Journal of Information Systems Engineering and Management
2025, 10(27s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Advancing Quantum Key Distribution: Challenges, Trends, and Future Prospects

Ramakrishna Kolikipogu[1], Amarthaluri Tirupathaiah[2], Prabhakar Kandukuri[3], Badugu Raja Koti[4], C. Raghavendra[5], Salakapuri Rakesh[6*]

[1]*Department of Information Technology, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India.*
[2]*Department of CSE, St. Ann's College of Engineering and Technology Chirala, Andhra Pradesh, India.*
[3]*Department of AIML, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India*
[4]*Department of Computer Science Engineering, GITAM School of Technology, Visakhapatnam, Andhra Pradesh, India.*
[5]*Department of Cyber Security, CVR College of Engineering, Hyderabad, Telangana, India.*
[6]*Symbiosis Institute of Technology, Hyderabad Campus, Hyderabad, Symbiosis International University, Pune, India.*
**Corresponding Author Email: srakesh@sithyd.siu.edu.in*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 16 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

The quantum Key Distribution (QKD) is a cryptographical approach that practices quantum mechanical properties to make entirely secured keys for safe message transmission among multiple users. Substantial advancement has been acquiring QKD models and specifications in recent years. This article systematically examines QKD models involving the diverse QKD standards, advantages, difficulties, constraints, and encounters. The article finishes with the potential scope of QKD and its probable applications.

Keywords: Quantum Entanglement, error rate, Key Distribution, Key generation, Key rate, State of polarization.

1. INTRODUCTION

The primary motivation of this article is to conduct an in detailed investigation of the subject matter and present a thorough evaluation of the topic. The domain of cryptography has seen a substantial evolution as a result of the growing significance of security and privacy in the dynamic realm of modern data transmission and communication. Quantum Key Distribution (QKD) is an innovative methodology that has emerged from the foundational principles of quantum physics. This approach presents a paradigm shift in effectively addressing the persistent challenge of safeguarding sensitive information. In contrast to traditional cryptography methods that depend on computational complexity, Quantum Key Distribution (QKD) leverages the intrinsic chattels of quantum physics to establish enciphered keys that exhibit resistance to compromise [1]. This development signifies a notable shift within the realm of secure communication. Quantum Key Distribution (QKD) is grounded on two fundamental ideas, namely quantum entanglement and the non-cloning theorem. These concepts enable the creation of cryptographic keys that feature intrinsic characteristics to thwart eavesdropping and decoding efforts. The increasing interconnection of our digital environment has necessitated a greater emphasis on safeguarding data, resulting in the introduction of QKD as a viable method to ensuring robust data refuge [2]. This essay conducts a comprehensive investigation into Quantum Key Distribution (QKD), meticulously scrutinizing its theoretical foundations, unveiling its various practical applications, and closely exploring the intricate interplay between its advantages and challenges. The transformative capabilities of QKD are evidenced by its ability to greatly enhance secure communication across diverse sectors. Quantum Key Distribution (QKD) possesses a transformative potential that can bring about significant changes in diverse domains such as finance, government, healthcare, cloud computing, and the IoT [12]. The attainment of secure financial transactions, the enhancement of government and military communications, the preservation of patient data integrity, and the safeguarding of cloud-based systems against interception transcend ordinary aspirations. The attainment of these objectives becomes feasible with the advent of Quantum Key Distribution (QKD). This essay provides a thorough examination of quantum key distribution (QKD), delving into the subtle aspects of safe communication inside the quantum realm. This paper provides a comprehensive examination of various models

of Quantum Key Distribution (QKD), highlighting their potential to enhance communication security by using the enigmatic and occasionally contradictory principles of quantum mechanics. In addition, the essay examines many applications in which Quantum Key Distribution (QKD) have the capacity to revolutionize data protection, rendering it impervious to very sophisticated cyber assaults. However, despite its considerable promise, Quantum Key Distribution (QKD) faces several obstacles throughout its development. The creation of innovative solutions is vital to address the problems posed by operational distances, the complexities inherent in required technology, and the intricate nature of essential distribution processes. Notwithstanding the aforementioned challenges, the significance of quantum key distribution (QKD) in transforming secure communication remains unchanged. This analysis explores the complex interplay between advantages and challenges, leading to a nuanced perspective on the impact of Quantum Key Distribution (QKD) in constructing a safe and resilient digital future. In the subsequent segments, we will analyze the historic evolution of quantum key distribution (QKD) models, tracing their origins from the fundamental principles of quantum physics to their practical applications in the present day. A comprehensive examination is undertaken to assess the unique attributes of each model, considering their own merits and limitations. This paper offers a complete analysis of the intricate characteristics inherent in Quantum Key Distribution (QKD). The primary goal of this article is to offer a comprehensive knowledge of the development and progress of Quantum Key Distribution (QKD) by employing a method of comparative analysis, examining case studies, and exploring its practical applications in real-world scenarios. This paper examines the role of QKD in shaping a future that emphasizes security and resilience inside the digital realm.

