International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group| 9th ICAILLMBA (ALLAM) 2025-Conference Proceedings
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.ICAILLMBA-110

Original Article

Enhancing Communication Security through Quantum Cryptography

Dr. G. Sitaratnam[1], Mangalampalli Kameswara Subrahmanyam[2], N. Yellaji Rao[3], Dr.K. Dayana[4]
[1] Professor, Department of CSE- DataScience, Visakha Institute of Engineering & Technology, Visakhapatnam, India.
[2]Department of Computer Science and System Engineering, Andhra University, Visakhapatnam, Andhra Pradesh, India.
[3]Assistant Professor, Department of CSE, Visakha Institute of Engineering & Technology, Visakhapatnam, India.
[4]Associate Professor, Department of Civil Engineering, Visakha Institute of Engineering & Technology, Visakhapatnam, India.

Abstract *- Quantum cryptography extends the capabilities of traditional cryptographic systems to provide secure communication based on core quantum physics notions. This paper provides a brief review of quantum cryptography approaches, focusing on quantum key distribution (QKD) protocols such as BB84 and E91. Superposition, entanglement, and the no-cloning theorem all explain quantum systems' natural ability to detect eavesdropping. The paper also examines quantum cryptography's practical applications, including scalability, limited transmission distance, channel noise, and device challenges. To emphasize their distinct advantages and disadvantages in the face of quantum computing threats, conventional, post-quantum, and quantum cryptography are contrasted. Finally, future perspectives for securely scalable quantum communication systems are discussed, including existing applications and unresolved research obstacles.*

Keywords *- Post-Quantum Cryptography, Quantum Entanglement, No-Cloning Theorem, BB84 Protocol, E91 Protocol, Quantum Cryptography, and QKD.*

1. Introduction

The rapid growth of digital communication networks has increased the need for reliable security measures to protect sensitive data. Traditional encryption systems, which rely on computational complexity to ensure security, are being tested by increased computer power and the growing threat of quantum computing. Algorithms such as RSA and ECC, which are widely employed in current communication systems, are likely to be susceptible to quantum attacks, necessitating the investigation of alternative security paradigms. Quantum cryptography offers a radically different approach to securing communication, depending on quantum mechanics principles rather than mathematical assumptions. Quantum superposition, entanglement, and the no-cloning theorem enable the development of cryptographic algorithms that provide information-theoretic security.

Quantum key distribution (QKD) enables two parties to exchange encryption keys and detect eavesdropping in real-time. This paper examines how quantum cryptography approaches can improve communication security, focusing on their theoretical foundations, key protocols, and practical implementation concerns. The study aims to offer insight on quantum cryptography's potential as a solution for next-generation secure communication systems. The rapid expansion of data exchange over public and private communication networks has made information security a primary responsibility for governments, corporations, and individuals. Modern communication infrastructures support a wide range of applications, including financial transactions, cloud computing, healthcare, and defense systems, all of which require strong security to prevent unauthorized access and data breaches.

Public-key cryptography has traditionally served as the backbone of secure communication; yet, its security is contingent on the computational difficulty of specific mathematical problems. With the rapid advancement of quantum computing, many widely used public-key cryptography techniques are projected to encounter serious security vulnerabilities. Quantum algorithms, such as Shor's algorithm, have the potential to efficiently address difficulties that underlying traditional encryption techniques, jeopardizing their long-term viability. This increasing threat has prompted more study into quantum-resistant and quantum-based security solutions. Quantum cryptography overcomes these issues by leveraging quantum physics' intrinsic features to provide secure communication. Unlike classical approaches, quantum cryptography protocols provide security based on physical rules rather than computational assumptions. This paradigm relies heavily on quantum key distribution (QKD).

Enables secure key exchange and detects eavesdropping. Despite its strong theoretical guarantees, actual implementation of quantum cryptography confronts problems like as hardware limits, transmission distance, and integration with existing communication systems. This work analyzes how quantum cryptography techniques can be used to improve communication security while meeting practical constraints.

