VOL. 20, NO. 19, OCTOBER 2025 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

QUANTUM CRYPTOGRAPHY: ADVANCEMENTS AND CHALLENGES IN SECURE COMMUNICATION

Arifuzzaman and Iftikhar Ahmad
Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Kingdom of Saudi Arabia
E-Mail: aarifuzzaman@stu.kau.edu.sa

ABSTRACT

Quantum computing poses a crucial threat against traditional cryptographic systems because it creates substantial weakness in existing encryption standards. This paper examines the quantum cryptography field by studying its three main frameworks, including Quantum Key Distribution (QKD) and post-quantum cryptographic (PQC) algorithms and hybrid security approaches. The research paper evaluates quantum- based protocols BB84 and E91 and PQC schemes using lattice and code methods in addition to machine learning-enhanced cryptography by analyzing existing works. The paper explores critical problems involving high execution expenses alongside scalability limitations and infrastructure compatibility problems, as well as side-channel attack susceptibility. Healthcare practitioners must focus on developing standardized deployment techniques alongside strong implementation strategies because these measures become essential for IoT and smart cities. This paper brings together insights from more than twenty-four fundamental studies to simplify the understanding of existing conditions and establish directions for secure quantum communication systems.

Index Terms: quantum cryptography, quantum key distribution (QKD), post-quantum cryptography (PQC), secure communication, quantum computing threats.

Manuscript Received 12 November 2025; Revised 9 January 2026; Published 20 January 2026

1. INTRODUCTION

The quick development of quantum computing methods now produces major changes in information security, which threatens the underlying principles of classical cryptography. The RSA, ECC, and Diffie-Hellman cryptography protocols experience vulnerability when attacked by quantum algorithms like Shor's algorithm because these algorithms can easily break the mathematical problems of integer factorization and discrete logarithms [20]. Experts now face an imperative to build and deploy PQC systems that prevent quantum attacks since classical cryptography standards are failing to resist upcoming quantum computing power [13, 24].

The future of secure communication promises to be found with Quantum Cryptography (QC) because it implements quantum mechanics to establish encryption through secure channels. QKD and various QKD protocols under the category of quantum cryptographic protocols utilize quantum phenomena to establish unbreakable encryption systems through Quantum Key Distribution technology [17] [22]. QKD found its seminal realization in the BB84 and E91 protocols because they protect communications through quantum properties [26].

Quantum cryptography maintains excellent theoretical strength yet experiences major obstacles when applying it to practical use. Quantum cryptography remains restricted because of high implementation expenses, together with restricted scalability, essential hardware components, and diverse integration issues with conventional network systems [11, 19, 21]. Quantum communication systems require specific measures to defend against practical vulnerabilities, including side-channel attacks and environmental disturbances, because these issues threaten their operational integrity [27].

Parallel to quantum-based techniques, research in post- quantum algorithms-including lattice-based, code-based, multivariate, and hash-based cryptographic methods-aims to develop secure schemes that can operate on classical infrastructure while resisting quantum decryption [1], [13], [24]. These approaches are being actively standardized by bodies like NIST and offer practical alternatives for quantum- safe communication, especially for applications in constrained environments such as IoT and cloud computing [14], [25].

Research on post-quantum algorithms explores secure schemes through lattice-based cryptographic methods, as well as code-based, multivariate, and hash-based approaches. Their objective is to establish defenses against quantum decryption by operating on classical infrastructure [1, 13, 24]. NIST, alongside other bodies, maintains active standardization of security methods which provide practical quantum-resistant communication solutions, particularly for IoT devices and cloud-based operated systems [14, 25].

The study delivers an extensive review of quantum cryptographic practices alongside their application modes, technical restrictions, and progressive solutions to execution limitations. Recent research studies enable this paper to assess quantum-secure system effectiveness while identifying essential development needs to combat rapidly evolving quantum threats.

2. BACKGROUND

RSA and ECC security methods face serious dangers from quantum computing because Shor's and Grover's algorithms show researcher show to break these methods [5, 17, 20]. The two dominant research fields that address cryptographic vulnerabilities have become QKD and PQC. QKD implements quantum mechanics principles of superposition and entanglement to distribute secure keys, which theoretically protect against eavesdropping activities [6] [7] [17]. Lattice-based and hash-based methods represent PQC algorithms which developers create to deliver quantum-resistant encryption capabilities that operate on standard infrastructure [1], [13], [24].

The implementation of both solutions encounters real-world implementation constraints. QKD solution demands specific hardware equipment and exhibits limited scaling capabilities, yet PQC algorithms consume many computational resources, which restrict their applications in IoT networks [11, 25]. Research attempts to create hybrid systems which unite quantum devices with classical components to reach proper encryption deployment levels [16] [30]. The implementation of machine learning for cryptographic operations continues to grow steadily, but emerges as a challenge since it requires new security measures [9] [29]. The necessity to create secure, standardized quantum-resistant communication systems rises because of recent technological advancements.

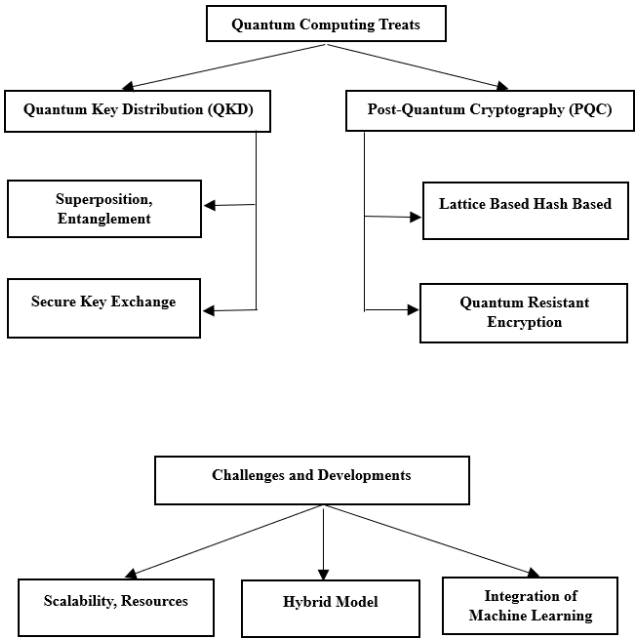

Figure-1. Overview of cryptographic strategies addressing quantum computing threats.