The upcoming sections of our work are denoted as stated in section II. We covered the comprehensive literature survey of various QKD standards, and afterward, we addressed various QKD models with detailed comparative result analysis. Background knowledge of the ABE standards, chaotic hash techniques, and QKD approach is discussed, along with the integrated proposed work in Section III, then we discussed different latest applications of QKD standards for providing robust security and privacy to users' sensitive data and we conclude our with possible outcomes and future enhancements in section V.

2. RELATED WORK

The BB84 protocol in realistic QKD with tangled polarization photons called qubits has been extensively handled and explored in numerous situations, containing long-distance QKD over optical fibers and free-space channels [1]. Numerous advances and alternatives of the BB84 protocol have been aimed, such as decoy states, weak coherent pulses, and error alteration codes. The investigational enactment of the E91 QKD protocol portrayed in "Investigational quantum cryptanalytics" was a substantial milestone in advancing QKD [2]. It proved the possibility of tapping tangled states to confirm secure keys and opened up new avenues for research in entanglement-based QKD protocols. The proposition of using entangled states for QKD in "Long-Distance Bell-State Entanglement for Quantum Communication" paved the way for developing several entanglement-based QKD protocols, such as the E91 and SARG04 protocols [3]. These protocols have been studied extensively and have shown agreeing solutions in various experimental scenarios. The introduction of continuous-variable QKD using coherent states in "Continuous-variable QKD using coherent states" has presented a complementary style to producing reliable keys expending quantum states [4]. This improvement has numerous benefits over discrete-variable QKD, such as advanced key rates and better tolerance to loss and noise. The proposal of using decoy states to improve the security of QKD etiquettes counter to illegal incidents by eavesdroppers in "Decoy-state quantum key distribution" has led to substantial progresses in the performance of QKD protocols. Decoy-state QKD is more secure and efficient than conventional QKD practices and has been implemented experimentally in several scenarios [5]. The proposal of a device-independent QKD protocol that does not rely on conventions about the core workings of the systems used to generate and measure the quantum states in "System-autonomous QKD with confined Bell test" has opened up new avenues for research in QKD [6].

Table 1: Evolutionary history of QKD Models

Year	Development
1950s	Theoretical work on quantum mechanics begins.
1960s	Development of quantum cryptography begins.
1970s	First proposals for QKD
1984	BB84 protocol proposed

1991	E91 protocol proposed
1992	B92 protocol proposed
2002	First continuous variable QKD (CV-QKD) protocol proposed
2003	DPS protocol proposed
2004	SARG04 protocol proposed
2007	MDI protocol proposed
2010s	Increasing research into practical implementations of QKD
2020s	Continued research and development of QKD technologies

The Device-independent QKD has the potential to provide stronger security guarantees than traditional QKD protocols and has been studied extensively in recent years. In [7], the authors proposed a model that can be applied with regular optical mechanisms with low recognition efficacy and extremely noisy channels.

Table 2: Comparison table of all QKD Models w.r.t key and error rates

Model	Year	Protocol	Encoding Basis	Security	Key Rate	Distance	Error Rate
BB84	1984	Prepare and Measure	Two conjugate bases (rectilinear and diagonal)	Information-Theoretic Security	Up to 1 Mbps	Up to 400 km (with repeaters)	Up to 1%
B92	1992	Prepare and Measure	Two non-orthogonal states	Information-Theoretic Security	Up to 1/3 Mbps	Up to 50 km (with ideal conditions)	Up to 20%
E91	1991	Entanglement-Based	Bell states	Information-Theoretic Security	Up to 1 Mbps	Up to 120 km (with photons)	Up to 10%
SARG04	2004	Entangl	Singlet	Informatio	Up	Up to 144	Up

		eme nt-Bas ed	state s	n-Theor etic Secur ity	to 1/ 3 M bp s	km (with ideal condi tions)	to 10 %
MD I	200 7	Mea sure men t-Devi ce-Ind epe nde nt	Bell state s	Infor matio n-Theor etic Secur ity	U p to 1/ 3 M bp s	Up to 100 km (with photo ns)	U p to 2 0 %
CV-QK D	1999	Con tinu ous-Vari able	Cohe rent state s	Infor matio n-Theor etic Secur ity	U p to 1 G bp s	Up to 50 km (with high-qualit y comp onent s)	U p to 10 ^-2

Table 3: Comparison table of all Quantum Key Distribution Models w.r.t key generation time and efficiency

Protocol	Number of qubits	Efficiency	Key generation time	Encryption time	Decryption time
BB84	2 per bit of key	25-50%	microseconds to milliseconds per qubit	microseconds to milliseconds per qubit	microseconds to milliseconds per qubit
B92	1 per bit of key	50%	microseconds to milliseconds per qubit	microseconds to milliseconds per qubit	microseconds to milliseconds per qubit
E91	1 per bit of key	50%	microseconds to milliseconds per qubit	microseconds to milliseconds per qubit	microseconds to milliseconds per qubit
SARG04	3 per bit of key	up to 91%	milliseconds per qubit	microseconds to milliseconds per qubit	microseconds to milliseconds per qubit
DPS	2 per bit of key	up to 95%	milliseconds per qubit	microseconds to milliseconds per qubit	microseconds to milliseconds per qubit