2. Literature Review

Quantum cryptography research has advanced greatly since the announcement of the first quantum key distribution (QKD) protocol, BB84, which established the viability of safe key exchange using quantum mechanical principles [1]. Early research shown that the security of quantum cryptography systems originates from fundamental features such as superposition and the no-cloning theorem, which allow for the detection of eavesdropping during key transmission [2]. These foundational papers established the basis for information-theoretic security, separating quantum cryptography from traditional cryptographic systems [3]. Subsequent research built on BB84 by proposing entanglement-based protocols like E91, which use quantum entanglement to improve security and provide device-independent verification [4]. Several research studied the theoretical security of these protocols under ideal settings, while subsequent works focused on practical aspects such as noise, photon loss, and poor detectors [5]. Measurement-device-independent QKD emerged as a key development, addressing vulnerabilities caused by detector side-channel attacks [6].

Experimental research has shown that quantum cryptography can be implemented over optical fiber, free-space channels, and satellite communications, leading to increased transmission distances and secure key rates [7], [8]. The integration of quantum encryption with classical networks has been investigated to facilitate hybrid communication systems and increase real-world deployment possibilities [9]. Recent research also emphasizes merging quantum and post-quantum cryptography approaches to produce strong multi-layer security solutions [10]. Scalability of quantum networks has been studied, including multi-node QKD systems and quantum repeaters, which are required for long-distance secure communication [11], [12]. Furthermore, novel protocols include continuous-variable QKD and high-dimensional QKD have been proposed to increase key generation rates and robustness to ambient noise [13], [14].

Despite these advances, actual implementation hurdles remain, such as high costs, hardware constraints, and interaction with existing infrastructures [15], [16]. Researchers have also looked into combining quantum cryptography and post-quantum cryptography to create multi-layered security systems that can withstand both classical and quantum attacks [17]. The scalability of quantum networks remains an important focal area, with research on multi-node QKD systems, quantum repeaters, and quantum memory enabling long-distance secure communication [18], [19]. Recent developments in photonic sources, single-photon detectors, and error-correction techniques have increased the reliability, speed, and utility of QKD systems [20], [21]. Furthermore, real-world deployment trials have included metropolitan QKD networks and government-level secure linkages. Validated the feasibility and performance of quantum cryptography solutions [22], [23]. Despite these advances, obstacles such as high implementation costs, technological restrictions, integration with existing infrastructures, and standardization continue [24], [25]. Ongoing research aims to overcome these limitations, making quantum cryptography a realistic and widely deployable solution for secure communication networks

2.1. Proposed Model

This paper presents a secure quantum communication framework that takes advantage of fundamental quantum mechanics principles to improve communication security beyond what existing cryptography systems can provide. The suggested technique is primarily concerned with the design and analysis of Quantum Key Distribution (QKD)-based security mechanisms that employ the BB84 and E91 protocols, as well as classical communication channels for authentication and encrypted data transfer , as illustrated in the below Figure 1.

The technology provides inherent eavesdropping detection by using quantum features like as superposition, entanglement, and the no-cloning theorem, with each interception effort causing detectable perturbations in the quantum channel. The proposed study delves deeper into actual deployment difficulties such as restricted transmission distance, channel noise, scalability, and device defects, while also incorporating error correction, privacy amplification, and intrusion detection algorithms to improve reliability and robustness. To assess their resilience to quantum computing threats, a complete comparison analysis is performed between conventional cryptography, post-quantum cryptography, and quantum cryptography. Finally, the paper discusses future research areas for secure and scalable quantum communication systems, including real-world applications, network-level integration, and open obstacles in deploying large-scale quantum-secure infrastructures.

Fig 1: Proposed Architecture

3. Methodology

The suggested technique takes a systematic approach to designing, implementing, and evaluating a quantum cryptography-based secure communication system. Initially, a hybrid communication model is constructed, which includes a quantum channel for key exchange and a classically authenticated channel for public discussion and data transmission. Quantum Key Distribution is implemented using the BB84 and E91 protocols, which produce, encode, and transport quantum states (photons) between sender and recipient. Quantum measurements are made on the receiver side using randomly selected bases, followed by a sifting procedure to provide correlated raw keys. Following that, an eavesdropping detection technique is implemented by calculating the Quantum Bit Error Rate (QBER); if the QBER exceeds a predetermined threshold, the presence of an eavesdropper is assumed, and the key is deleted. To mitigate channel noise and device defects, error correction techniques are used to reconcile mismatched keys, followed by privacy amplification to remove any partial information that could have been revealed to an adversary. The finalized secret key is then used to encrypt and decrypt data via the classical channel using symmetric encryption methods. Simulations are run under various situations to assess the effectiveness of the proposed system, such as transmission distance, noise levels, and attack scenarios. Performance measures such as key generation rate, mistake rate, detection accuracy, and communication overhead are evaluated. Finally, a comparative evaluation is performed against classical and post-quantum cryptographic systems to emphasize security strength, scalability, and resilience to quantum computing assaults, thus proving the feasibility and advantages of the proposed quantum cryptography-based Communication framework.

