WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Quantum Key Distribution Protocols- A Recent Survey

Maddila Akhilesh [a]*, Naidu Thanusri [a], P. L. K Naidu [a], Konchada Divya [a], R. Cristin [a]

[a] *Department of CSE, GMR Institute of Technology, Rajam, Andhra Pradesh, India*

DOI : https://doi.org/10.55248/gengpi.5.1124.3334

A B S T R A C T

Quantum Key Distribution (QKD) brings a revolutionary approach to secure communication by using the principles of quantum mechanics to safeguard the transfer of cryptographic keys. This project explores the practical deployment of two foundational QKD protocols: BB84 and E91. The BB84 protocol secures key distribution through photon polarization, while the E91 protocol uses the unique properties of quantum entanglement to enhance resistance to eavesdropping. By contrasting these quantum methods with classical cryptographic techniques, the study provides a comprehensive look at their relative strengths and limitations. Practical implementation and thorough analysis demonstrate that QKD protocols offer significant advantages in preventing interception, shedding light on their potential role in advancing cryptographic security in the era of quantum technology. This research not only assesses the practical challenges of implementing QKD but also considers future advancements that could broaden its real-world applications.

Keywords: Quantum Key Distribution, BB84 protocol, E91 protocol, quantum mechanics, secure key transfer, photon polarization, quantum entanglement, cryptography.

1. Introduction

Quantum Key Distribution (QKD) marks a major leap forward in the field of secure communication, using quantum mechanics to establish cryptographic keys that are highly secure. Unlike traditional methods of encryption that depend on complex mathematical problems, QKD guarantees security through the physical properties of quantum particles, such as superposition and entanglement. One of QKD's key strengths is its built-in ability to detect any unauthorized attempts to intercept the key during transmission. Any interference from an eavesdropper changes the quantum states of the particles, exposing the interception attempt and protecting the communication from compromise.This study focuses on two essential and well-studied QKD protocols: BB84 and E91. The BB84 protocol, introduced in 1984, transmits single quantum bits (qubits) in different quantum states to generate keys. The protocol's security is reinforced by the principle that measuring a quantum system unavoidably disturbs it, allowing the detection of potential eavesdropping. Meanwhile, the E91 protocol, developed in 1991, uses quantum entanglement, a phenomenon where particles remain connected even when separated by large distances. The entangled states in the E91 protocol enable the creation of shared keys while ensuring that any tampering is revealed through the disruption of quantum correlations.This project aims to explore and simulate the BB84 and E91 protocols in software to study how these key generation methods perform and respond to simulated attacks. By focusing on computational simulations rather than physical hardware, this research provides a practical and cost-effective way to delve into the workings of QKD. Using quantum computing tools like ProjectQ and integrating cryptographic software, the research involves key generation and transmission processes. Scenarios with and without eavesdropping will be tested to analyze the ability of these protocols to detect unauthorized monitoring and maintain secure communication. This work will contribute valuable insights into how well these quantum protocols can protect against emerging threats and what their future role in secure communications might be.

2. Literature Survey

This research compares three quantum key distribution (QKD) schemes: BB84, E91, and B92, focusing on quantum cost and raw key efficiency. Simulations were carried out under ideal, noiseless conditions using the Qiskit framework to assess the performance of each scheme. The results indicate that BB84 offers the highest cost-efficiency, while E91 proves to be less practical due to its higher quantum cost. The analysis underlines the need to account for noise sensitivity in real-world applications, though noise was not factored into the present simulations [1]. Quantum cryptography leverages the laws of quantum mechanics to strengthen data security, overcoming the limitations of classical cryptographic techniques. QKD is one of the main components of quantum cryptography, providing a method for secure key exchange that resists eavesdropping. Various protocols, such as SARG04 and KMB09, have been analyzed for their effectiveness in terms of performance and security. Proper key management is identified as essential for ensuring confidentiality, integrity, and availability (CIA) in network security systems [2].

