10.48047/jocaaa.2022.30.02.74

Advanced Quantum Key Distribution Techniques for Secure Post-Quantum Communication Networks: A Comprehensive Study

Hridesh Gupta
Ph.D. - Research Scholar, Department of Computer Science, C.S.J.M. University, Kanpur.
hhrideshh@gmail.com

Dr. Sandesh Gupta
Department of Computer Science, Faculty of Computer Science, C.S.J.M. University, Kanpur.

Abstract

The rapid advancement of quantum computing has created significant challenges for conventional cryptographic systems that rely on computational complexity for security. Public-key algorithms such as RSA, Diffie–Hellman, and Elliptic Curve Cryptography are expected to become vulnerable once large-scale quantum computers become practical. Quantum Key Distribution (QKD) has emerged as one of the most promising technologies for ensuring secure communication by utilizing the fundamental principles of quantum mechanics rather than mathematical assumptions. Unlike traditional encryption techniques, QKD enables two communicating parties to generate a shared secret key while guaranteeing that any eavesdropping attempt can be detected through the disturbance introduced into quantum states. This paper presents a comprehensive study of advanced Quantum Key Distribution techniques and their role in securing post-quantum communication networks. The research examines the theoretical foundations of quantum communication, including quantum superposition, entanglement, Heisenberg's uncertainty principle, and the no-cloning theorem. Various QKD protocols such as BB84, B92, E91, and SARG04 are analyzed with respect to their operational mechanisms, security characteristics, implementation requirements, and practical limitations. The study further investigates different attack models, including intercept-resend attacks, photon-number splitting attacks, Trojan horse attacks, and side-channel attacks, together with modern countermeasures developed to enhance protocol robustness. Practical implementation aspects of QKD using optical fibers, free-space optical communication, and satellite-based quantum communication are also discussed. The paper highlights the integration of QKD with existing classical communication infrastructures to facilitate secure communication in government organizations, financial institutions, healthcare systems, cloud computing platforms, military networks, and Internet of Things (IoT) environments. Furthermore, the study reviews recent developments in quantum repeaters, trusted-node architectures, and quantum networks that enable long-distance secure communication. Finally, the paper identifies current technological challenges including transmission losses, hardware imperfections, limited communication distance, detector vulnerabilities, implementation costs, and standardization issues. It concludes that Quantum Key Distribution represents a fundamental component of future cybersecurity infrastructures and will play an increasingly significant role in protecting digital communications against both classical and quantum-enabled cyber threats.

10.48047/jocaaa.2022.30.02.74

Keywords: Quantum Key Distribution, Quantum Communication, Quantum Cryptography, BB84 Protocol, Post-Quantum Security, Quantum Networks, Secure Communication, Quantum Computing.

Introduction

The rapid evolution of information technology has transformed digital communication into an essential component of modern society. Governments, financial institutions, healthcare organizations, educational institutions, military agencies, and cloud service providers continuously exchange enormous volumes of confidential information through interconnected communication networks. The security of these communications primarily depends upon cryptographic algorithms that ensure confidentiality, integrity, authentication, and non-repudiation. However, recent advances in quantum computing have raised serious concerns regarding the long-term security of conventional cryptographic systems.

Traditional public-key cryptographic algorithms, including RSA, Diffie–Hellman, and Elliptic Curve Cryptography (ECC), derive their security from the computational difficulty of mathematical problems such as integer factorization and discrete logarithms. Classical computers require an impractical amount of time to solve these problems when sufficiently large key sizes are employed. Nevertheless, the emergence of quantum computers capable of executing Shor's algorithm dramatically changes this security assumption. A sufficiently powerful quantum computer can efficiently solve these mathematical problems, rendering many widely deployed cryptographic protocols insecure.

Quantum Key Distribution (QKD) has emerged as one of the most promising solutions for addressing these challenges. Unlike conventional cryptographic techniques that rely upon computational assumptions, QKD provides information-theoretic security based on the fundamental laws of quantum mechanics. The security of QKD does not depend upon the computational power available to an adversary but instead relies on physical principles such as quantum superposition, quantum entanglement, Heisenberg's uncertainty principle, and the no-cloning theorem. These principles ensure that any attempt by an unauthorized party to observe transmitted quantum information inevitably introduces detectable disturbances, enabling legitimate users to identify the presence of an eavesdropper.