MDI	2 per bit of key	up to 90%	milliseconds per qubit	microseconds to milliseconds per qubit	microseconds to milliseconds per qubit
CV-QKD	Infinite	up to 90%	microseconds to milliseconds per pulse	microseconds to milliseconds per pulse	microseconds to milliseconds per pulse

Here the idea varies with the other existing approach solution of full device-independent QKD in that it doesn't depend on detectors with near-perfect detection efficacy, qubit amplifiers upon teleportation, or quantum no demolition dimension of photon pulsations. In [8], The purported CV-QKD system can achieve a key_rate of 90 kbit/s from a distance of 20 km, believing an idyllic QKD device multiplexed with 2-mW optical power. Additionally, the authors effectively proved, for the first time, the encipherment of a 10GE client service over a installable optical communication network legacy paraphernalia using the CV-QKD above system over a 20 km distance. In [9], the authors surveyed the QKD protocols. Also, presented a little experiment of some QKD protocols such as DPS, B92, and BB84 etc.

Table 4: comparison table of all QKD Models w.r.t limitations and challenges

Model	Description	Applicability	Advantages	Disadvantages	Limitations	Challenges
BB84	Uses two non-orthogonal bases to represent polarization of photons	Short-distance communication	High security, conceptually simple	Susceptible to loss and noise, requires trusted sources and detectors	Limited distance, requires expensive hardware	Development of practical QKD systems
B92	Uses single-photon states to transmit key	Short-distance communication	High security, simpler implementation than BB84	Limited distance, vulnerable to some attacks	Limited to short distances, requires low-loss channel	Improving distance and key rate
E91	Uses quantum entanglement to transmit key	Long-distance communication	High security, no assumption on measurement devices	Limited to few km, requires loss-tolerant detectors and stable entanglement	High resource requirements, limited scalability	Improving distance and scalability, practical implementation
SARG04	Uses four non-orthogonal states in two non-orthogonal bases	Short-distance communication	High security, relatively simple implementation	Susceptible to loss and noise, limited distance	Limited distance, requires low-loss channel	Improving key rate and distance
DPS	Uses dual-rail encoding with single or two photons	Short-distance communication	High key rate, may be instigated expending off-	Vulnerable to photon number splitting	Limited distance, less secure than information-	Improving security and distance

			the-shelf apparatuses	attack, limited distance	theoretic protocols	
MDI	Uses interference between two photons to transmit key	Long-distance communication	High security, no assumption on measurement devices	Limited to few hundred km, requires loss-tolerant detectors and stable entanglement	High resource requirements, limited scalability	Improving distance and scalability, practical implementation
CV-QKD	Uses quadrature amplitude modulation for continuous variables	Long-distance communication	High key rate, implementation using existing optical technology	Susceptible to homodyne detector attacks, limited distance	Limited distance, less secure than information-theoretic protocols	Improving security and distance

2.1. DEVELOPMENT HISTORY OF QKD

Quantum Key Distribution (QKD) has undergone significant advancements since its inception, rooted in the foundational principles of quantum mechanics formulated in the 1950s. The initial theoretical exploration of quantum cryptography in the 1960s laid the groundwork for subsequent developments in QKD protocols.

- In 1984, Charles Bennett and Gilles Brassard introduced the first practical QKD protocol, known as BB84, which leverages the principles of quantum mechanics to ensure secure communication. This protocol uses polarized photons to encode bits and provides information-theoretic security, meaning its security is based on the laws of physics rather than computational hardness.
- The 1991 proposal of the E91 protocol by Artur Ekert marked a significant milestone by introducing entanglement-based QKD. This protocol utilizes entangled photon pairs and the violation of Bell's inequalities to guarantee secure key distribution, offering an alternative approach to the prepare-and-measure paradigm of BB84.
- The 1992 B92 protocol, proposed by Charles Bennett, simplified QKD by using only two non-orthogonal states. This reduction in complexity made the protocol easier to implement but introduced new challenges in terms of security and distance limitations.

2.2. INNOVATIONS AND ADVANCEMENTS IN QKD

Numerous innovations have emerged to address the limitations of early QKD protocols, enhancing their security, efficiency, and practical applicability:

- Decoy States: Introduced in "Decoy-state quantum key distribution" (2003), decoy states are used to thwart eavesdropping attempts by varying the intensity of the photon pulses. This technique enhances the security and efficiency of QKD protocols and has been implemented in various experimental setups.
- Weak Coherent Pulses: Utilizing weak coherent pulses instead of single photons helps mitigate issues related to photon number splitting attacks, thereby improving the security of QKD systems.
- Error Correction Codes: Advanced error correction codes have been integrated into QKD protocols to improve their resilience against noise and loss, thereby extending the viable communication distance.
- Continuous-Variable QKD (CV-QKD): First proposed in "Continuous-variable QKD using coherent states" (2002), CV-QKD represents a shift from discrete-variable to continuous-variable encoding. This approach leverages quadrature amplitude modulation, offering higher key rates and better noise and loss tolerance than discrete-variable QKD.
- Device-Independent QKD (DI-QKD): The concept of DI-QKD, proposed in "System-autonomous QKD with confined Bell test" (2007), aims to eliminate the need for trust in the internal workings of the quantum devices used. By relying solely on the observed correlations between measurement outcomes, DI-QKD provides stronger security guarantees and opens new research avenues.