3. RELATEDWORK

Throughout the quantum computing age, quantum cryptography has proven to be the essential response for protecting against classical encryption flaws. RSA and ECC, along with other traditional cryptographic algorithms, face a threat of vulnerability from quantum computers implementing the algorithm named Shor's algorithm. Research and development of post-quantum cryptographic (PQC) techniques, such as lattice- based, code-based, and multivariate cryptographic methods, were created to protect against quantum attacks [1]. The latest homomorphic encryption techniques enable the execution of operations on encrypted information before any decryption occurs, which creates secure methods for processing cloud-based data [1]. The recent cryptographic advancements demonstrate the continuous advancement of security methods designed for maintaining secure communication systems after the quantum computing age.

The promising aspect of quantum cryptography includes Quantum Key Distribution (QKD) because it uses quantum mechanical principle stod is tribute keys while detecting eaves- dropping [2]. Research demonstrates that technicians can use QKD and fiber-optic quantum networking through satellites for large-scale distribution [2]. QKD provides the theoretical security, yet it encounters several hurdles because implementation costs remain high, and the technology is difficult to scale and works poorly with current classical networks. Quantum communication networks face challenges that re- searchers tackle by developing innovative quantum network designs together with combination encryption approaches and quantum-resistant cryptographic systems to improve security in quantum networks [2].

Recent studies on Quantum Cryptography (QC) through systematic review eliminate any doubt about building quantum-resistant network protocols [3]. The review combines research from 134 studies to examine quantum channel noise and limitations of transmission distances, together with the difficulties of implementing secure quantum communication frameworks. The researchers propose that Quantified Secured Encryption (QSE), together with post-quantum cryptographic standards need more development work for establishing robust cybersecurity defenses against changing security threats [3]. Research on quantum cryptographic methods remains vital because of increasing interest, which demands more study into methods to establish affordable interoperable quantum security solutions that can easily merge with current digital systems.

The main practical use of quantum cryptography focuses on protecting Unmanned Aerial Vehicles (UAVs). The research article by Ralegankar *et al*. [4] describes how Quantum Cryptography-as-a-Service (QCaaS) secures UAV communication systems despite their known vulnerability to cyber intrusions. A multi-tiered quantum cryptographic architecture serves both protection needs and helps data transmission run efficiently in UAV communication networks. The research shows battlefield QKD implementation with a case study which improves network reliability and security effectiveness. The study points out implementation problems as well as latency issues while recognizing the advantages of quantum-based security systems.

Sodiya *et al*. [5] conducted research which investigates the complete implications of quantum

computing for cyber security by analyzing how both RSA and ECC encryption schemes become vulnerable to quantum attacks. The authors assess the critical need for quantum-resistant encryption protocols, which include lattice-based and code-based and multivariate methods. The research delves into Quantum Key Distribution (QKD) techniques because they safeguard data in the upcoming quantum cryptography age. The research identifies the necessity of establishing worldwide standards that protect digital assets through quantum-safe cryptographic solutions because of the current urgent situation. The identification of scalability as well as costs and infrastructure modifications persists as a main barrier to the widespread implementation of these solutions. The paper by Ganeshkar and Kulkarni [6] examines Quantum Cryptography (QC) by reviewing its fundamental principles which includes uper position, and entanglement and quantum uncertainty. The examination details BB84 and E91 QKD protocols and demonstrates their capabilities for protecting secure data transmission. The research discusses modern developments in quantum network design and demonstrates their implementation for smart cities, along with industrial IoT and financial systems. The research evaluation recognizes fundamental gaps which demand quantum-safe authentication solutions and effective deployment approaches for QKD net- work environments. The paper recognizes hardware constraints and integration difficulties, along with expense restrictions for quantum cryptography despite demonstrating its potential uses. The paper by Sahuand Mazumdar [7] presents a modern review of quantum cryptography implementations alongside analyses of the cryptographic threat's quantum computing arrays present to RSA and ECC algorithms. The paper outlines quantum encryption methods while focusing on essential QKD protocol implementations, including BB84andE91. The authors emphasize the need to create encryption solutions that resist quantum attacks because of increasing security concerns. Very high technology costs together with challenges with scalability and standardization prevent wide spread deployment of quantum cryptographic solutions.

The research paper by Revathi [8] explores quantum key cryptography through a discussion on key generation procedures and security properties of QKD-based systems. QKD paper demonstrates its protective capabilities against eavesdropping and brute-force attacks; however, it is compared against post-quantum cryptographic solutions in the research. The author mentions important deployment obstacles alongside hardware constraints as well as environmental impact while explaining the complexity of deploying QKD in real-world settings. Variable framework combinations between quantum and classical security protocols show promise to enhance practical secure communication methods, according to the research findings.

The paper by Chandre *et al*. [9] demonstrates how machine learning integration strengthens QKD by enhancing operational efficiency, key speed generation capabilities, and security threat detection effectiveness. A discussion in the paper describes how ML-based error correction functionalities, together with adaptive protocol optimization, enable quantum cryptographic systems to operate more efficiently. This research describes vulnerabilities at the same time as it acknowledges risks that exist in ML-powered quantum security infrastructure and the difficulties AI models face when trained to work in quantum domains. The research finds that upcoming investigations must explore combination cryptography systems of quantum and classical entities together with security methods developed via artificial intelligence.

A survey by Subramani *et al*. [10] is conducted on the security schemes provided by the classical and quantum cryptography, in terms of security achievement, encryption efficiency, and computation complexity performance evaluation. The paper explain show to obtain security beyond the classical encryption through the quantum key distribution (QKD) protocols using the quantum entanglement to prevent eavesdropping. The study reveals, however, substantial practical obstacles, such as a big computational burden, network synchronization issues, along with the necessity for quantum- secure verification protocols.

Another study by Hasanetal. [11] delvesintothevision, protocols, applications, and challenges of quantum communication systems. The authors give an overview of quantum communication structures guaranteeing how qubits and quantum entanglement enhance the security and precision of data transfer. The study points out implementation hurdles such as the expensive cost of acquiring a QI, interfacing challenges between the existing communication network and the quantum network, and quantum error correction functionalities. Even if this stands in the way, the paper points out that hybrid classical-quantum communication systems could provide a practical path to switching everything over to quantum-secure. Tariq, *et al*. [12] deals concerning quantum inspired cryptographic protocols for cloud security, exposing quantum mechanics' side alike Superposition, Entanglement and so as to further increase the data encryption. The research has assessed the performance of quantum-code protocols against a back drop of classical cryptography and argues the security benefits they can bring an under-threat data base on the cloud. Yet, the study points out that scalability challenges, computational resource needs and integration challenges still are considerable barriers to wide usage.