Since the introduction of the BB84 protocol by Bennett and Brassard in 1984, Quantum Key Distribution has experienced remarkable theoretical and experimental advancements. Numerous QKD protocols have been proposed to improve security, efficiency, communication distance, and implementation feasibility. Significant progress has also been achieved in optical communication technologies, single-photon generation, quantum repeaters, satellite-based quantum communication, and integrated photonic devices, making practical deployment increasingly realistic.

Modern communication infrastructures demand security solutions capable of protecting sensitive information not only against current cyber threats but also against future attacks involving quantum computers. Governments across the world are investing heavily in quantum technologies to establish quantum communication networks capable of supporting national cybersecurity infrastructures. Financial institutions, healthcare systems, defense organizations, and critical infrastructure providers are similarly exploring QKD as a means of ensuring long-term confidentiality for highly sensitive data.

10.48047/jocaaa.2022.30.02.74

Despite these advances, several practical challenges remain. Quantum channels suffer from photon loss, environmental noise, detector imperfections, limited transmission distance, and high implementation costs. Furthermore, practical QKD systems remain vulnerable to implementation-specific attacks, including detector blinding attacks, photon-number splitting attacks, Trojan horse attacks, and various side-channel attacks. Consequently, ongoing research focuses not only on improving protocol security but also on developing cost-effective hardware, robust countermeasures, and standardized implementation frameworks.

This paper provides a comprehensive review of advanced Quantum Key Distribution techniques for secure post-quantum communication networks. The study discusses the theoretical foundations of quantum cryptography, analyzes major QKD protocols, evaluates practical implementation methods, investigates common security threats, examines real-world applications, and highlights emerging research directions that will shape the future of secure quantum communications.

Objectives of the Study

The primary objectives of this research are:

1. To examine the theoretical principles underlying Quantum Key Distribution.
2. To analyze major QKD protocols including BB84, B92, E91, and SARG04.
3. To investigate security threats and attack models affecting practical QKD systems.
4. To evaluate practical implementation technologies used in quantum communication.
5. To explore real-world applications of QKD across various industrial sectors.
6. To identify current research challenges and future opportunities in post-quantum secure communication.