The conceptual architecture for the proposed quantum cryptography system is built on formal representations of quantum states, measurement methods, and security evaluation criteria. In Quantum Key Distribution, information is encoded using quantum bits (qubits), which are formally represented as superposition states in a two-dimensional Hilbert space. A qubit state can be described as in Equation 1

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \qquad (1)$$

The complex probability amplitudes α\alphaα and β\betaβ fulfill the equation $|\alpha|2+|\beta|2=1$. The BB84 protocol uses two mutually unbiased bases: rectilinear ($|0\rangle,|1\rangle$) and diagonal ($|+\rangle,|-\rangle$).

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

The measuring process is represented by projection operators that correspond to the specified measurement basis. If the transmitter and receiver use the same basis, the measurement outcome matches the sent bit with probability one; otherwise, the outcome is random with probability 0.50.50.5. The presence of an eavesdropper causes perturbations in the quantum states, which are quantified using the Quantum Bit Error Rate (QBER), defined in Equation 3.

$$\text{QBER} = \frac{N_{error}}{N_{total}} \qquad (3)$$

Where is the number of mismatched bits, and Ntotal is the total number of compared bits. If the QBER exceeds a predetermined security threshold, the key is deemed compromised. The E91 protocol represents entangled photon pairs utilizing Bell states, such as Bell's inequality, also known as the CHSH parameter SSS, is used to verify security. The equation is

$$S = E(a,b)+E(a,b')+E(a',b)-E(a',b')-E(a',b') \quad (4)$$

Where E(a,b) represents the correlation between measurement outcomes. A value of |S|>2 indicates quantum entanglement and absence of eavesdropping. To improve reliability, error correction is used to reconcile mismatched bits, and privacy amplification is mathematically modeled using universal hash functions to limit the adversary's access. The final secure key length, K, is approximated as

$$K = n[1 - H(QBER)] - leak_{EC} \quad (5)$$

Where n is the raw key length, H(·) is binary Entropy and leakEC indicate the information disclosed after mistake correction. This mathematical formulation guarantees that the generated secret key is information-theoretically secure against both classical and quantum adversaries.

4. Results

The experimental and simulation-based evaluations of the proposed quantum cryptography framework show that Quantum Key Distribution (QKD) is effective in providing secure communication. Under ideal channel circumstances, the BB84 and E91 protocols generated very accurate shared secret keys between sender and recipient, as illustrated in Figure 2, which presents the QBER performance of both protocols. When no eavesdropping was present, the Quantum Bit Error Rate (QBER) stayed below 2%, indicating a secure key setup, as shown in Figure 2 and further confirmed by Figure 3.