2.3.. EXPERIMENTAL MILESTONES

The practical implementation of QKD has seen significant milestones:

- E91 QKD Protocol: Demonstrated in "Investigational quantum cryptanalytics" (1991), the experimental implementation of the E91 protocol validated the use of entangled states for secure key distribution, spurring further research in entanglement-based QKD.
- Long-Distance QKD: Advances in optical fiber technology and free-space communication have enabled long-distance QKD. Experimental setups have achieved key distribution over distances up to 400 km using repeaters and advanced error correction techniques.
- Field Deployment: Recent experiments, such as those described in "Decoy-state quantum key distribution" and subsequent studies, have demonstrated the feasibility of QKD over existing optical communication networks, paving the way for real-world applications.

3. QUANTUM KEY DISTRIBUTION MODELS EXPERIMENTAL ANALYSIS

Several QKD models, including the BB84 protocol, are the most widely used one. Other protocols include the E91 standard, the SARG04 standard, the B92 protocol, the six-state standard, and the decoy state protocol. Each of these protocols has different characteristics and advantages, but they all rely on the characteristics of quantum mechanics to generate secure keys. QKD emerged in the 1970s, and the first QKD standard, the BB84 protocol, was anticipated in 1984 [10]. Here is an evolutionary table for QKD models and related developments from 1950 to 2023:The primary advantage of QKD is that it offers unconditionally secure communication. This means that even if an eavesdropper intercepts the key, it cannot use it to decode the message. Additionally, QKD provides perfect forward secrecy, which means that if an attacker gains access to the key later, they cannot see it to decode past messages. QKD is also resistant to traditional cryptographic attacks, such as brute force attacks. Although QKD has many pros in its counterparts, it has a few restrictions also. One of the primary restrictions is the remoteness over which QKD can function. It needs an explicit optical fiber connection between the source and destination, and the gap over which QKD can be completed is constrained by the loss of photons in the fiber. Also, QKD is exposed to side-channel attacks, letting an attacker mine information about the key without immediately interrupting it. Another limitation of QKD is the complexity and expense of the equipment expected. QKD wants dedicated hardware involving single-photon detectors, which can be costly. Furthermore, mounting QKD equipment can be complicated and requires experienced workers. Numerous challenges face the adoption of QKD as a standard for secure communication. The primary challenge is the development of practical QKD systems that are easy to use and deploy. Furthermore, the cost and complexity of QKD equipment need to be reduced to make it more available to a broader audience. There is also a necessity for consistent testing processes to assess the safety of QKD systems.