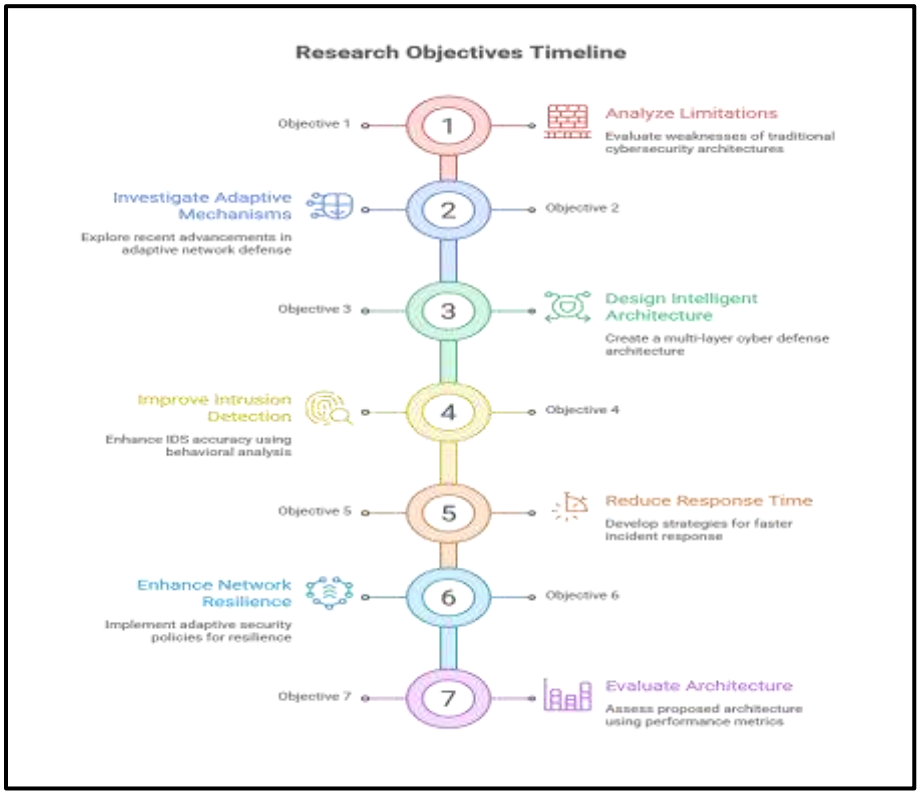

Fig. 1 Major research flow and objectives

10.48047/jocaaa.2022.30.02.74

Literature Review

Quantum Key Distribution (QKD) has evolved into one of the most significant research areas in quantum cryptography due to its ability to provide unconditional security based on the principles of quantum mechanics. Since its introduction in the early 1980s, numerous theoretical and experimental studies have contributed to improving the efficiency, security, scalability, and practical implementation of QKD systems. This section reviews the major contributions made by researchers toward the development of secure quantum communication.

The foundation of quantum cryptography was established by **Bennett and Brassard (1984)** through the introduction of the **BB84 protocol**, which demonstrated for the first time that cryptographic keys could be securely exchanged using quantum states. The protocol exploits the uncertainty principle of quantum mechanics, ensuring that any eavesdropping attempt introduces detectable disturbances in the transmitted photons. This pioneering work laid the foundation for modern quantum cryptography and remains the most widely implemented QKD protocol.

Ekert (1991) proposed the **E91 protocol**, introducing the concept of entanglement-based quantum key distribution. Unlike BB84, E91 relies on entangled photon pairs and Bell's theorem to guarantee communication security. This protocol demonstrated that quantum entanglement could provide stronger security guarantees while opening new possibilities for quantum networking and distributed quantum communication.

Bennett (1992) introduced the **B92 protocol**, which simplified quantum key distribution by employing only two non-orthogonal quantum states instead of four polarization states used in BB84. Although simpler in implementation, the protocol requires careful management of channel noise and detection efficiency to maintain security.

The first successful experimental implementation of quantum cryptography was reported by **Bennett et al. (1992)**. Their work demonstrated that quantum key distribution was not merely a theoretical concept but could be realized using practical optical communication equipment. This achievement encouraged extensive experimental research aimed at extending communication distances and improving system reliability.

The unconditional security of QKD over long communication distances was established independently by **Lo and Chau (1999)** and **Mayers (2001)**. Their security proofs demonstrated that the secrecy of generated keys remains intact regardless of the computational capabilities available to an adversary. These results significantly strengthened confidence in QKD as a future-proof cryptographic technology.

An important simplification of BB84 security analysis was presented by **Shor and Preskill (2000)**, who developed an elegant proof connecting quantum error correction with secure key generation. Their work remains one of the most influential theoretical contributions to quantum cryptography.

Gisin et al. (2002) published one of the earliest comprehensive reviews of quantum cryptography, discussing theoretical principles, experimental implementations, communication channels, practical limitations, and future research opportunities. Their survey became a foundational reference for researchers entering the field.

10.48047/jocaaa.2022.30.02.74

The practical security of quantum key distribution systems was comprehensively analyzed by **Scarani et al. (2009)**. Their work examined implementation-specific vulnerabilities, finite-key effects, detector imperfections, and realistic communication channels, highlighting the importance of bridging theoretical security proofs with practical deployment.

As implementation attacks became increasingly sophisticated, **Lo, Curty, and Qi (2012)** introduced **Measurement-Device-Independent Quantum Key Distribution (MDI-QKD)**. This protocol eliminates detector side-channel attacks by removing trust assumptions associated with measurement devices, representing one of the most significant advancements in practical QKD security.

Further improvements in practical implementations were discussed by **Diamanti et al. (2016)**, who investigated technological limitations affecting commercial deployment, including photon generation, detector efficiency, synchronization, channel losses, and system integration with existing optical communication networks.

The rapid development of satellite-based quantum communication significantly expanded QKD research. **Yin et al. (2017)** demonstrated long-distance entanglement distribution exceeding 1,200 kilometers using satellite platforms, while **Liao et al. (2017)** successfully implemented satellite-to-ground quantum key distribution, establishing the feasibility of global-scale quantum communication networks.

Comprehensive advances in quantum cryptography were summarized by **Pirandola et al. (2020)**, covering continuous-variable QKD, discrete-variable QKD, security proofs, quantum repeaters, network architectures, satellite communication, and emerging industrial applications. Their review reflects the maturity achieved by the field after nearly four decades of research.