The study focuses on two key QKD protocols: BB84, which uses single photons, and E91, which relies on entangled photons to detect the presence of an eavesdropper. BB84 identifies eavesdropping through measurement errors, while E91 uses quantum entanglement to detect intrusion. QKD has been

successfully demonstrated both on terrestrial networks and via satellite communication. A major breakthrough was the 2017 Micius satellite experiment, which achieved secure key distribution over a distance of 1,200 km, significantly expanding QKD's potential range. These advancements are laying the foundation for a global quantum communication network, which promises more secure communications [3]. Several QKD protocols—including BB84, B92, and E91—employ key quantum principles, such as Heisenberg's Uncertainty Principle and Bell's Inequality, to ensure security. The protocols are designed to resist eavesdropping, with quantum cryptography offering unconditional security in appropriate conditions. Advances in quantum optics and communication technologies have enabled QKD deployment across several kilometers, achieving key exchange rates of thousands of bits per second [4].

E91, introduced by Artur Ekert, employs quantum entanglement for secure key exchange. Prior research primarily focused on preventing eavesdropping but did not fully examine how noise affects quantum communication. This study introduces a model that evaluates the security of the E91 protocol under collective-rotation noise, demonstrating that an eavesdropper could extract up to 50% of the key in certain noise conditions. These findings contribute to a more comprehensive understanding of QKD security in noisy environments [5]. In addition to discrete-variable protocols like BB84 and E91, continuous-variable QKD (CV-QKD) is explored. CV-QKD uses the continuous degrees of freedom of quantum states, achieving higher key rates and easier integration with current infrastructure. Satellite-based QKD is highlighted as a promising solution for secure communication over long distances. Experimental results confirm the feasibility of creating secure links between distant ground stations, with implications for future large-scale quantum networks. Integrating multiple communication nodes into a unified network architecture allows multi-party key distribution, creating secure communication channels. Measurement-Device-Independent QKD (MDI-QKD) further enhances security by eliminating trust assumptions regarding measurement devices [6].

Fundamental concepts of quantum computing, such as qubits, superposition, and entanglement, are essential to understanding quantum systems. Quantum computing shows great potential in secure communications, including QKD and quantum teleportation, by enhancing both security and efficiency. However, significant challenges remain, including high error rates, the need for efficient algorithms, and hardware limitations. Future research is expected to focus on improving quantum error correction and developing scalable systems to enable practical quantum computing applications [7]. Quantum cryptography is identified as a crucial countermeasure against potential quantum computing threats. For example, Shor's algorithm could break classical encryption systems such as RSA. This has prompted the design and validation of Quantum Key Management Systems (QKMS) to secure communication infrastructures, such as KREONET, by generating and distributing symmetric quantum-encrypted keys. Current QKD systems face limitations, such as difficulties in achieving network-to-network (N2N) communication and distance constraints of 80–200 km [8].

A review of existing QKD protocols, including BB84 and E91, demonstrates their capability to provide information-theoretic security against eavesdropping. The integration of QKD into optical networks supports the wider adoption of quantum cryptography. Additionally, post-quantum cryptographic methods, such as lattice-based and code-based algorithms, are being developed to ensure security in a post-quantum world. However, practical challenges—such as cost, miniaturization, and infrastructure compatibility—must be addressed for broader implementation [9]. The transition from classical cryptographic methods, which are vulnerable to reverse engineering, to modern encryption systems has enabled secure online transactions. QKD, by leveraging individual light quanta, provides security that even quantum computers cannot break. However, terrestrial QKD systems are limited by channel losses, restricting the distance to a few hundred kilometers, though satellite-based systems offer a promising solution for global networks [10].

Quantum cryptography offers significant potential for improving network security and privacy in the digital communication era. Developing more advanced QKD protocols, secure post-quantum algorithms, and solutions for IoT devices will be critical for the practical application of quantum cryptography. Researchers are also working on improving security proofs for CV-QKD and building efficient quantum repeater networks to extend communication distances. Integrating QKD into optical networks could pave the way for secure services, including Key-as-a-Service (KaaS) frameworks [11]. Various studies focus on QKD protocols from the perspectives of security against eavesdropping and efficient implementation on quantum hardware. Physical models have been applied to enhance protocol security by utilizing quantum properties. Protocols such as BB84, B92, and E91 offer different advantages and limitations in their application for secure key distribution [12].