Digital communication security now faces significant changes because of the quantum computing advancement. A systematic review of post-quantum hash-based signature (PQHS) schemes took place according to Fathalla and Azab [13]. Hash- based signatures represented by WOTS and MSS hold security through cryptographic hash functions' properties according to the study. The authors outlined the barriers to implementing these schemes regarding performance acceleration and

efficient key management requirements. The research establishes a detailed exploration of how PQHS schemes currently stand before showing plans for future development with an emphasis on cryptographic infrastructure combination.

Raeisi-Varzaneh and fellow researchers studied in [14] how cryptographic technologies can handle security demands that IoT devices generate. Raeisi-Varzaneh *et al*. [14] examined IoT system weaknesses in authentication security and communication and privacy functions before showing how symmetric and asymmetric encryption can address these problems. The investigation discussed how post-quantum cryptography could protect IoT communication links due to the growing presence of quantum computing. The article pointed out the necessity of developing minimalistic encryption technologies that would run optimally on IoT equipment yet deliver thorough resistance against conventional and quantum-digital threats.

Table-1. Analysis of quantum cryptography survey papers.

Ref.	Problem Addressed	Proposed Solution	Algorithms & Methodology	Limitations
[22]	Security breaches for classic cryptography of quantum computers; requirements for safe communication procedures.	A detailed study on various quantum Cryptographic protocols like QKD, QSDC, SQKD, DIQKD.	Analysis of existing QKD protocols and experimental implementations; classification of attacks and security risks.	Limited focus on practical deployment issues and integration with classical systems.
[23]	Cryptography system existing to Quantum attack taken; need an aluminium secure post-quantum.	Analysis of lattice based, hash-based, Code based and multivariate based post quantum algorithms.	Survey of PQC algorithms under NIST standardization; evaluation of key performance and security factors.	Challenges in real-world deployment due to computational and infrastructure requirements.
[24]	Limiting factors for deploying post-quantum in constrained devices (e.g., IoT) - low power and small memory.	Study of lattice-based, multivariate, hash-based and code-based constructions done for low-power devices.	Performance assessment of PQC for Constrained devices; trade-off between security and efficiency.	Performance trade-off between-curity and computational efficiency in low-power environments.
[25]	Requirement for secure key black market; vulnerability of classical key trade markets to quantum.	Evaluation and classification of QKD protocols; proposal of hybrid quantum-classical systems.	Classification of QKD protocols; Evaluation of security guarantees and vulnerabilities.	Limited scope for real-world-implementation and scalability issues.
[26]	Requirements for a secure transportation of the information over classical and quantum carriers; difficulties in harmonization and integration of the quantum and classical worlds.	Evaluation and classification of QKD protocols; proposal of hybrid quantum-classical systems.	Classification of QKD protocols; Evaluation of security guarantees and vulnerabilities.	Limited scope for real-world implementation and scalability issues.
[27]	In precautions to secure key distribution & eaves dropping prevention by means of quantum related sciences.	ApplicationofBB84andanyother QKD protocol to implement secure communication.	Thorough study of BB84, B92, and six-state protocols, Security and key exchange performance assessment.	Security limitations under practical conditions; vulnerability toside-channel attacks.

The research by Mohammed [15] introduced a new smart city communication security method that merged quantum cryptographic techniques with convolutional neural networks (CNNs). The introduced hybrid system enables QKD to handle secure key exchange alongside CNN-based encryption for data security protection. The authors made a case that this method would deliver advanced security protocols which benefit essential smart city functions, including real-time video monitoring and IoT data protection. A combination of quantum cryptography and AI techniques, specifically CNNs, demonstrates effective security methods in detecting eaves dropping through the assessment of quantum key distribution and encryption efficiency. This

method demonstrates its ability to protect against cyber-attacks as well as ensure safe data transmission through extensive smart city networks.

Quantum cryptography systems linked with block chain technology have recently gained popularity to secure IoT devices because standard cryptographic methods remain weak in limited resource conditions. The researchers presented an extensive architecture which unite block chain technology with quantum cryptography to safeguard multimedia data at IoT devices [16]. The authors stressed that key management effectiveness combined with QKD technology and block chain authentication systems enable strong data confidentiality alog with integrity protection and non-repudiation properties. Their research showed that ZKPs integrated with block chain systems establish powerful endpoint security that defends against intrusion attempts, particularly in smart environments with healthcare applications.

Renner and Wolf [17] analyzed the fundamental shortcomings of classical RSA and Diffie-Hellman encryption methods because they count on computational assumptions that quantum attacks render vulnerable. The authors supported quantum key distribution because it provides information-theoretically secure communication, which relies on physical quantum mechanics laws, specifically superposition and entanglement, and the no-cloning theorem for key interception protection. The study assessed post-quantum cryptography techniques to show that QKD stands alone as the only cryptographic system ensuring absolute long-term secret data transmission, although post-quantum schemes provide short-term protections. The researchers specified both the practical boundaries and usage areas of quantum cryptography, which focus on generating symmetric keys for the security needs of IoT systems.

Chawla and Mehra [18] developed their research by performing a survey focused on quantum computing applications for IoT security. The authors presented the weaknesses of RSA and ECC cryptographic systems and showed the successful application of QKD and quantum entanglement methods for overcoming key distribution obstacles in extensive IoT networks. The authors presented both hardware scalability problems and integration complexities in their implementation assessment work. The authors proposed that quantum encryption protocols provide greater defense against quantum at tacks in addition to decreasing network delays as well as ensuring real-time protection for smart city and smart grid systems.

Post-quantum cryptography (PQC) is an alternative to secure communication in the quantum age by building cryptographic algorithms that are safe against quantum-based attacks. Bavdekar *et al*. (2019) examined the effects of quantum computing on classical cryptographic systems, which they underlined that Shor's algorithm could efficiently solve the prime factorization problem, making RSA, Diffie-Hellman, and ECC susceptible to quantum attack. They also discussed upper-bound impacts of quantum algorithms, related to a specific cryptographic problem, and surveyed major families of post-quantum cryptographic algorithms, i.e., lattice-based, hash-based, code-based, and multivariate cryptography, and lattice-based as one of the most promising schemes to learn about quantum attacks. The NIST post-quantum cryptography standardisation process has also been described by Bavekar *et al*., with emphasis on the importance of developing roughly scalable and efficient PQC algorithms for critical communication in future quantum networks [20].