Similarly, **Xu et al. (2020)** examined realistic QKD devices, analyzing finite-key security, practical detector vulnerabilities, source imperfections, and implementation challenges associated with commercial quantum communication systems.

One of the most significant milestones in practical deployment was reported by **Chen et al. (2021)**, who demonstrated an integrated space-to-ground quantum communication network spanning approximately 4,600 kilometers. This achievement illustrated the feasibility of combining terrestrial fiber networks with satellite communication to establish large-scale secure quantum communication infrastructures.

Overall, existing literature indicates that quantum key distribution has progressed from theoretical cryptographic concepts to practical communication systems capable of protecting sensitive information against both classical and quantum-enabled cyber threats. Nevertheless, challenges related to transmission distance, hardware complexity, implementation cost, network scalability, and protocol standardization continue to motivate ongoing research.

Research Gap

Despite substantial advancements in Quantum Key Distribution, several research challenges remain unresolved:

10.48047/jocaaa.2022.30.02.74

- Practical QKD systems continue to suffer from transmission losses and limited communication distances.
- Hardware imperfections create opportunities for implementation-specific attacks, including detector blinding and side-channel attacks.
- Large-scale integration of QKD with existing Internet and cloud infrastructures remains limited.
- The high cost of quantum hardware restricts widespread commercial adoption.
- Efficient quantum repeaters capable of enabling global quantum communication networks are still under active development.
- Standardized international protocols and interoperability frameworks are yet to be fully established.
- Hybrid architectures combining QKD with post-quantum cryptographic algorithms require further investigation.

Practical Implementation of Quantum Key Distribution

The practical implementation of Quantum Key Distribution (QKD) has progressed significantly over the past two decades. Initially considered a theoretical concept, QKD has evolved into a practical technology capable of securing communication across optical fiber networks, free-space optical links, and satellite communication systems. Advances in photonic devices, single-photon detectors, quantum repeaters, and integrated optical circuits have enabled researchers and industries to demonstrate secure quantum communication over increasingly longer distances. However, practical deployment requires overcoming challenges related to transmission loss, environmental interference, synchronization, and hardware imperfections.

Architecture of a Practical QKD System

A practical QKD system consists of both **quantum** and **classical** communication channels working together to establish a secure cryptographic key.

Main Components

1. **Alice (Sender)**
    - Generates random binary keys.
    - Encodes bits into quantum states.
    - Transmits photons through the quantum channel.
2. **Quantum Channel**
    - Optical fiber or free-space optical communication.
    - Carries quantum information encoded in photons.
3. **Bob (Receiver)**
    - Measures incoming photons using randomly selected bases.
    - Generates the raw key.
4. **Classical Communication Channel**
    - Authenticated but publicly accessible.
    - Used for basis reconciliation, error correction, and privacy amplification.
5. **Key Management System**
    - Stores and distributes the final secret key for encryption and decryption.

10.48047/jocaaa.2022.30.02.74

Optical Fiber-Based QKD

Optical fiber communication is the most widely used medium for implementing QKD because of its compatibility with existing telecommunication infrastructure.

Working Principle

Single photons generated by Alice travel through optical fibers to Bob. After transmission, both parties compare their measurement bases over an authenticated classical channel and derive the secret key.

Advantages

- High transmission stability.
- Compatible with existing fiber-optic networks.
- Low environmental interference.
- Suitable for metropolitan communication networks.

Limitations

- Photon attenuation limits communication distance.
- Signal loss increases with fiber length.
- Requires highly sensitive single-photon detectors.

Free-Space Quantum Communication

Free-space QKD transmits photons through the atmosphere instead of optical fibers.

Communication may occur between:

- Buildings
- Mobile platforms
- Aircraft
- Ground stations
- Satellites

Advantages

- No physical fiber installation required.
- Suitable for inaccessible geographical regions.
- Enables mobile secure communication.

Challenges

- Atmospheric turbulence.
- Weather conditions.
- Beam alignment.
- Background sunlight.
- Limited transmission reliability.

10.48047/jocaaa.2022.30.02.74

Satellite-Based Quantum Communication

Satellite-based QKD extends secure communication over thousands of kilometers by combining satellite links with terrestrial communication networks.

