1\rangle$ with probability $|\beta|^2$ or in the case of $|0\rangle$ with probability $|\alpha|^2$.

For example, two or more qubit can be formed by combining individual qubits. Consider a 2 qubit system, there would be 4 states of size that can be denoted by $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. Similarly, a 2-qubit system can be represented as a linear combination of these 4 states:

$$|\phi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|j11\rangle \quad \text{(ii)}$$

where α, β, γ, and δ are all complex numbers such that $|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2=1$.

Superposition: Qubits can act as a combination of 0 and 1 at a time. This enables the quantum computers to perform many operations parallel and exponentially increasing the processing power for specific tasks.

Entanglement: Entanglement is a condition in which one qubit is connected to another even though they are physically separated. This property allows qubits to be connect together in ways that classical bits cannot, increasing the information processing capabilities of quantum computers. Figure 2 shows the superposition and the entanglement.

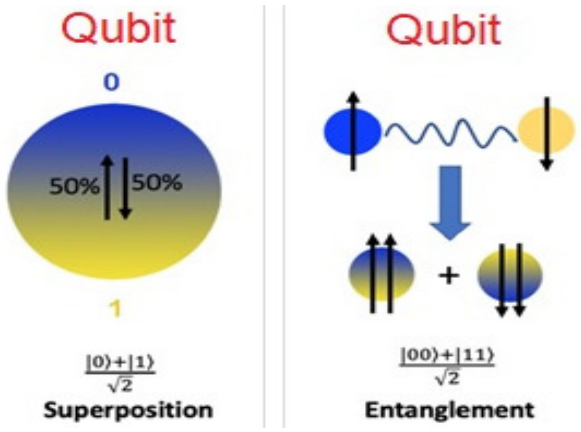

Figure 2 Superposition and Entanglement

Quantum Gate: Like classical logic gates, quantum gates operate qubits to perform particular functions. These are very important for implementing quantum algorithms and computing.

II. LITERATURE REVIEW

A. BB84 Protocol

According to [1] a protocol was proposed to share secret key between 2 parties using quantum mechanics principles namely Heisenberg's uncertainty principle. It described how the photon polarization state could be used to transmit the data of secret key via a quantum communication channel and was the first quantum cryptography protocol. It is known as BB84 protocol and is classified as aprepare & measure based QKD protocol. BB84 protocol uses a single photon to forward and distribute random bits of a secret key.

A single photon is polarized in 1/4 polarization modes, selected using one of two interpolating bases called diagonal basis for diagonal and its anti-diagonal polarization and rectilinear basis for vertical and horizontal polarization, Figure 3 explains these bases polarization.

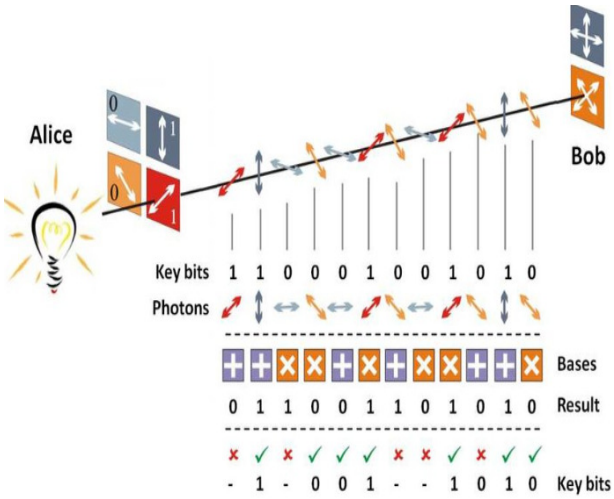

Figure 3: BB84 Protocol Basic scheme

B. Key Distribution in Quantum

QKD: Quantum-Key-Distribution, specifically the **BB84** protocol, is a widely used quantum communication protocol to ensure secure key exchange [2]. There are two kinds of QKD protocol schemes: the first type is prepare-and-measure-based, and the second type is entanglement-based.

This protocol is known as prepare-and-measure since the sender readies the information using polarized photons and the receiver measures the sent photons. According to Heisenberg's uncertainty principle, measuring the quantum state of a system without altering its original state is not achievable. As the no-cloning theorem [3] elucidates, it declares that quantum bits (qubits) cannot be replicated or increased without causing disruption to them.

The QKD system can detect eavesdroppers by measuring error parameters that occur when photons are transmitted from sender to receiver. In the QKD protocol, secure keys are created and shared between two parties that are only known to them, and can be detected if the eavesdropper tries to access the keys [4]. Therefore the QKD provides absolute security for communication by preventing all eavesdropping attempts [5]. However, QKD is sensitive to noise and distance, which limits its performance [6]. Figure 4 illustrate the QKD system implementing the BB84 Protocol.