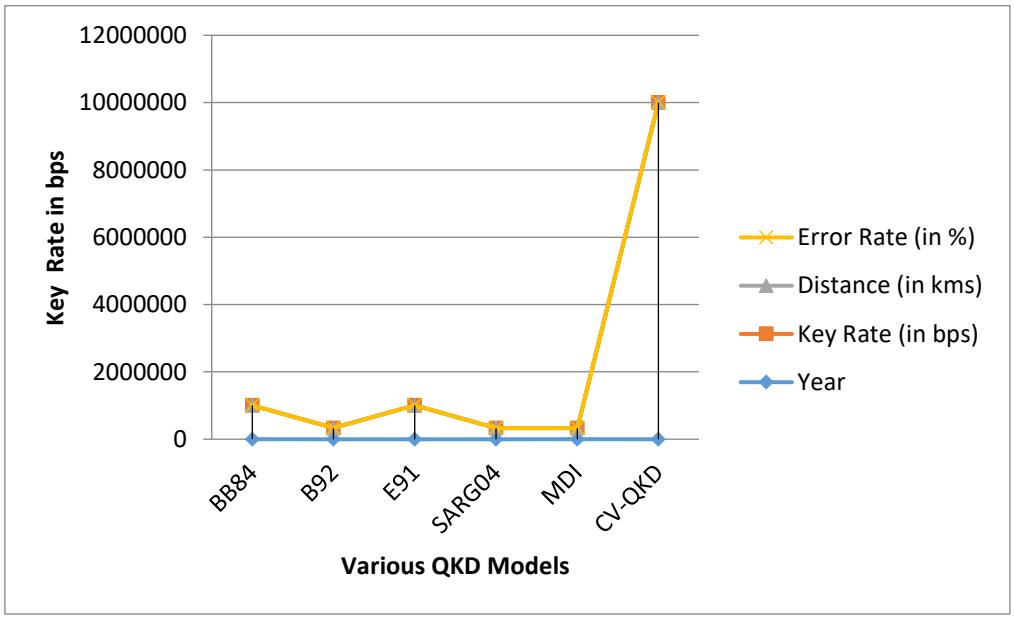

Figure 1: comparative analysis of all QKD Models w.r.t key rate

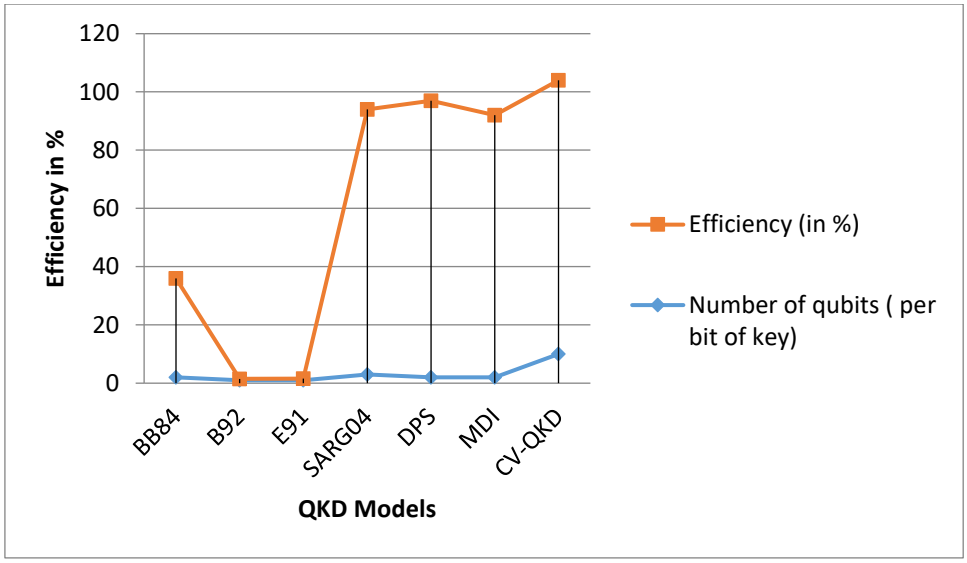

Figure 2: Comparative analysis of all QKD Models w.r.t efficiency

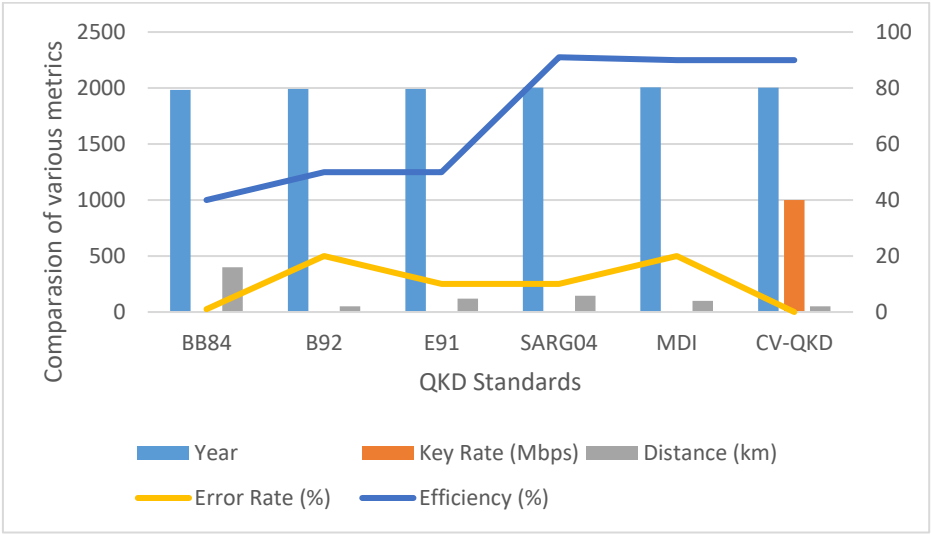

Figure 3: Comparative simulation result analysis of various QKD Models w.r.t various metrics

4. QKD PRINCIPLES WITH MATHEMATICAL DERIVATIONS

Quantum Key Distribution (QKD) allows two parties, typically referred to as Alice and Bob, to generate a shared secret key with information-theoretic security, guaranteed by the principles of quantum èmechanics. This section aims to elucidate the fundamental principles of QKD, focusing on the BB84 protocol, and includes essential mathematical derivations to clarify the underlying concepts.

Principles of QKD: The BB84 Protocol

Quantum States and Bases: In the BB84 protocol, information is encoded using the polarization states of photons. There are two bases used for encoding:

- **Rectilinear (or Z) Basis**: |0⟩(horizontal) and |1⟩ (vertical).
- **Diagonal (or X) Basis**: |+⟩=1/sqrt(2) ((|0⟩+|1⟩) and |−⟩

The choice of basis is random for each bit, providing security against eavesdropping.

Quantum State Preparation: Alice randomly selects a bit (0 or 1) and a basis (Z or X) for each photon. The photon is then prepared in the corresponding state:

- If the bit is 0 and the basis is Z, the state is |0⟩.

- If the bit is 1 and the basis is Z, the state is $|1\rangle$.
- If the bit is 0 and the basis is X, the state is $|+\rangle$.
- If the bit is 1 and the basis is X, the state is $|-\rangle$.