Operational Process

1. Quantum states are generated at a satellite or ground station.
2. Photons are transmitted through free space.
3. Ground stations perform quantum measurements.
4. Secret keys are generated after basis reconciliation.

Single-Photon Detectors

Single-photon detectors measure incoming quantum states with extremely high sensitivity.

Detector Types

- Avalanche Photodiodes (APDs)
- Superconducting Nanowire Single-Photon Detectors (SNSPDs)
- Photomultiplier Tubes (PMTs)

Performance Parameters

- Detection efficiency.
- Dark count rate.
- Timing accuracy.
- Recovery time.
- Operating temperature.

High detector efficiency directly improves secret key generation rates and communication distance.

Quantum Repeaters

One of the greatest challenges in quantum communication is photon loss over long distances.

Quantum repeaters extend communication distance by:

- Entanglement swapping.
- Quantum memory.
- Quantum error correction.
- Entanglement purification.

Current Challenges

- Quantum memory stability.
- High implementation complexity.
- Experimental limitations.

10.48047/jocaaa.2022.30.02.74

- Cost of deployment.

Integration with Classical Communication Networks

Complete replacement of existing communication infrastructure is economically impractical. Therefore, modern QKD systems are designed to operate alongside conventional networks.

Hybrid Architecture

The quantum channel distributes cryptographic keys, while the classical network transmits encrypted data using symmetric encryption algorithms such as AES.

Benefits

- Lower deployment cost.
- Compatibility with existing infrastructure.
- Easier commercial adoption.
- Enhanced long-term security.

Commercial QKD Systems

Several organizations have developed commercial QKD products for enterprise and government applications.

Major Features

- Secure key generation.
- Automatic key management.
- Real-time monitoring.
- Integration with existing encryption systems.
- Enterprise network compatibility.

These systems are increasingly used in sectors requiring high levels of information security.

- **Practical Challenges:** Despite remarkable progress, several implementation challenges remain.

- **Transmission Loss:** Photon absorption and scattering reduce communication distance.

- **Hardware Imperfections:** Real devices deviate from ideal theoretical models, creating security vulnerabilities.

- **Synchronization:** Accurate timing synchronization between sender and receiver is essential.

- **Environmental Noise:** Temperature variation, vibration, and atmospheric turbulence affect photon transmission.

10.48047/jocaaa.2022.30.02.74

- **Cost:** Quantum hardware remains expensive, limiting widespread deployment.
- **Scalability:** Building large-scale quantum communication networks requires substantial technological advancements.

Performance Evaluation Parameters

The performance of practical QKD systems is commonly evaluated using the following parameters:

Table 1 Major Parameter and description

Parameter	Description
Secret Key Rate	Number of secure bits generated per second
Quantum Bit Error Rate (QBER)	Percentage of incorrectly received quantum bits
Communication Distance	Maximum secure transmission range
Detection Efficiency	Probability of detecting incoming photons
Channel Loss	Optical attenuation during transmission
System Stability	Reliability under long-term operation
Security Level	Resistance against known quantum attacks

Challenges in Quantum Key Distribution

Despite significant progress in Quantum Key Distribution (QKD), several technical, operational, and economic challenges limit its widespread deployment. While QKD provides theoretically unconditional security, practical implementations are constrained by hardware limitations, communication infrastructure, and implementation complexity. Addressing these challenges is essential for realizing secure, large-scale quantum communication networks.

Limited Transmission Distance

One of the primary challenges in QKD is the limited communication distance. During transmission through optical fibers or free-space channels, photons experience attenuation due to absorption, scattering, and environmental disturbances. As the transmission distance increases, photon losses become more significant, reducing the secret key generation rate and communication reliability.

Although quantum repeaters have been proposed to overcome this limitation, practical and scalable quantum repeaters are still under development.

High Implementation Cost

Practical QKD systems require specialized hardware components, including:

- Single-photon sources
- High-efficiency photon detectors
- Quantum random number generators
- Precision optical components
- Synchronization equipment

10.48047/jocaaa.2022.30.02.74

The high cost of these components makes QKD deployment economically challenging, particularly for small and medium-sized organizations.