Uplink quantum communication from space is an important tactic for establishing global quantum networks. Sidhu *et al*. (2021) provided insights into recent developments in space quantum communications, which were from the point of utilizing satellite-based QKD to get beyond the space limitation in terrestrial QKD networks. Some of the operational challenges of the space-based QKD, namely signal losses, atmospheric turbulence, and beam alignment errors, were also discussed in the study, together with the solutions like enhanced satellite tracking systems and error correction techniques. Sidhu et al have pointed out the need for a combination of space and ground and terrestrially-based quantum communication infrastructure toward the creation of a quantum global internet. The paper found the necessity for future advanced quantum repeaters and inter satellite communications to better satellite-based QKD systems scalability and performance. In conclusion, the authors stated that space-based quantum communication has many possibilities for secure communication globally [21].

Quantum cryptography has emerged as a promising area that provides secure networking against potential threats brought by quantum computers. The basis of quantum cryptography comes from the truths of quantum mechanics-quantum secure key exchange and communication are provided through the Heisenberg Uncertainty Principle and the no-cloning theorem, for example. Several quantum key distribution (QKD) protocols were devised and improved in time in order to increase security and efficiency. Especially, Bennett and Brassard proposed the BB84 protocol in 1984, which still plays a basic role in QKD and is the basis for several modern cryptographic systems [22]. The original protocols have been further studied by the researchers, introducing new techniques, device-independent QKD to overcome various practical limitations and enhance the security under the conditions. Semi-quantum protocols are continuous-variable QKD.

Numerous extensive reviews are known that have investigated the progress/disadvantages in quantum cryptography. The most recent hope survey by Kumar and Garhwal (2021) does a deep investigation of quantum cryptographic protocols, including QKD, quantum secure direct communication (QSDC), semi-quantum key distribution (SQKD), and device-independent quantum cryptography (DIQKD) [23]. It describes categorizing

QKD protocols into discrete and continuous variable methods and a variety of attacks, such as photon number splitting (PNS) and Trojan horse attacks. The survey also includes experimental implementations, the gains in satellite-based QKD, and quantum networks. The authors point to the growing research on quantum cryptography fol- lowing the requirement to secure against prospective quantum computing threats.

Cille's transition from the classical to quantum cryptography isnoteasy.Post-quantum cryptography (PQC) was suggested.

Table-2. Quantum cryptography survey comparison.

Survey	[22]	[23]	[24]	[25]	[26]	[27]
QKD Protocols	✓	✗	✗	✓	✓	✓
Post-Quantum Cryptography	✗	✓	✓	✗	✗	✗
Hybrid Systems	✗	✗	✗	✗	✓	✗
Security Issues	✓	✓	✓	✓	✗	✓
Implementation Challenges	✓	✓	✓	✗	✗	✗
Performance Analysis	✓	✓	✓	✗	✗	✗
Scalability	✗	✗	✗	✗	✓	✗
Real-World Deployment	✗	✓	✓	✗	✓	✗

As a fix to sequence cryptographic systems against quantum attacks. Dam *et al*. (2023) is a comprehensive survey on post- quantum cryptography, outlining the algorithms in consideration in the NISTPQC standardisation process [24]. The survey treats lattice-based, code-based, hash-based, and multivariate- based cryptographic schemes. It reviews the options in each of these approaches, especially the implementation problem in dissimilar hardware platforms. The authors also highlight the developments made in hybrid quantum-classical cryptographic systems for an easy smooth transition during the post-quantum era.

Quantum cryptography for resource-constrained devices is a special case of design because of computing and battery power constraints. Roy and Kalita (2019) conducted research with a focus on post-quantum cryptosystems that have the capability to be used in a limited scenario environments such as Internet of Things (IoT) devices [25]. The paper surveys lattice schemes as NTRU and Ring-LWE, multivariate schemes as Rainbow, and code-based schemes as McEliece from the perspectives of being viable for low-bandwidth storage and cheap devices. Authors say that lattice-based cryptography is a balanced approach between security and speed, meaning it a good thing to be on resource-poor devices.

Besides, quantum key distribution (QKD) technologies have also advanced with novel designs and new cryptographic primitives. Li *et al.* (2018) present a survey of quantum key distribution, past, present, future, and concepts and principles for BB84, B92, E91, and six-state protocol [26]. The authors cover the security requirements offered by QKD, including resistance to eavesdropping and eavesdropping using photon splitting. The survey covers the progress of the QKD networks, such as the DARPA Quantum Network and Tokyo QKD Network. The paper authors also discuss the impact of quantum entanglement for enhanced security and scalability of the QKD systems.

Li *et al*. (2017) discuss a thorough overview of quantum cryptographic schemes and the development of quantum secure communication networks [27]. The paper surveys the merging of quantum cryptography with classical networks and the problems associated with it, key management, authentication and error-correcting codes. The authors investigate hybrid quantum-classical systems and their capability of enhancing the security and the performance of Present-day communication networks. The survey shows that more research in applications and development of standardized protocols for the quantum communication is needed.

A powerful solution against evolving quantum computing threats has appeared in the form of quantum cryptography. QKD serves as a security mechanism that Vadakkethil and Polimetla [28] utilize for developing eavesdropping-proof communication lines. QKD achieves its strength by utilizing the quantum mechanical properties of entanglement together with no-cloning to protect keys from interception, which cannot go unnoticed. The study identifies important restrictions related to high expense levels and specialized equipment demands, as well as technical barriers to ensuring broader implementation. Quantum cryptographic protocols demonstrate stronger resistance to classical attacks yet the authors warn about potential misinterpretation of complete security since quantum cryptography does not defend against social engineering or software-based threats.

Temara and his team added machine learning methods to their post-quantum cryptography to develop better defenses in their research paper [29]. Their system design associates neural networks with anomaly finding techniques, plus reinforcement learning and predictive analysis for quantum- beating threat prediction. Our hybrid ML-PQC solution detects threats promptly to keep cryptography strong and achieves better than static systems at identifying anomalies (98%). The adaptive approach tackles key schedule problems in QKD systems and adds better security response to future quantum threats in digital environments.

Aydeger *et al*. [30] studied organizational abilities to include PQC in their security plan using NIST Cybersecurity Framework 2.0 as their foundation. They design a step-by- step approach for quantum-resistant environments which includes planning, guarding, finding threats, handling incidents, and restoring services. The research demonstrates how using mixtures of traditional and quantum-protected cryptographic methods helps companies keep past security but starts to block quantum dangers. The experts see the need for standardization of

PQC standards alongside regulated rulemaking because PQC solutions still show high performance costs, as well as integrated difficulties plus unproven algorithm testing results. Their recommendations for leadership decisions and system transition preparation match well with the technology information provided by other reports to show why PQC needs to become part of the security strategy.