The BB84 protocol, introduced by Bennett and Brassard in 1984, employs Heisenberg's Uncertainty Principle for secure key exchange. Ekert's work in 1991 expanded on these ideas by using Bell's theorem and quantum entanglement to detect eavesdropping. QKD protocols are broadly divided into those based on the uncertainty principle and those utilizing quantum entanglement, reflecting the diverse approaches within the field. A multi-user QKD network model is proposed, extending the E91 protocol to allow simultaneous key sharing among several users. This model utilizes Spontaneous Parametric Down Conversion (SPDC) to generate entangled photons, which are crucial for key distribution. The use of wavelength-division multiplexing (WDM) enables the transmission of entangled photons across different wavelengths, improving key sharing efficiency. Polarization states of photons are used for key generation, emphasizing the importance of matching measurement bases for successful exchange [14].

Quantum properties offer a solution to the vulnerabilities of classical cryptography by ensuring unconditional security in communication. The challenge of eavesdropping is mitigated through QKD, which allows secure key exchange to prevent unauthorized interception. Protocols like BB84, B92, and those based on Einstein-Podolsky-Rosen (EPR) states provide effective mechanisms for secure key generation. Key management plays a crucial role in maintaining secure networks, with quantum cryptography offering more robust solutions than traditional methods [15]. Experimental implementations of QKD protocols demonstrate the importance of entangled states in secure communication. Verification of the BB84 protocol with three measurement bases has been performed, accounting for possible attacks by an eavesdropper, often referred to as Eve. The B92 protocol, introduced by Charles Bennett in 1992, is also evaluated along with potential attack scenarios. Additionally, the implementation of a CHSH-based protocol showcases how

entangled qubits can be measured to generate raw keys. These experiments, conducted on the IBM Quantum Experience platform, highlight the practical application of quantum computing in cryptographic systems [16].

3. Illustrations

Fig.1 Quantum Key Distribution (QKD) typically illustrates the process of secure key exchange between two parties, often named Alice and Bob. The diagram shows how Alice sends quantum bits (qubits) encoded as photons to Bob through a quantum channel. These qubits can represent states such as polarization angles, enabling the transmission of quantum information. The accompanying classical channel, depicted separately, is used for communication between Alice and Bob to perform key reconciliation and error checking.Fig.2 States about the Result of key and text exchange between Sender and Receiver without an attacker.Fig.3 States about the Result of key and text exchange between Sender and Receiver when an attacker interrupt.