Hardware Imperfections

Theoretical QKD assumes ideal devices; however, real-world hardware exhibits imperfections such as:

- Detector inefficiency
- Dark counts
- Laser fluctuations
- Timing inaccuracies
- Polarization drift
- Optical component losses

These imperfections may introduce errors and create opportunities for implementation-specific attacks.

Scalability Issues

Current QKD implementations primarily support point-to-point communication. Developing large-scale quantum communication networks involving multiple users requires advanced quantum networking technologies, including quantum repeaters, quantum switches, and quantum routing protocols.

Integration with Existing Networks

Modern communication infrastructures are based on classical networking technologies. Integrating QKD with existing Internet, cloud computing, and telecommunication systems presents challenges related to compatibility, network management, synchronization, and protocol standardization.

Table 2: Yearly progress and major milestone

Year	Estimated Progress (%)	Major Milestone
2015	20%	Early superconducting and trapped-ion prototypes
2016	28%	Improved qubit coherence and cloud-based access begins
2017	36%	IBM and Rigetti expand quantum cloud services
2018	48%	Growth in quantum software frameworks (Qiskit, Cirq)
2019	60%	Google's "Quantum Supremacy" demonstration
2020	72%	Increased industrial investment and commercialization
2021	85%	NISQ-era hardware maturity and wider enterprise adoption

10.48047/jocaaa.2022.30.02.74

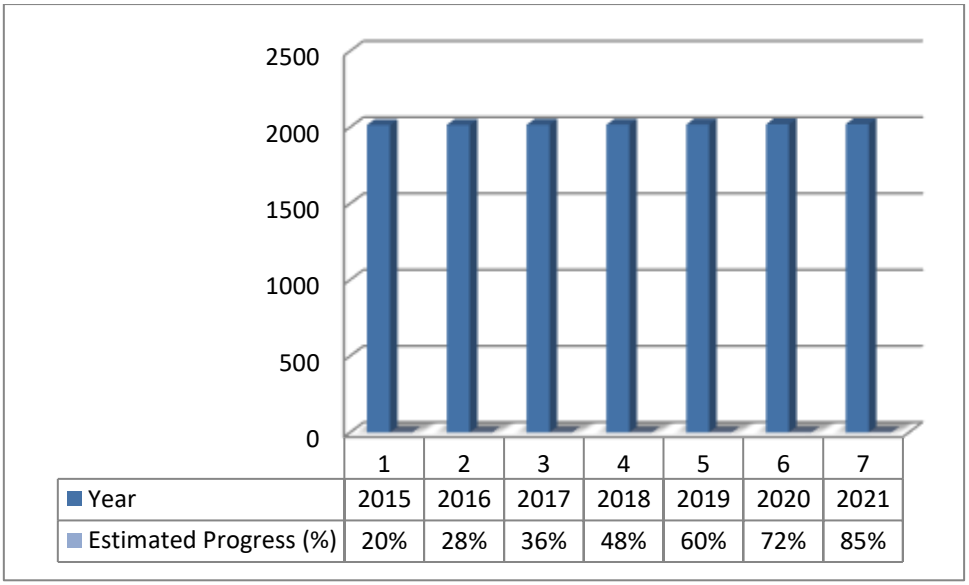

Fig. 2 Yearly progress analysis

Future Research Directions

Continuous advancements in quantum information science are expected to improve the efficiency, scalability, and practicality of Quantum Key Distribution systems.

Artificial Intelligence for Quantum Network Management

Artificial Intelligence (AI) and Machine Learning (ML) techniques can optimize QKD systems by:

- Predicting channel conditions.
- Detecting anomalies.
- Optimizing routing.
- Improving synchronization.
- Enhancing resource allocation.
- Detecting cyber threats.

AI-driven quantum network management is expected to improve the performance and reliability of future quantum communication infrastructures.