4. TAXONOMY

The fundamental concept of quantum cryptography produces four fundamental divisions. The field of Quantum Threats evaluates the vulnerabilities faced by RSA and ECC cryptographic systems by analyzing algorithms Shor's and Grover's.

Digital Signatures represents the second branch which maintains data authenticity while protecting its integrity from quantum threats. The creation of hash-based and lattice-based digital signature methods represents part of the post-quantum signature scheme development.

Post-Quantum Cryptography (PQC) exists as the third cryptography paradigm alongside quantum-resistant algorithms that implement on current classical infrastructure systems. NIST has standardized the quantum-resistant algorithms which fall into four categories: lattice-based, code-based, multivariate, and hash-based methods.

The fourth segment titled IoT Security, shows twice in the paper, indicating its dual purpose as an independent study domain and critical PQC application. The IoT environment faces particular difficulties implementing quantum- secure communication because it must operate within power restrictions, memory limits, and the need for real-time data movement.

Figure-2 presents a visual taxonomy structure of Quantum Cryptography, which arranges the principal areas in the field through a hierarchical flowchart framework.

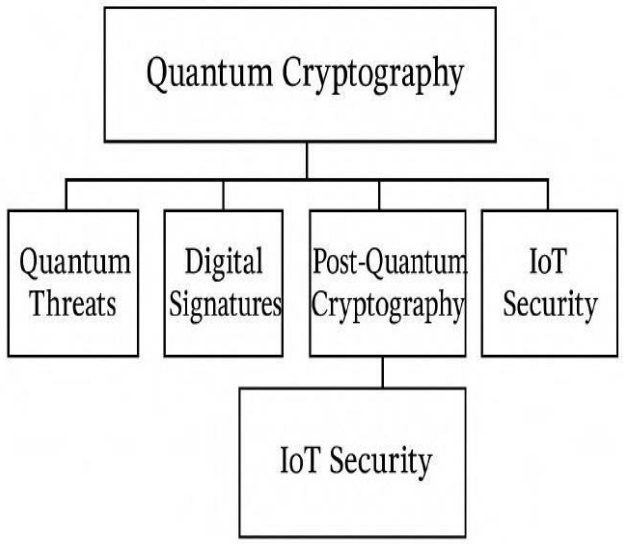

Figure-2. Taxonomy of key domains in quantum cryptography research, including threats, digital signatures, post-quantum techniques, and IoT security.

- The central node of "Quantum Cryptography" occupies the top position to establish the main domain.
- Quantum Cryptography divides into four essential subdomains that stem from its main node.

a) Quantum Threats delineates all potential security hazards that quantum computers introduce for conventional encryption systems.
b) The research analyzes cryptographic fundamentals devoted to secure digital signatures, particularly within quantum risk evaluation.
c) Post Quantum Cryptography (PQC) represents encryption methods that quantum attackers cannot break without using quantum-based hardware.
d) Internet of Things security describes the method of implementing quantum-resistant cryptographic techniques to protect IoT systems.
e) The phrase "IoT Security" appears twice in the diagram to indicate its position as an individual domain and critical PQC implementation field.

Quantum Cryptography meets both theoretical concepts about threats and digital mechanics and real-world applications con-

Table-3. Summary and comparison of the related works.

Ref.	Problem Addressed	Proposed Solution	Algorithms & Methodology	Limitations
[1]	Encryption methods used in the past become weakened when quantum computing reaches maturity, which drives the necessity for quantum-resistant cryptography development.	The paper investigates different post-quantum cryptographic methods which include lattice-based approaches as well as code-based and multivariate cryptographic methods.	The paper examines multiple post-quantum cryptographic algorithms but lacks actual experimental demonstration while focusing mainly on published research.	The research paper examines post-quantum cryptography methods while neglecting to explore implementation obstacles. The research fails to test the proposed encryption methods through laboratory experiments
[2]	Secure network communication becomes necessary because classical cryptographic protocols will become extinct through the advancement of quantum computing capabilities.	The use of Quantum Key Distribution (QKD) functions as an alternative cryptographic method to classical encryption techniques because its research investigates satellite-based QKD implementations.	The paper examines both BB84 and E91 QKD protocols along with their application in classical network integration using real-world evidence and academic research.	The paper investigates QKD but fails to explain the intricate aspects of both quantum and classical cryptographic methodologies. The study fails to conduct a deep evaluation regarding practical implementation hurdles and expense assessments.
[3]	Scientists examine quantum cryptography through detailed research which includes security network communication obstacles assessment and available solution evaluation.	A systematic evaluation of 134 research studies established both current quantum cryptographic techniques and their unexplored research areas.	Research analysing security threats And counter measures with in quantum cryptography through Systematic Literature Review (SLR) methodology studied studies dating from 2016 to2023.	The system overview contains thorough evaluations of quantum cryptography but does not include either practical experiments or empirical case studies. The research fails to provide extensive information about recent developments in hybrid cryptographic systems.
[4]	The communication networks of UAV systems face security weaknesses from cyber-attacks and conventional encrypted data methods.	A secure UAV network requires a Quantum Cryptography-as-a-Service (QCaaS) model, where QKD is used to strengthen network security.	The proposed quantum cryptographic architecture features multiple layers with analysis of battlefield examples to measure performance regarding delay time, security level, and system integrity.	The proposed quantum cryptographic architecture features multiple layers with analysis of battlefield examples to measure performance regarding delay time and security level, and system integrity.
[5]	New encryption methods are essential for quantum computing advancement because traditional cryptographic standards become exposed to quantum computing attacks.	Digital assets gain protection against quantum-based cyber threats through the deployment of PQC together with QKD.	The research examine show quantum computing affects cybersecurity and shows that both classical encryption systems and new quantum-proof methods need construction. This study looks into PQC algorithms, checks their power, and studies the issues with setting industry standards.	The process of switching to quantum-Safe cryptography runs into trouble somescaleup problems along with monetary barriers and difficult regulations.
[6]	A secure communication system Based on quantum mechanics must be developed to stop cyber threats along with eavesdropping activities.	Future-proof cryptographic security Through the deployment of QKD protocols which use BB84 and E91.	The document studies how superposition and entanglement work in quantum cryptography while testing multiple secure communication methods and network plans.	The system faces expensive setup expenses while adapting to hardware restrictions and connecting properly with traditional data networks.
[7]	The growing power of quantum	Better QKD protocols such as BB84	Detailed research in to post-quantum	The implementation becomes expensive while scalability faces