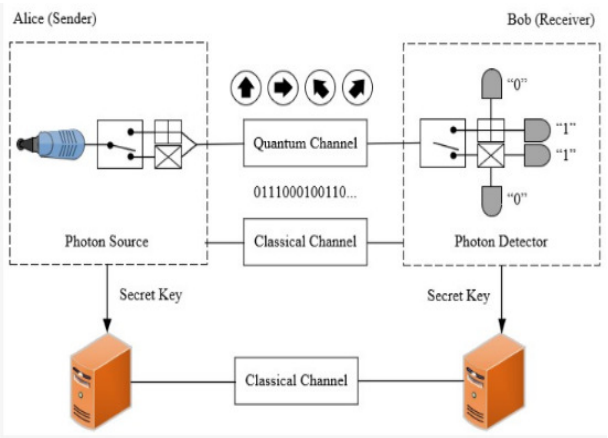

Figure 4: QKD system implementing BB84 Protocol

C. Quantum Teleportation

QT: Quantum teleportation is the transfer of quantum information between locations using a shared entangled channel, which can only be measured using classical physics. Entanglement is crucial in quantum teleportation due to its non-local characteristics.

When multiple parties share an entangled quantum state, they are able to transmit a message through the entangled link via teleportation. Certain unitary operations need to be applied on the right qubits in order to teleport the message to a specific qubit.

The quantum teleportation was first proposed by Bennett et al. [7]. It relies on quantum entanglement and traditional communication and provides a secure way to exchange data as shown in Figure 5. However, the need for pre-shared entanglement and traditional communication channels shows latency [8].

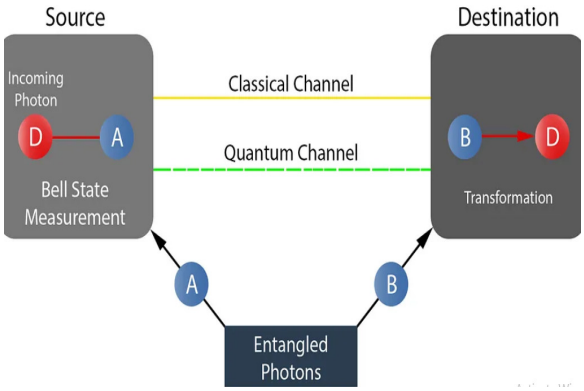

Figure 5 : Quantum Teleportation

D. Error Correction in Quantum

QEC: Quantum-Error-Correction is important for reduce errors in quantum computations due to cancellation and other quantum noise. Various types of QEC codes, like as the surface and Shor codes, have been proposed [9]. Although these codes are efficient, they require significant overhead in terms of qubits and operations [10]. Figure 6 shows the trend for QEC.

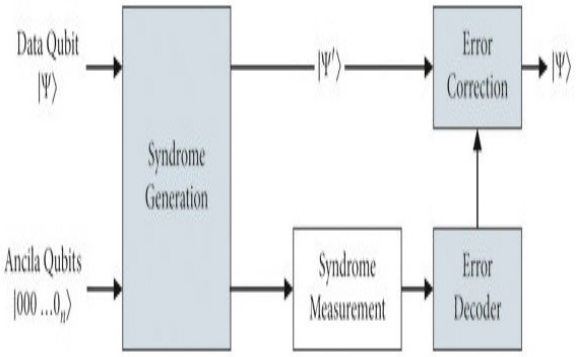

Figure 6 : **Quantum Error Correction**

III. METHODOLOGY

Protocol Comparison

In this section, we compared the QKD , QT and QEC protocols based on several criteria, including security, performance, resource requirements, and scalability.

A. Security Limitations

I] QKD: Provides security against tampering, but is vulnerable to some side-channel attacks [11].

II]. Quantum Teleportation: Provides secure transmission but depends on the security of classical communication channels [12].

III}. QEC: Enhances the security of quantum computing by correcting errors, but does not directly address communication security [13].

B. Efficiency Limitations

I]. QKD: It is efficient in short-distance communications but suffers from scalability issues over long distances [14].

II]. Quantum Teleportation: Good for transmitting quantum data but requires large resources for entanglement distribution [15].

III]. QEC: Requires high qubit overhead which reduces overall efficiency [16].

IV. PROPOSED HYBRID QUANTUM PROTOCOL

Considering the limitations identified in the existing protocols, we propose a hybrid protocol

that combines the strengths of QKD, Quantum Teleportation, and QEC. The proposed protocol involves the following steps:

1] Shared Key Distribution: use QKD for key exchange, with additional QEC checks to ensure key integrity.