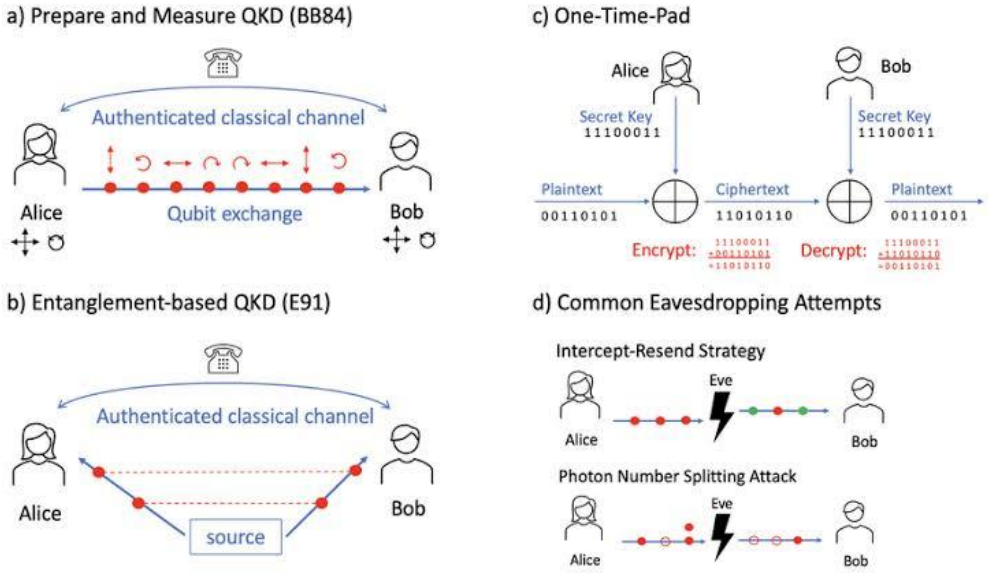

Fig. 1 – Key generation Schemes

```
Enter the message to encrypt: hello
Original Message: hello
(Note: This is the (slow) Python simulator.)
Generated BB84 Key (128 bits): 01a04a8818801000690049262100068 8
Encrypted Message: 378dfea45f9d4a09c97a1d16ed6eae62961da093fca938ca70bbb04549198330
Decrypted Message: hello
```

Fig. 2 – Results without Attacker

```
Enter the message to encrypt: hellio
Original Message: hellio
(Note: This is the (slow) Python simulator.)
Generated Alice's BB84 Key (128 bits): 89a1252daf7b2619
Generated Bob's BB84 Key (128 bits): a3a1b57d303e0d08
Key mismatch detected in bits at indices: [2, 4]
Alice's bits: [0, 1]
Bob's bits: [1, 0]
Key discarded due to mismatches.
```

Fig. 3 – Results with Attacker

4. Experiments

4.1 Quantum State Representation (BB84 Protocol):

The BB84 protocol uses qubits in quantum states to represent key bits. The qubits are represented using the following basis states:

- Rectilinear basis (standard basis):

$|0\rangle=(10\quad),|1\rangle=(01\quad)$

- Diagonal basis (superposition states):

|+⟩=1/√ 2(11),|−⟩=1/√2 (1−1)

Probability of Detection (BB84 Protocol):

The probability of detecting an eavesdropper (Eve) is derived from the fact that measuring a quantum state in the wrong basis introduces errors:

- Probability of detecting Eve if she measures half the qubits:

Pdetect =1−(3/4)^n

where n is the number of bits measured.

4.2 Bell's Inequality (E91 Protocol):

The E91 protocol uses entanglement and tests Bell's inequality to ensure the security of the shared keys:

- Bell's inequality is expressed as:

S=|E(a,b)−E(a,b′)+E(a′,b)+E(a′,b′)|≤2

where E(a,b)E(a, b)E(a,b) represents the correlation between measurement outcomes at settings aaa and bbb. If S>2S > 2S>2, it indicates the violation of Bell's inequality, confirming entanglement and secure key distribution.

4.3 Quantum Entanglement (E91 Protocol):

The state of entangled qubits shared between two parties, Alice and Bob, is typically represented as:

$$|\Psi\rangle=1/\sqrt{\ }\ 2\ \ (|00\rangle+|11\rangle)$$

Any measurement by an eavesdropper will disrupt this state, leading to detectable anomalies in the outcomes.

4.4 Error Rate (Quantum Bit Error Rate - QBER):

The Quantum Bit Error Rate (QBER) is used to quantify the error introduced during key exchange and assess security:

$$QBER=\text{Total number of transmitted bits / Number of incorrect bits}$$

A high QBER may indicate the presence of an eavesdropper.

5. Results and Discussions

In the project results, the BB84 protocol proved effective for generating cryptographic keys with consistent outcomes and relatively low error rates when conditions were well managed. However, as noise levels increased, its vulnerability became apparent, impacting its reliability. On the other hand, the E91 protocol demonstrated greater security benefits through the use of entangled photons, showcasing the violation of Bell's inequality as evidence of secure quantum correlations. Yet, this came at the cost of greater implementation complexity and a higher sensitivity to noise, presenting practical challenges.These observations indicate that BB84 offers a simpler, more feasible approach for current quantum key distribution applications, particularly in stable environments. Meanwhile, E91 stands out for its advanced security features but requires more sophisticated setups, making it harder to implement. The decision between using BB84 or E91 ultimately depends on the need for simplicity versus the level of security required. Future work could involve combining the advantages of both protocols to achieve balanced, real-world solutions and extending testing under varied operational conditions to refine practical use cases.