	computers affects encryption security which requires quantum-resistant methods for protection.	and E91mustbecombinedwithnewdevelopment of quantum-resistant encryption algorithms.	encryption methods and QKD protocol evaluation follows an assessment of actual implementation obstacles.	challenges along with insufficient standardization of quantum security protocols.
[8]	The deployment of quantum key cryptography faces two main obstacles due to security weaknesses and hardware system constraining factors.	A combination of QKD technology for guaranteed key exchange functions with a hybrid cryptographic framework implementation.	Research of quantum key cryptography, through traditional encryption comparison along with QKD security case examinations.	Hardware dependencies interrupt QKD Security while environmental influences and difficulties faced when merging classical security systems with QKD remain major obstacles.
[9]	Pattern recognition algorithms contribute to maximizing both efficiency and security efficiency of quantum cryptographic systems.	The application of machine learning Techniques for maximizing QKD key speeds and performing quantum error correction and authentication functions.	Optimizing machine learning that Leads to enhancing key rate, or adapting security mechanism, for quantum cryptographic protocols.	The challenges related to adversarial attacks on quantum security that result from ML-based implementation along-side the difficulty of training AI models with in quantum systems.
[10]	Standard crypto graphic methods remain exposed to quantum computing threats because they need alternative cryptographic systems that maintain security.	Quantum Key Distribution (QKD) presents itself as a secure cryptographic solution together with post-quantum cryptographic methods, according to the study.	Security evaluation of classical and Quantum cryptographic methods focus on the analysis of three aspects, including encryption efficiency, security levels, and computational complexity.	Post-quantum cryptographic solutions face material execution issues together with high computational requirements that make QKD deployment practical.
[11]	Quantum communication systems meet several implementation obstacles which consist of networks integration difficulties, security threats, and budget constraints.	A mixed classical-quantum communication system helps achieve more secure and efficient quantum communication networks.	An evaluation of quantum communication strategies in combination with QKD protocols and their integration barriers for present network platforms.	High price of quantum infrastructure, challenge of integration with traditional network, and limitationinquantumerrorcorrectiontechniquesisdifferentbarriertowide adoption of quantum communication technique.
[12]	Boosting cloud computing security By adding quantum inspired cryptography protocols so as to counter quantum or classical threats.	Cryptographic protocols based on a notation inspired by the very principles of quantum mechanics, those of superposition and entanglement, which allows securing the cloud data.	Quantum original crypto graphic method assessment by theory analysis and performance evaluation in the cloud infrastructure.	Scalability problems, augmented application computing needs, and issues of integrating cloud computing security frameworks.
[13]	The research focuses on digital signature vulnerabilities to quantum threats with an analysis of how RSA alongside ECC, become vulnerable because of Shor's and Grover's algorithms.Digitalcommunicationse-curityrequiresimmediateimplemen-tations of post-quantum hash-based signature (PQHS) systems because existing digital communication methods face increasing	This study reviews post-quantum hash-based signature (PQHS) schemes, focusing on WOTS, MSS, and XMSS to assess security proofs, efficiency, and key length optimization. The findings highlight strengths and limitations of PQHS, offering a foundation for enhancing quantum-resistant cryptography.	The research implements PRISMA methodology to perform systematic reviews on PQHS schemes including WOTS, MSS, and XMSS. The research examines both security proofing and efficiency and key size performance to find resilient quantum-proof solutions. The designated analytical framework delivers an extensive examination covering both positive aspects	PQHS scheme implementation requires further development because practical testing is minimal and security measures conflict with system performance levels. Standard guidelines must exist for PQHS schemes to achieve wide spread adoption. PQHS deployment advancement depends on additional research activities, standardized procedures and field verification testing approaches.

	security threats.		and weak points of PQHS solutions	
[14]	The research investigates IoT security issues through examinations of authentication flaws, communication security, and data protection threats. The research investigates light-weight and post-quantum types of cryptography to enhance secure IoT data exchange mechanisms specific to resource-limited Io T settings.	The research uses symmetric cryptography along with asymmetric systems and post-quantum based methods to handle security issues in IoT systems. The research objective is to build lightweight quantum-secure protection protocols that secure IoT resources.	Research investigates AES, RSA, ECC and lightweight cryptography designed for limited devices to determine their security capability in IoT transmissions. The research analyses post-quantum protection strategies that defend IoT systems from imminent quantum threats.	The limited resources and non-standardized security protocols make the protection of IoT devices difficult to attain. New developments in quantum-resistant cryptography create more difficulties for integration operations. The immediate need for research-driven innovation becomes evident through these security-related problems.
[15]	The investigation targets smart city communication security methods to protect against quantum security risks and cyber threats. Advanced cryptographic methods enable this research to create better security for data protection, together with safekeeping of sensitive urban information.	The authors present a security frame-work which blends QKD for dependable key distribution protocols alongside CNNs for strong encryption protocols. The joint implementation of QKD and neural networks creates a security system that battles both quantum-level and cyber-space threats to protect smart city communications.	The proposed research design uses QKD protocols together with CNN encryption to provide secure communication systems. A BLSTME-CNN hybrid system functions as a traffic prediction alongside a secure communication platform for smart cities that resists quantum security threats and digital attacks.	Encryption with CNN technology needs enormous computing capacity that would reduce its functionality in real-time, and QKD systems face difficulties in extending their functionality to extensive smart city network infrastructure. The requirement for advanced hardware creates barriers to large-scale adoption because improved solutions need to be developed.
[16]	Vulnerability of multimedia data in IoT devices due to limited resources and insecure channels.	The implementation of Block chain Quantum Cryptography contains QKD and Zero-Knowledge Proofs.	Block chain ledger for immutable Data handling, QKD for secure key exchange, ZKP for authentication.	The deployment of QKD faces practical Obstacles because of hardware restrictions as well as standardization barriers.
[17]	The limitations to which classical cryptography faces when defending against quantum computing threats exist.	Information-theoretic security comes From implementing Quantum Key Distribution (QKD).	Theoretical modeling of QKD, One-Time Pad (OTP), and quantum randomness for key generation.	The implementation of QKD operates Through symmetrical cryption while depending on secure physical channels.
[18]	RSA and ECC show shortfalls as security methods for IoT environments because of quantum computing dangers.	Secure IoT depends on quantum-Based protocols that use superposition together with entanglement.	Research and categorization of quantum-secured communicationmethods;fundamentalunderstandingofquantumkeydistributiontogether with quantum mechanics fundamentals.	Quantum technologies exist as complex systems that remain challenging to deploy across multiple network types found in IoT environments.
[19]	The actual cryptographic systems are weak to quantum computing threats there by it becomes necessary to develop the quantum resistant mechanism for secure communication.	Upgraded QKD protocols (e.g.MDI-QKD (TF-QKD), and integration with optical communication networks through Key-as-a-Service (KaaS) to secure and scalable.	This paper examines 20 leading-edge works related to QS, PQC, and CQKD, and build new architectures for the integration of QS with optical networks.	QKD is limited by its range and key rate; efficiency of quantum repeaters must be improved; practical challenges need to be solved.
[20]	Shorand Grover'salgorithmshave broken previous classical encryption methods, including RSA, Diffie-Hellman, and ECC.	Researching post-quantum cryptography (PQC) using lattice, hash, code, multivariate andisogeny based cryptography.	The paper compares PQC techniques, outlines the NIST PQC standardization process, and assessments of PQC candidates are given.	PQC algorithms are computationally costly; requirement for a compact hardware implementation and key size reduction.