Conclusion

Quantum Key Distribution has emerged as one of the most promising technologies for ensuring secure communication in the post-quantum era. Unlike traditional cryptographic methods, whose security depends on the computational difficulty of mathematical problems, QKD derives its security directly from the fundamental principles of quantum mechanics. The use of quantum superposition, entanglement, the uncertainty principle, and the no-cloning theorem enables the secure generation and distribution of cryptographic keys while ensuring that any eavesdropping attempt can be detected. This study presented a comprehensive review of advanced Quantum Key Distribution techniques, beginning with the theoretical foundations of quantum communication and extending to practical

10.48047/jocaaa.2022.30.02.74

implementations and real-world applications. Major QKD protocols, including BB84, B92, E91, SARG04, Measurement-Device-Independent QKD, and Device-Independent QKD, were analyzed with respect to their operating principles, security characteristics, and implementation requirements. The study also examined practical deployment through optical fiber networks, free-space optical communication, and satellite-based quantum communication systems. Furthermore, the research discussed major security challenges affecting practical QKD implementations, including intercept-resend attacks, photon-number splitting attacks, detector blinding attacks, Trojan horse attacks, and side-channel attacks. Various countermeasures, such as decoy-state protocols, privacy amplification, Measurement-Device-Independent QKD, and hardware security improvements, were highlighted as effective approaches for enhancing system robustness. The paper also explored the growing applications of QKD in government communication, military networks, banking, healthcare, cloud computing, Internet of Things (IoT), telecommunications, satellite communication, and critical infrastructure protection. These applications demonstrate the practical significance of QKD in safeguarding sensitive information against both classical and quantum-enabled cyber threats. Despite its considerable advantages, several challenges remain before QKD can achieve widespread commercial deployment. These include limited communication distance, hardware imperfections, environmental noise, high implementation costs, scalability issues, and the need for international standards. Continued research in quantum repeaters, integrated photonic technologies, satellite communication, hybrid quantum-classical architectures, and the Quantum Internet is expected to address these limitations. In conclusion, Quantum Key Distribution represents a transformative advancement in secure communication and is expected to become a foundational component of next-generation cybersecurity infrastructures. As quantum computing continues to evolve, the integration of QKD with emerging communication technologies will play a crucial role in ensuring the long-term confidentiality, integrity, and resilience of digital communications worldwide.

References

1. Bennett, C. H., & Brassard, G. (1984). *Quantum cryptography: Public key distribution and coin tossing*. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 175–179.
2. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters, 67*(6), 661–663.
3. Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters, 68*(21), 3121–3124.
4. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (1992). Experimental quantum cryptography. *Journal of Cryptology, 5*(1), 3–28.
5. Brassard, G., & Salvail, L. (1994). Secret-key reconciliation by public discussion. In *Advances in Cryptology—EUROCRYPT'93* (pp. 410–423). Springer.
6. Lo, H. K., & Chau, H. F. (1999). Unconditional security of quantum key distribution over arbitrarily long distances. *Science, 283*(5410), 2050–2056.
7. Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters, 85*(2), 441–444.
8. Mayers, D. (2001). Unconditional security in quantum cryptography. *Journal of the ACM, 48*(3), 351–406.
9. Elliott, C. (2002). Building the quantum network. *New Journal of Physics, 4*, 46.
10. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics, 74*(1), 145–195.

10.48047/jocaaa.2022.30.02.74

11. Lo, H. K., Ma, X., & Chen, K. (2005). Decoy state quantum key distribution. *Physical Review Letters, 94*, 230504.
12. Pirandola, S., Braunstein, S. L., & Lloyd, S. (2008). Characterization of collective Gaussian attacks in quantum cryptography. *Physical Review Letters, 101*(20), 200504.
13. Peev, M., et al. (2009). The SECOQC quantum key distribution network in Vienna. *New Journal of Physics, 11*, 075001.
14. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics, 81*(3), 1301–1350.
15. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.
16. Sasaki, M., et al. (2011). Field test of quantum key distribution in the Tokyo QKD Network. *Optics Express, 19*(11), 10387–10409.
17. Lo, H. K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical Review Letters, 108*(13), 130503.
18. Imre, S., & Balazs, F. (2013). *Quantum Computing and Communications: An Engineering Approach*. Wiley.
19. Lo, H. K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. *Nature Photonics, 8*(8), 595–604.
20. Diamanti, E., Lo, H. K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Information, 2*, 16025.
21. Yin, J., et al. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science, 356*(6343), 1140–1144.
22. Liao, S. K., et al. (2017). Satellite-to-ground quantum key distribution. *Nature, 549*(7670), 43–47.
23. Yan, F. (Ed.). (2019). *Quantum Information Processing*. Springer.
24. Pirandola, S., Andersen, U. L., Banchi, L., et al. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics, 12*(4), 1012–1236.