Quantum State Transmission and Measurement: Alice sends the prepared photon to Bob, who randomly selects a basis (Z or X) to measure the photon:

- If Bob's measurement basis matches Alice's preparation basis, he correctly identifies the bit.
- If the bases do not match, Bob's measurement result is random, and he obtains no useful information about Alice's bit.

Mathematically, if Alice sends a photon in state $|\psi\rangle$ and Bob measures in a basis $\{|0\rangle,|1\rangle\}$, the probability P of Bob measuring the state $|\phi\rangle$ is given by: $P(\phi|\psi)=|\langle\phi|\psi\rangle|^2$, For example, if Alice sends $|+\rangle$ and Bob measures in the Z basis, the probabilities are: $P(0|+)=|\langle 0|+\rangle|^2 = ½$, $P(1|+)=|\langle 1|+\rangle|^2 = 1/2$

4. Key Sifting: After the transmission, Alice and Bob publicly announce their bases (without revealing the actual bits). They retain only the bits where their bases match, discarding the others. This process is known as **sifting**.

5. Error Correction and Privacy Amplification: To ensure the key is error-free and secure from eavesdroppers (Eve), Alice and Bob perform error correction and privacy amplification:

- **Error Correction**: Alice and Bob exchange information over a classical channel to correct any discrepancies in their keys.
- **Privacy Amplification**: They apply hash functions to reduce the knowledge Eve might have gained, resulting in a shorter but secure key.

Mathematical Formulation of Security: The security of the BB84 protocol is based on the no-cloning theorem and the principles of quantum mechanics. Key aspects include:

Information Gain vs. Disturbance: Any attempt by Eve to gain information about the key disturbs the quantum states, which can be detected by Alice and Bob. If Eve intercepts and measures a photon, she introduces errors detectable through the quantum bit error rate (QBER). The probability P_E that Eve guesses correctly without causing disturbance is limited by: $PE=1/2 + \epsilon$, where ϵ is a small disturbance. The error rate e introduced by Eve is related to her information gain I_E by: $e \approx I_E/2$

Privacy Amplification: The final key length all after privacy amplification is given by: $l \leq n[1-H(e)] - \lambda$, where n is the length of the sifted key, H(e) is the binary entropy function, and λ accounts for the information leaked during error correction.

5. QKD APPLICATIONS

QKD has several probable apps in various disciplines, such as healthcare, government and military connections, financial communications, cloud processing, and the IoT. For instance, in financial transactions, QKD can provide a secure way to protect sensitive information, such as online banking and stock trading. Similarly, QKD can secure government and military communications such as diplomatic cables and classified information. In healthcare, QKD can safeguard patient data and preserve personal medicinal data secluded and reliable. Furthermore, QKD can protect data in cloud computing systems from interception and theft. In IoT, QKD can secure communication among devices, ensuring that transmitted data is kept confidential and cannot be accessed by illicit parties. In the article [11], the authors presented a new approach for quantum integrity-based validation and key arrangement in cloud server construction. This scheme leverages the principles of quantum cryptography, a necessary expertise for guaranteeing confidentiality and concealment in data and network security. A proper investigation has been conducted with help of the AVISPA software to evaluate the safety of the anticipated standard. The safety investigational analysis results demonstrate that the anticipated standard is resilient over all types of attacks, thus confirming its effectiveness in ensuring security. In [12], authors combined the chaotic CPABE model with the QKD model to provide protection and confidentiality to the IIoT-based user's sensitive information. In [13] [14] work, authors addressed the safety methods for the cloud by proposing an advanced hash-based CPABE standard to advance the safety and secrecy of the cloud user's personal info, including unstructured data. In [15] [16], a dynamical

randomized quantum key distribution model combined with hash-based CPABE to improve the fortification of cloud consumer-sensitive data. In this model, both unstructured and structured massive volume-sized healthcare datasets are employed as inputs. In [17] [18] [19], novel chaotic integrity and QKD-centered CPABE standard used over the cloud platforms and investigational fallouts demonstrated that the anticipated standard had elevated computational capacity, limited storage cost, and safe key circulation related to old ABE standards. On top of a secure blockchain paradigm, the authors applied a non-linear dynamic polynomial chaotic quantum hash algorithm that can be employed to increase cloud consumer security while preserving user confidentiality. Both organized and disorganized large-scale clinical data are considered inputs in the suggested approach for trustworthy corroboration and encoding, which proved more efficient compared to traditional ABE models [20]. In [21], the authors applied new dynamical chaotical maps to quantum-based CPABE standards to improve cloud security and privacy. Applied experimental outcomes proved that the anticipated standard has competent accurateness in tenures of enciphered and deciphered time and enough storage compared to the traditional ABE standards. In [22], the authors projected a standard centered on blind quantum computing to protect communication among the cloud's consumers sensitive information, and service providers. They improved the hierarchal ABE model using BCQ key distribution, which offers consumers information affording and cluster access to consumers' sensitive information. The investigational outcomes prove that the anticipated standard is more effective than the prevailing standards. In [23] [24] [25] [26], the authors thoroughly inspected the "keys age" device and encipherment metrics utilized in cloud computing environments. As a result, they have proposed a new set of security mechanisms that aim to overcome existing limitations and vulnerabilities and consider using Quantum Key Allocation to strengthen the security of cloud computing systems. The proposed tools have been designed to address potential security threats and to provide enhanced protection against security breaches. In [27-31] the experimental configuration has been optimized for the photon stream. A photon stream is generated by laser light, and polarization is provided to the photon stream using a stepper motor controlled by an Arduino. An optical fiber cable transmits light from the sender to the receiver. At the receiver's end, light is captured using a photodiode.