[21]	Secure global communication is not possible with ground based network alone, as QKD over Terrestrial net-works is limited by distance because of signal loss and noise.	Satellite-based QKD for extending The secure communication distance; hybrid ground-space infrastructure.	The paper presents a review of satellite-based QKD, considers the entanglement distribution and quantum repeaters, as well as ground-based and satellite-based QKD performance comparison.	Loss of signal from signal mask due to turbulent atmosphere and beam wander; need for better satellite tracking/alignment systems; low key gen.
[28]	Increasing vulnerability of classical Encryption methods to quantum computing threats.	Adoption of Quantum Cryptography- using Quantum Key Distribution (QKD) for secure communication.	Qua Quantum Key Distribution (QKD), specifically protocols like BB84 and EPR, uses quantum entanglement and the no-cloning theorem.	High implementation costs, need for specialized equipment, and limited trans mission range.
[29]	Ineffectiveness of traditional cryptography against quantum-based attacks and lack of adaptive security mechanisms.	An ML-augmented cryptographic A framework combining PQC with real-time anomaly detection and adaptive key management.	Lattice-based and hash-based PQC algorithms; neural networks for anomaly detection, reinforcement learning for key management.	Computational overhead, integration complexity, and potential false positives in anomaly detection.
[30]	Need for structured transition strategy- Egytopost-quantum cryptography amidst growing quantum threats.	A strategicmigrationplanto PQC integrating with the NIST Cybersecurity Frame work and hybrid crypto graphic systems.	PQC algorithms like CRYSTALS-Kyber, Dilithium; integration with Cybersecurity Frame work 2. 0phases (Identify, Protect, etc.).	Lack of standardization, high resource requirements, and challenges in interoperability and implementation scalability.

Concerning post-quantum cryptography and IoT security through this taxonomy structure, thus covering various security areas.

5. FUTURERESEARCHTREND

Future advancements of quantum computing require quantum cryptography research to build mature, technically affordable, and globally adaptable security solutions. A top priority exists to improve Quantum Key Distribution (QKD) protocols for extended-range and time-sensitive communications across satellite-linked and joint space-terrestrial systems. Researchers must study advanced quantum repeater concepts as well as experimental error correction processes and dependable key management approaches to extend QKD communication capabilities [21].

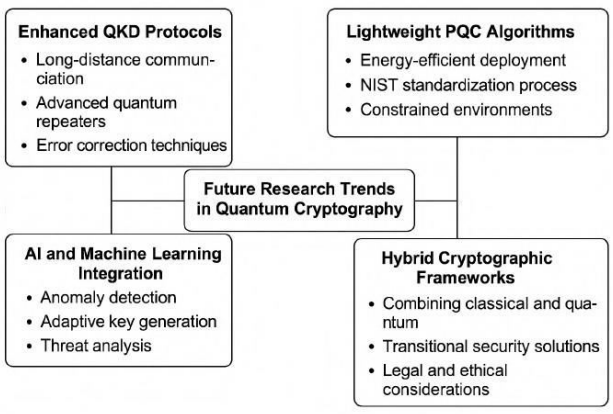

Figure-3. Future research trends in quantum cryptography.

PQC research will focus on creating power-saving and practical algorithms for use in limited environmental systems like IoT and embedded devices. The further development of PQC schemes for NIST standards remains vital to make them work everywhere across the world [13, 24]. The best use of artificial intelligence and machine learning right now is in detecting anomalies as they happen while creating new encryption keys and forecasting threats. The integration requires effective protection against AI attacks plus smart handling of available resources [9] [29].

Research should explore new systems that unite quantum and classical and AI-based encryption techniques to serve as a transitional framework for security structures during the quantum age transition. The deployment of quantum-secure communication depends on solving both technical and legal security issues. The quantum age requires broad interdisciplinary groups that will link abstract research progress with operational implementation to create secure communication systems.

6. CONCLUSIONS

The technological advancement of digital communications security depends heavily on quantum cryptography due to rising quantum computing threats. Quantum Key Distribution (QKD) technology, which operates from fundamental quantum mechanics principles, provides a fundamental change from computational protection measures to physical protection security. Although QKD offers such strong theoretical assurances, the actual use of the technology faces practical barriers due to elevated installation fees alongside complex

implementation needs and restricted growth potential. Post- Quantum Cryptography (PQC) includes two complementary approaches in its framework through lattice-based and hash- based schemes, which provide resistant solutions to quantum attacks by working on existing classical infrastructures.

Hybrid models, integrating quantum and classical cryptographic techniques, have emerged as a viable path toward scalable and cost-effective secure systems. Furthermore, the incorporation of machine learning techniques into quantum cryptographic infrastructures has enhanced threat detection, key management, and adaptive security response. However, these innovations also introduce new attack surfaces and computational overheads that demand further research.

The full potential of quantum-secure communication requires future work that includes standardization methods together with efficient protocol development, hardware improvements, and cross-domain communication devices. Research collaborations between scientists, together with industries and governments, need to grow rapidly due to the fast pace of quantum-safe infrastructure development. The need exists to develop defensive cryptographic systems through innovative strategic planning so they will survive threats from both classical and quantum periods.

REFERENCES

[1] M. Victor, D. D. W. Praveenraj, S. R., A. Alkhayyat and A. Shakhzoda. 2023. Cryptography: Advances in Secure Communication and Data Protection. E3S Web of Conferences, 399: 07010, DOI: 10.1051/e3sconf/202339907010.

[2] P. C. Nwaga and S. Nwagwughiagwu. 2024. Exploring the significance of quantum cryptography in future network security protocols. World Journal of Advanced Research and Reviews, 24(3): 817-833, Dec. 2024. DOI: 10.30574/wjarr.2024.24.3.3733.