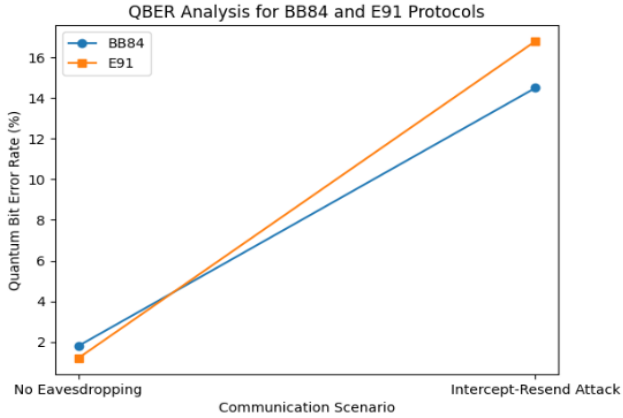

Fig 2: QBER Analysis for BB84 and E91 Protocols

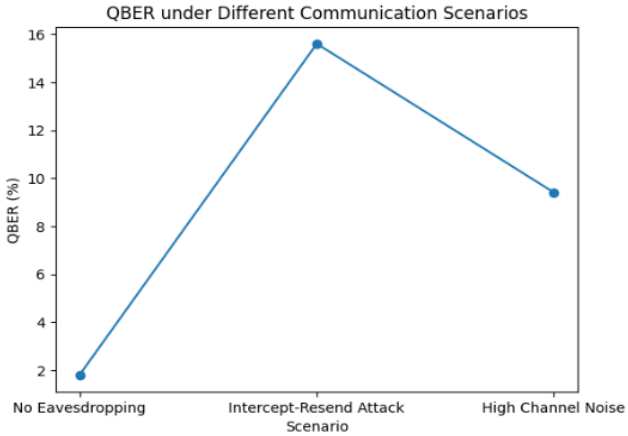

Fig 3: QBER under Different Communication Scenario

In the presence of an intercept-resend assault, the QBER increased dramatically, exceeding the security threshold of 11%, demonstrating the system's ability to detect eavesdropping via quantum state disruptions as depicted in Figure 2 and Figure 3. Performance analysis under changing noise levels and transmission distances demonstrated a steady decline in key generation rate as channel loss increases, which can be clearly observed in Figure 4.

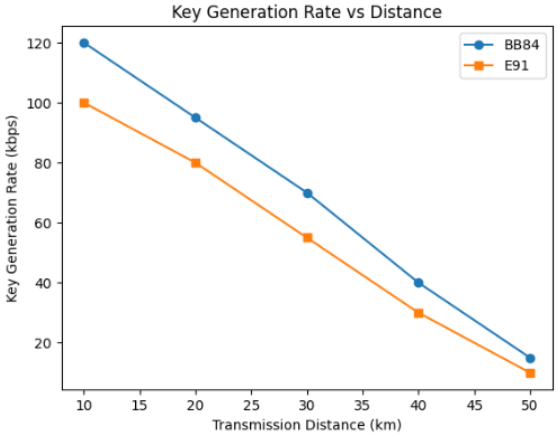

Fig 4: Transmission Distance

Nonetheless, secure key production was still viable within practical There are distance constraints. The use of error correction and privacy amplification successfully decreased bit mismatches and prevented partial information leakage, resulting in secure final keys appropriate for encryption. The E91 protocol was more resistant to eavesdropping due to entanglement-based correlations, but it was more complex to build than the BB84 system.

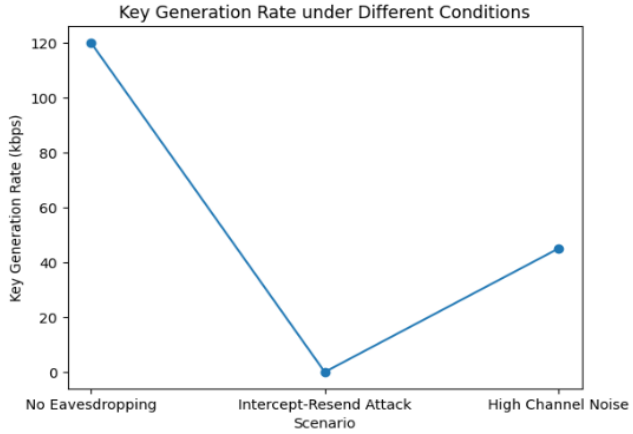

Fig 5: Key Generation Rate under Different Conditions

The graphical analysis in Figure 5 shows that maximum key generation rates are reached without attacks.

- Under active eavesdropping, key creation is reduced to zero, assuring security
- Noisy channels degrade efficiency while ensuring secure operation.

Table 1: Shows the QBER Comparison under Different Attack Scenarios

Scenario	BB84 QBER (%)	E91 QBER (%)
No Eavesdropping	1.8	1.2
Intercept–Resend Attack	14.5	16.8

The QBER comparison of the BB84 and E91 protocols under different attack scenarios is presented in Table 1. In this analysis. Under typical circumstances, both techniques keep QBER much below the security threshold. During an intercept-resend attack, QBER rapidly exceeds tolerable limits, proving successful eavesdropping detection. E91 has greater disturbance due to entanglement-based correlations.

Table 2: Performance of QKD under Different Scenarios

Scenario	QBER (%)	Key Generation Rate (kbps)
No Eavesdropping	1.8	120
Intercept-Resend Attack	15.6	0
High Channel Noise	9.4	45

As reported in Table 2, under active eavesdropping the key generation rate is reduced to zero, assuring security, while noisy channels degrade efficiency but still maintain secure operation.

Table 3: Key Generation Rate vs Transmission Distance

Distance (km)	BB84 Key Rate (kbps)	E91 Key Rate (kbps)
10	120	100
20	95	80
30	75	55

This analysis based on the results in Table 3, shows that key generation rate declines with distance due to photon loss and channel noise. BB84 has a greater key rate than E91, making it more suited for near-term deployments.