6.Conclusion

Quantum Key Distribution (QKD) stands out as a powerful advancement in secure communication, leveraging quantum mechanics to establish encryption keys with theoretically guaranteed security. By relying on principles such as superposition, entanglement, and the fundamental behavior of quantum particles, QKD can detect any attempt at eavesdropping, offering a level of security that surpasses classical cryptographic methods. Protocols like BB84 and E91 demonstrate the effectiveness of QKD in real-world applications, especially as cybersecurity threats continue to evolve. As quantum computing advances, QKD will play an essential role in protecting sensitive information, marking a promising step forward for future-proof cryptographic solutions.

References

Lidbjörk, Erik, and Rasmus Söderström Nylander. "Cost and efficiency comparison of Quantum Key Distribution schemes." (2023).

Moizuddin, Mohammed, Joy Winston, and Mohammed Qayyum. "A comprehensive survey: quantum cryptography." 2017 2nd international conference on anti-cyber crimes (ICACC). IEEE, 2017.

Li, Leilei, et al. "The security analysis of E91 protocol in collective-rotation noise channel." International Journal of Distributed Sensor Networks 14.5 (2018): 1550147718778192.

Trizna, Anastasija, and Andris Ozols. "An overview of quantum key distribution protocols." Inf. Technol. Manage. Sci 21 (2018): 37-44.

Padamvathi, V., B. Vishnu Vardhan, and A. V. N. Krishna. "Quantum cryptography and quantum key distribution protocols: A survey." 2016 IEEE 6th international conference on advanced computing (IACC). IEEE, 2016.

Goyal, Rohit. "Quantum Cryptography: Secure Communication Beyond Classical Limits." Journal of Quantum Science and Technology 1.1 (2024): 1-5.

Z. Yang, M. Zolanvari and R. Jain, "A Survey of Important Issues in Quantum Computing and Communications," in IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1059-1094, Secondquarter 2023, doi: 10.1109/COMST.2023.3254481.

Shim, K.-S. ., Kim, Y.- hwan ., Sohn, I. ., Lee, E. ., Bae, K.- il ., & Lee, W. . (2022). Design and Validation of Quantum Key Management System for Construction of KREONET Quantum Cryptography Communication. Journal of Web Engineering, 21(05), 1377–1418. https://doi.org/10.13052/jwe1540-9589.215.

M. S. Akter, J. Rodriguez-Cardenas, H. Shahriar, A. Cuzzocrea and F. Wu, "Quantum Cryptography for Enhanced Network Security: A Comprehensive Survey of Research, Developments, and Future Directions," 2023 IEEE International Conference on Big Data (BigData), Sorrento, Italy, 2023, pp. 5408-5417, doi: 10.1109/BigData59044.2023.10386889.

Kumari Neha, Internet Security, & Amrita Research Scholar. (n.d.). *Quantum cryptography - The future of communication and*. B R M College, Patna.

V. K. Ralegankar et al., "Quantum Cryptography-as-a-Service for Secure UAV Communication: Applications, Challenges, and Case Study," in IEEE Access, vol. 10, pp. 1475-1492, 2022, doi: 10.1109/ACCESS.2021.3138753.

Begimbayeva, Y., and T. Zhaxalykov. "Research of quantum key distribution protocols: BB84, B92, E91." Scientific Journal of Astana IT University (2022).

Lopes, Minal, and Nisha Sarwade. "Cryptography from quantum mechanical viewpoint." arXiv preprint arXiv:1407.2357 (2014).

Jha, Vikas Kumar, and Pankaj Srivastava. "A Theoretical Model of Multi-user QKD Network as the Extension of E91 Protocol." International Journal of Information and Network Security 2.4 (2013): 311.

Moizuddin, Mohammed, Joy Winston, and Mohammed Qayyum. "A comprehensive survey: quantum cryptography." 2017 2nd international conference on anti-cyber crimes (ICACC). IEEE, 2017.

Warke, Aakash, Bikash K. Behera, and Prasanta K. Panigrahi. "Experimental realization of three quantum key distribution protocols." Quantum Information Processing 19.11 (2020): 407.