[3] D. Shahwar, M. Imran, A. B. Altamimi, W. Khan, S. Hussain, and M. Alsaffar. 2024. Quantum Cryptography for Future Networks Security: Asy stematic Review. IEEE Access, 12: 180048-180056, 2024.DOI: 10.1109/ACCESS.2024.3504815.

[4] V. K. Ralegankar, J. Bagul, B. Thakkar, R. Gupta, S. Tanwar, G. Sharma, and I.E. Davidson. 2021. Quantum Cryptography-as-a-Service for Secure UAV Communication: Applications, Challenges, and Case Study. IEEE Access, 10: 1475-1485, DOI: 10.1109/AC-CESS.2021.3138753.

[5] E. O. Sodiya, U. J. Umoga, O. O. Amoo, and A. Atadoga. 2024. Quantum Computing and Its Potential Impact on U.S. Cybersecurity: A Review. Global Journal of Engineering and Technology Advances, 18(2): 49-64, DOI: 10.30574/gjeta.2024.18.2.0026.

[6] V. Ganeshkar and M. Kulkarni, 2024. Quantum Cryptography for Secure Communication. International Journal of Research in Computer Applications and Information Technology (IJRCAIT), 7(1): 17-29, Available: https://iaeme.com/Home/issue/IJRCAIT?Volume=7&Issue=1.

[7] S. K. Sahu and K. Mazumdar. 2024. State-of-the-art analysis of quantum cryptography: Applications and prospects. Frontiers in Physics, vol. 12, DOI: 10.3389/fphy.2024.1456491.

[8] A. Revathi. 2023. Quantum Key Cryptography: Advancements and Challenges in Secure Communication. Journal of Multidimensional Research & Review. 3(4): 1-6.

[9] P. R. Chandre, B. D. Shendkar, S. Deshmukh, S. Kakade, and S. Potdukhe. 2023. Machine Learning-Enhanced Advancements in Quantum Cryptography: A Comprehensive Review and Future Prospects. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11s): 642-648, DOI: 10.17762/ijritcc.v11i11s.8300.

[10] S. Subramani, M. Selvi, A. Kannan, and S. K. Svn. 2023. Review of Security Methods Based on Classical Cryptography and Quantum Cryptography. Cybernetics and Systems, 56(3): 302-320, DOI: 10.1080/01969722.2023.2166261.

[11] S. R. Hasan, M. Z. Chowdhury, M. Saiam and Y. M. Jang. 2023. Quantum Communication Systems: Vision, Protocols, Applications, and Challenges. IEEE Access, 11: 15855-15864, 2023. DOI:10.1109/ACCESS.2023.3244395.

[12] L. Tariq, A. Atta, U. Farooq, N. Anwar, M. Asim, and N. Tabassum. 2024. Quantum-Inspired Cryptography Protocols for Enhancing Security in Cloud Computing Infrastructures. Journal of Statistics, Computing and Interdisciplinary Research. 6(1): 19-31.

[13] E. Fathalla and M. Azab. 2024. beyond Classical Cryptography: A systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations. IEEE Access. 12: 175970-175984.

[14] M. Raeisi-Varzaneh, O. Dakkak, H. Alaidaros, and I. Avci. 2024. Internet of Things: Security, Issues, Threats, and Assessment of Different Cryptographic Technologies. Journal of Communications. 19(2): 78-89.

[15] N. J. Mohammed. 2023. Quantum Cryptography in Convolution Neural Network Approach in Smart Cities. Journal of Survey in Fisheries Sciences. 10(2S): 2043-2056.

[16] D. Harinath, M. Bandi, A. Patil, M. V. R. Murthy, and A. V. S. Raju. 2024. Enhanced Data Security and Privacy in IoT Devices using Block chain Technology and Quantum Cryptography. Journal of Systems Engineering and Electronics. 34(6): 61-66.

[17] R. Renner and R. Wolf. 2023. Quantum Advantage in Cryptography. AIAA Journal, 61(5): 1895-1900, doi: 10.2514/1.J062267.

[18] D. Chawla and P. S. Mehra. 2023. A Survey on Quantum Computing for Internet of Things Security. Procedia Computer Science. 218: 191-2200..

[19] M. S. Akter, J. Rodriguez-Cardenas, H. Shahriar, and F. Wu. 2012. Quantum cryptography for enhanced network security: A comprehensive survey of research, developments, and future directions. In 2023 IEEE International Conference on Big Data (Big Data). pp. 5408-5411.

[20] R. Bavdekar, E. J. Chopde, A. Bhatia, K. Tiwari, S. J. Daniel, and A. Atul. 2019. Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. ArXiv. 2202.02826: 1-15.

[21] J. S. Sidhu et al. 2021. Advances in space quantum communications. IET Quantum Communication. 2(4): 182-217.

[22] Li H., Li W. and Li Y. 2018. A Survey on Quantum Cryptography. Chinese Journal of Electronics. 27(2): 281-290.

[23] Kumar A. and Garhwal S. 2021. State-of-the-Art Survey of Quantum Cryptography. Archives of Computational Methods in Engineering. 28(4): 3831-3868.

[24] Dam D.-T., Tran T.-H., Hoang V.-P., Pham C.-K. and Hoang T.-T. 2023. A Survey of Post-Quantum Cryptography: Start of a New Race. Cryptography. 7(3): 40.

[25] Roy K. S. and Kalita H. K. 2019. A Survey on Post-Quantum Cryptography for Constrained Devices. International Journal of Applied Engineering Research. 14(11): 2608-2615.

[26] Li Y., Li X. and Wang H. 2018. A Survey on Quantum Key Distribution and Protocols. Chinese Journal of Electronics. 27(2): 281-290.

[27] Li X., Wang Y. and Chen Z. 2017. Quantum Cryptographic Protocolsand Secure Communication Systems. Journal of Cryptology, vol.30, no.3, pp. 498-520.

[28] S. E. V. Somanathan Pillai and K. Polimetla. 2024. Analyzing the Impact of Quantum Cryptography on Network Security. 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), pp. 1-7, doi: 10.1109/ICICACS60521.2024.10498417.

[29] S. Temara *et al*. 2025. Cryptography Innovations for Securing Data in the Quantum Computing Era: Integrating Machine Learning for Enhanced Security. 2025 International Conference on Computer, Electrical & Communication Engineering (ICCECE), pp. 1-8, doi: 10.1109/IC-CECE61355.2025.10940245.

[30] A. Aydeger *et al*. 2024. Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography. 2024 15th International Conference on Network of the Future (NoF), pp. 195-200, doi: 10.1109/NoF62948.2024.10741441.