6.CONCLUSION

Quantum Key Distribution is a novel expertise that utilizes the quantum mechanical properties to grant secure transmission channels. This intends that if an opponent captures the message, they cannot interpret the communicated data without interrupting it, notifying authentic users. QKD has the potential to revolutionize secure communication across different industries such as finance, defense, and healthcare. QKD can keep secure communication channels for high-frequency trading and financial transactions in the finance industry. In security, QKD can be used to secure military communication channels, which are exposed to interception by adversaries. In healthcare, QKD can prepare secure channels for transmitting sensitive patient information, such as medical records. Although the QKD is potential, several challenges must be addressed to make it a practical and cost-effective solution for secure communication. One of the significant challenges is the distance limitation of QKD, which is currently limited to a few hundred kilometers. Another challenge is the high cost of implementing QKD, which makes it prohibitive for many organizations. To conquered these encounters, researchers are actively developing new QKD protocols that can extend the distance restrictions of QKD and reduce its implementation cost. New technologies like quantum repeaters and quantum memories are also expanding to enable long-distance QKD communication. In conclusion, QKD is a promising technology that offers unconditionally secure transmission. With further research and development, QKD has the probable to develop a practical and cost-effective solution for certain information across different industries.

7.FUTURE SCOPE

The future scope of QKD is vast, and there are several probable apps for the technology. Secure networks for critical transportation, such as power grids and transportation networks, is one possible application. A potential alternative app is the secure transmission of medical data, with patient logs and diagnostic information. As the technology progresses, QKD will tend find its way into other areas, such as secure cloud computing, voting systems, and messaging platforms. In count to getting bigger of its application domains, investigators are also investigating paths to improve the performance of QKD systems. This includes developing more efficient QKD protocols, strengthening the distance over which QKD can be performed, and adjusting the speed and reliability of QKD systems. One area of research that shows promise is using artificial intelligence (AI) in QKD systems. AI can optimize QKD systems' performance, advance error correction and detection, and reduce the overall cost of QKD implementations. Another

domain of study is the expansion of quantum network infrastructures that can support the scaling of QKD systems. Quantum networks can attach multiple QKD systems, enabling secure communication across considerable distances and with more users. The future of QKD looks bright, with many exciting chances for technology. As researchers persist in fostering and processing QKD systems, we expect widespread adoption of this technology in various industries and applications, providing unparalleled protection and isolation.

REFERENCES

[1] P. W. a. J. P. Shor, "Simple proof of security of the BB84 quantum key distribution protocol," Physical review letters, vol. 85, no. 22, p. 441, 2000.

[2] A. e. a. Ling, "Experimental E91 quantum key distribution," Advanced Optical Concepts in Quantum Computing, Memory, and Communication , vol. 6903, no. 30, 2008.

[3] C. e. a. Branciard, "Security of two quantum cryptography protocols using the same four qubit states," Physical Review A, vol. 72, no. 3, 2005.

[4] P. e. a. Jouguet, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nature photonics, vol. 7, no. 5, pp. 378-381, 2013.

[5] X. e. a. Ma, "Practical decoy state for quantum key distribution," Physical Review A, vol. 72, no. 1, 2005.

[6] C. C. W. e. a. Lim, "Device-independent quantum key distribution with local Bell test," Physical Review X, vol. 3, no. 3, 2013.

[7] H.-K. M. C. a. B. Q. Lo, "Measurement-device-independent quantum key distribution," Physical review letters, vol. 108, no. 13, p. 130503, 2012.

[8] F. e. a. Karinou, "Toward the integration of CV quantum key distribution in deployed optical networks," IEEE Photonics Technology Letters, vol. 30, no. 7, pp. 650-653, 2018.

[9] A. I. a. N. R. S. Nurhadi, "Quantum key distribution (QKD) protocols: A survey," in 4th International Conference on Wireless and Telematics (ICWT). IEEE., Nusa Dua, Bali, Indonesia, 2018.

[10] V. e. a. Scarani, "The security of practical quantum key distribution," Reviews of modern physics, vol. 81, no. 3, p. 1301, 2009.

[11] G. a. S. K. Sharma, "Identity based secure authentication scheme based on quantum key distribution for cloud computing.," Peer-to-Peer Networking and applications, vol. 11, pp. 220-234, 2018.

[12] K. K. e. a. Singamaneni, "A novel QKD approach to enhance IIOT privacy and computational knacks," Sensors , vol. 22, no. 18, p. 6741, 2022.