2] Enhanced Teleportation: Implement an advanced version of Quantum Teleportation that uses error correcting qubits to reduce the effect of noise and improve reliability.

3] Adaptive Error Correction: It includes a dynamic QEC mechanism that adjusts according to the noise levels in the quantum channel and optimizing resource utilization.

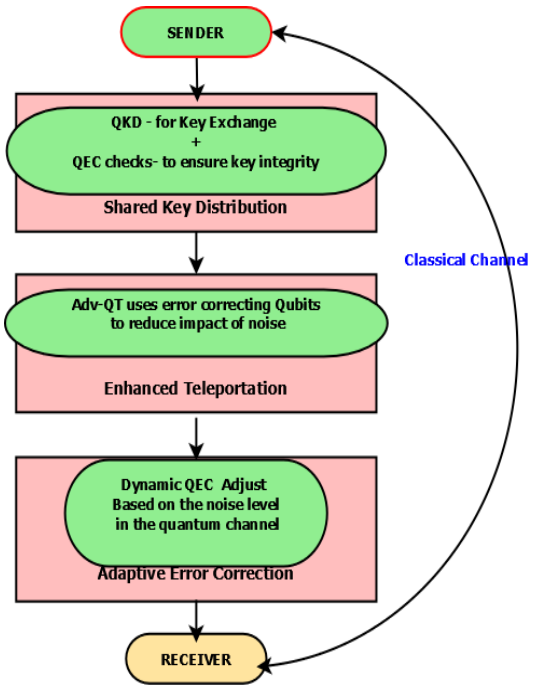

Figure 7: The proposed hybrid protocol model

V. RESULTS AND DISCUSSION

The proposed hybrid method can help alleviate the constraints of existing quantum protocols in terms of security and efficiency, particularly in high-noise environments and over long distances by combining their strengths.

VI. CONCLUSION AND FUTURE WORK

In this paper, we discussed a comparison of important quantum protocols and proposed a hybrid protocol that increases security and efficiency in quantum communications. We didn't perform any performance analysis using any simulation tools. In future using simulation tools we can test and evaluate the effectiveness of the proposed hybrid model.

REFERENCES

[1] C. H. Bennett, et.al., "Quantum cryptography: Public key distribution and coin tossing," Theor. Comput. Sci. 560, pp. 7-11, 2014.

[2] McMahon David. Hoboken, New Jersey: "Quantum Computing Explained" John Wiley & Sons -2008.

[3] W.K. Wootters, et.al., "A single quantum cannot be cloned", Nature 299, pp. 802-803, October 1982.

[4]. Martinez, J.E., "Decoherence and Quantum Error Correction for Quantum Computing and Communications", (2022). arXiv:220208600.

[5]. Peev, M., et al., "A novel protocol-authentication algorithm ruling out a man-in-the-middle attack in quantum cryptography", Int. J. Quant. Inf. 03(01), 225–231 (2005).

[6]. Gisin, N., et.al., "Quantum cryptography-*Reviews of Modern Physics"*,2002, 74(1), 145.

[7]. Bennett, C.H., et al., "Teleporting an unknown quantum state via dual classical and

Einstein-Podolsky-Rosen channels", Phys. Rev. Lett. 70(13), 1895–1899 (1993).

[8]. Bouwmeester, D., et al. ," Experimental quantum teleportation", *Nature*, 390(6660), 575-579 , 1997.

[9]. Shor, P. W., "Scheme to reducing decoherence in Quntum Computer Memory", *Physical Review A*, , 52(4), R2493, 1995.

[10]. Fowler, A. G., et al. "Surface codes: Towards practical large-scale quantum computation", *Physical Review A*, 86(3), 032324, 2012.

[11]. Scarani, V., et al.," The Security of Practical Quantum Key Distribution", Reviews *of Modern Physics*, 81(3), 1301, 2009.

[12]. Pan, J.-W., et al., "Experimental entanglement swapping: Entangling photons that never interacted", *Nature*, 421(6923), 721-725, 2003.

[13]. Gottesman, D. , "Stabilizer codes and quantum error correction", *arXiv preprint quant-ph/9705052, 1997.*

[14]. Lo, H.-K., et.al., "Secure quantum key distribution", *Nature Photonics*, 8(8), 595-604, 2014.

[15]. Pirandola, S., et al., "Advances in quantum teleportation", *Nature Photonics*, 9(10), 641-652.

[16]. Terhal, B. M., "Quantum error correction for quantum memories", *Reviews of Modern Physics*, 87(2), 307, 2015.