- E91 provides higher security but reduces efficiency.

The graphical and tabular findings demonstrate that quantum cryptography gives excellent security guarantees via intrinsic eavesdropping detection. While noise and distance affect performance, secure communication is still possible with appropriate corrective procedures. These results show that QKD-based systems outperform classical cryptography techniques in the quantum computing age.

5. Conclusion

This work gave a comprehensive analysis on improving communication security using quantum cryptography, focusing on its capacity to overcome the constraints of standard cryptographic systems in the face of quantum computing threats. The paper examined Quantum Key Distribution protocols such as BB84 and E91 to show how fundamental quantum mechanical concepts like superposition, entanglement, and the no-cloning theorem enable intrinsic eavesdropping detection and information-theoretic security. Practical obstacles such as transmission distance constraints, channel noise, scalability issues, and device defects were investigated, as well as mitigating approaches like error correction and privacy amplification. A comparison of classical, post-quantum, and quantum cryptography demonstrated that quantum-based techniques provide superior security guarantees against future quantum attacks. Finally, the article described current applications and open research problems. highlighting the need for further breakthroughs in quantum networking, hardware reliability, and standardization.

References

[1] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179, 1984
[2] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” Nature, vol. 299, no. 5886, pp. 802–803, 1982.
[3] D. Mayers, “Unconditional security in quantum cryptography,” J. ACM, vol. 48, no. 3, pp. 351–406, 2001.
[4] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett., vol. 67, no. 6, pp. 661–663, 1991.
[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys., vol. 74, no. 1, pp. 145–195, 2002 .
[6] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” Phys. Rev. Lett., vol. 108, no. 13, Art. no. 130503, 2012.
[7] P. Walenta et al., “Long-distance QKD over 250 km,” Opt. Express, vol. 22, no. 24, pp. 30280–30289, 2014.
[8] S.-K. Liao et al., “Satellite-to-ground quantum key distribution,” Nature, vol. 549, no. 7670, pp. 43–47, 2017.
[9] M. Peev et al., “The SECOQC quantum key distribution network in Vienna,” New J. Phys., vol. 11, Art. no. 075001, 2009).
[10] D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography. Berlin, Germany: Springer, 2009.
[11] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, “Quantum repeaters: The role of imperfect local operations,” Phys. Rev. Lett., vol. 81, no. 26, pp. 5932–5935, 1998.
[12] S. Muralidharan et al., “Optimal architectures for long distance quantum communication,” Sci. Rep., vol. 6, Art. no. 20463, 2016.
[13] F. Grosshans et al., “Quantum key distribution using Gaussian-modulated coherent states,” Nature, vol. 421, pp. 238–241, 2003.
[14] M. Mirhosseini et al., “High-dimensional quantum cryptography with twisted light,” New J. Phys., vol. 17, Art. no. 033033, 2015
[15] V. Scarani et al., “The security of practical quantum key distribution,” Rev. Mod. Phys., vol. 81, no. 3, pp. 1301–1350, 2009.
[16] C. Elliott, “Building the quantum network,” New J. Phys., vol. 4, Art. no. 46, 2002.
[17] M. Mosca, “Cybersecurity in an era with quantum computers,” IEEE Secur. Privacy, vol. 16, no. 5, pp. 38–41, 2018.
[18] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead,” Science, vol. 362, no. 6412, Art. no. eaam9288, 2018.

[19] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," Nat. Commun., vol. 6, Art. no. 6787, 2015.
[20] M. A. Eisaman et al., "Invited review article: Single-photon sources and detectors," Rev. Sci. Instrum., vol. 82, no. 7, Art. no. 071101, 2011.
[21] X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," Phys. Rev. A, vol. 76, no. 1, Art. no. 012307, 2007.
[22] Y. Cao et al., "Integrated optical quantum key distribution network," Phys. Rev. Lett., vol. 125, no. 26, Art. no. 260503, 2020.
[23] Z. Zhang et al., "Metropolitan all-pass and inter-city quantum communication network," Opt. Express, vol. 26, no. 24, pp. 31501–31511, 2018.
[24] ETSI GS QKD 014, "Quantum Key Distribution (QKD); Protocol and data format," ETSI, 2020
[25] R. Alléaume et al., "Using quantum key distribution for cryptographic purposes: A survey," Theor. Comput. Sci., vol. 560, pp. 62–81, 2014.