[13] K. K. e. a. Singamaneni, "An Efficient Hybrid QHCP-ABE Model to Improve Cloud Data Integrity and Confidentiality," Electronics , vol. 11, no. 21, p. 3510, 2022.

[14] H. e. a. Ghayvat, "CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications," IEEE Journal of Biomedical and Health Informatics , pp. 1937-1948., 2021.

[15] K. K. e. a. Singamaneni, "An Enhanced Dynamic Nonlinear Polynomial Integrity-Based QHCP-ABE Framework for Big Data Privacy and Security," Security and Communication Networks , vol. 20, no. 22, 2022.

[16] B. R. S. S. S. a. M. S. Y. L. Kanth, Int. J. Comput. Trends Technol., vol. 16, no. 5, p. 204–207, 2014.

[17] K. K. a. P. S. N. Singamaneni, "An efficient quantum hash-based CP-ABE framework on cloud storage data," International Journal of Advanced Intelligence Paradigms, vol. 22, no. 3, pp. 336-347, 2022.

[18] L. e. a. Yuchuan, " "Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage.," China Communications, vol. 11, pp. 114-124, 2014.

[19] I. e. a. Gupta, "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions.," IEEE Access, (2022)..

[20] K. K. e. a. Singamaneni, "A novel blockchain and Bi-linear polynomial-based QCP-ABE framework for privacy and security over the complex cloud data," Sensors , vol. 21, no. 21, p. 7300, 2021.

[21] K. K. a. S. N. P. Singamaneni, "An improved dynamic polynomial integrity based QCP-ABE framework on large cloud data security.," International Journal of Knowledge-Based and Intelligent Engineering Systems, vol. 24, no. 2, pp. 145-156, 2020.

[22] K. K. a. P. S. N. Singamaneni, "IBLIND Quantum Computing and HASBE for Secure Cloud Data Storage and Accessing," Revue d'Intelligence Artificielle, vol. 33, no. 1, pp. 33-37, 2019.

[23] K. K. a. P. N. Singamaneni, "Secure key management in cloud environment using quantum cryptography," Ingénierie des Systèmes d'Information, vol. 23, no. 5, pp. 213-222, 2018.

[24] O. K. J. e. a. Mohammad, "Securing cloud computing environment using a new trend of cryptography," 2015 International Conference on Cloud Computing (ICCC). IEEE, , 2015..

[25] C. e. a. Liu, "Multicarrier multiplexing continuous-variable quantum key distribution at terahertz bands under indoor environment and in inter-satellite links communication.," IEEE Photonics Journal , vol. 13, no. .4 , pp. 1-13, (2021.

[26] G. e. a. Vest, " Design and evaluation of a handheld quantum key distribution sender module," IEEE journal of selected topics in quantum electronics , vol. 21, no. 3, pp. 131-137, 2014 .

[27] K. K. P. S. N. a. P. V. S. K. Singamaneni, "Efficient quantum cryptography technique for key distribution," Journal Européen des Systèmes Automatisés, vol. 51, no. 4, pp. 283-293, 2018.

[28] J. a. C. R. F.-P. Capmany, " Analysis of passive optical networks for subcarrier multiplexed quantum key distribution," IEEE transactions on microwave theory and techniques , vol. 58, no. 11, pp. 3220-3228, 2010.

[29] Y. e. a. Cao, "Time-scheduled quantum key distribution (QKD) over WDM networks," Journal of Lightwave Technology , vol. 36, no. 16, pp. 3382-3395, 2018.

[30] W.-K. a. S. O. H. Lee, " "High throughput implementation of post-quantum key encapsulation and decapsulation on GPU for Internet of Things applications," " IEEE Transactions on Services Computing , vol. 15, no. 6, pp. 3275-3288, 2021.

[31] Singamaneni, Kranthi Kumar, Ghulam Muhammad, and Zulfiqar Ali. "A Novel Multi-Qubit Quantum Key Distribution Ciphertext-Policy Attribute-Based Encryption Model to Improve Cloud Security for Consumers." IEEE Transactions on Consumer Electronics (2023).

[32] Singamaneni, K.K., Budati, A.K. & Bikku, T. An Efficient Q-KPABE Framework to Enhance Cloud-Based IoT Security and Privacy. Wireless Pers Commun (2024). https://doi.org/10.1007/s11277-024-10908-8

[33] K. K. Singamaneni, G. Muhammad and Z. Ali, "A Novel Quantum Hash-Based Attribute-Based Encryption Approach for Secure Data Integrity and Access Control in Mobile Edge Computing-Enabled Customer Behavior Analysis," in IEEE Access, vol. 12, pp. 37378-37397, 2024, doi: 10.1109/ACCESS.2024.3373648.

[34] Singamaneni, K.K., Yadav, K., Aledaily, A.N. et al. Decoding the future: exploring and comparing ABE standards for cloud, IoT, blockchain security applications. Multimed Tools Appl (2024). https://doi.org/10.1007/s11042-024-19431-1.