Radius: Journal of Science and Technology
Vol. 2, Issue 2, (2025) 252006 (21pp)

A Comprehensive Review of Post-Quantum Cryptography Protocols for Secure Communications in Heterogeneous Network Environments

Manju Singh[1,*] | Fakhrun Jamal[1]

[1]Shobhit Institute of Engineering & Technology, Meerut – 250110, Uttar Pradesh (India)

*Corresponding author: manju9761@gmail.com

Abstract: The advent of quantum computing has precipitated an estimated attack resistant cryptography system necessitating quantum attacks. The classical asymmetric algorithms, i.e., RSA and ECC are susceptible to Shor algorithm and a transition should be made to Post-Quantum Cryptography (PQC) anymore. The novelty of this work lies in providing a unified comparative framework that analyzes PQC families through security assumptions, concrete key/ciphertext sizes, and implementation complexity an aspect not addressed collectively in prior surveys. This survey gives a general picture of the status of the design process and general evaluation of PQC accounting its application within the paradigm of the diversified networks including the IoT and 5G/6G and in the cyber-physical environment. Furthermore, this review uniquely synthesizes practical hybrid-deployment strategies, including protocol layering, coexistence models, and backward-compatibility mechanisms, offering actionable guidance for real-world migration. Additionally, the manuscript contributes a prioritized list of open problems across IoT, 5G/6G, blockchain, and cyber-physical systems, highlighting domains facing the most urgent quantum-resilience challenges. In this paper, the authors will evaluate the most popular PQC schemes, including schemes based on lattice, code, hash, and isogeny, depending on their performance, scalability, and interoperability (with reference to the recent research). It also examines the problems of integration as implemented with respect to the computational overhead, latency and adoption of hybrid with classical cryptography. This is expounded more to the standardization of PQC by NISTs and with a focus on such algorithms as CRYSTALS-Kyber and Dilithium. The findings suggest that, hybrid PQC protocols are able to control quantum resistance and actual performance in numerous infrastructures in computing systems.

Keywords: Post-Quantum Cryptography, Quantum-Resilient Security, 6G Networks, IoT Security, Lattice-Based Encryption

1. Introduction

The fast development of quantum processing is both a danger and a chance to the current cybersecurity mechanisms. The algorithm models Shors and Grovers are examples that show quantum computers can crack classical cryptosystems, like RSA and elliptic curve cryptography, in a polygamous time highlighting the real-world urgency of PQC adoption due to ongoing large-scale quantum hardware investments by Google, IBM, and national laboratories (Abbasi et al., 2025). This has become a cause of concern that has prompted

https://doi.org/10.5281/zenodo.17664126
Received: 04 November 2025 | **Revised:** 20 November 2025
Accepted: 21 November 2025 |**Published Online:** 02 December 2025

researchers and institutions such as NIST, ETSI, and IETF to create quantum-resistant solutions in a collective effort referred to as PQC.

The security environment of modern heterogeneous network systems, including Internet of Things (IoT) systems, 5G/6G communication frameworks, and distributed cloud-edge systems, is becoming more complicated (Fathalla & Azab, 2024). These environments need light and scalable and interoperability cryptographic schemes that can easily operate with resource constraint. Regulatory bodies such as CISA and ENISA have issued PQC-readiness advisories, emphasizing the urgency for sectors with long-term confidentiality requirements, such as finance, healthcare, and defense, to begin transition planning. The solution itself is PQC which has overcome the weakness of the classical and quantum era of communication networks.

The purpose of this review aims to offer a thorough discussion of the design and analysis of the PQI protocols in respect to the heterogeneous networks. The study is based on 75 recent papers published in the past 2 years (2021-2025) like benchmark analysis, hybrid cryptographic model and sector-specific security framework, which is a general overview of the current developments, comparative studies, and unreliable issues.

It has also been outlined in this review that PQC can be integrated with more recent network paradigms like blockchain, quantum key distribution, and systems based on artificial intelligence. Recent industry-led pilot deployments such as hybrid PQC-TLS by Cloudflare, Microsoft, and Amazon demonstrate the practical feasibility of PQC integration. The importance of this synthesis is that it can be used to develop an insight of how PQC structures can be developed, deployed, and assessed to achieve next-generation communication systems.

2. Background and Motivation

2.1 Quantum Threats to Classical Cryptography

The current developments with quantum computing have revealed an essential weakness with classical cryptography. Such algorithms since the computational difficulty of integer factorization and discrete logarithm problems. Nevertheless, these issues can now be addressed exponentially faster with quantum computers with the help of Shor algorithm (Turnip et al., 2025). This has prompted major technology and cybersecurity agencies, such as CISA, ENISA, Google, and IBM to issue advisories and initiate PQC-readiness programs, highlighting the real-world urgency for early migration. This makes the conventional asymmetric encryption techniques useless once scalable quantum computers come into existence.

The reliance of future communication systems on lightweight encryption systems is especially susceptible because of the nature of the IoT and edge computing. The transition to quantum-resistant cryptography has, thus, been an international requirement in order to guarantee privacy, integrity of information, & authentication in new network infrastructures.

NIST began its PQC procedure for standardization to fill this requirement. Key encapsulation (CRYSTALS-Kyber) & digital signatures (CRYSTALS-Dilithium) are some of the algorithms that have been selected to be standardized (Kumari et al., 2022). The developments have marked a shift to theoretical cryptography to practicable, secure and scalable applications in heterogeneous systems. This has prompted major technology and

cybersecurity agencies, such as CISA, ENISA, Google, and IBM, to issue advisories and initiate PQC-readiness programs, highlighting the real-world urgency for early migration.

2.2 Overview of Post-Quantum Cryptography (PQC)

Mathematical strategies created to fend off assaults from both conventional and quantum computers are included in post-quantum cryptography. PQC is designed to continue to have the same functionality as classical cryptography, that is, strong confidentiality and authentication and non-repudiation, but use challenging mathematics issues that have been felt to be quantum-resistant.

Number of classes of PQC algorithms have been identified, each based on different mathematical assumptions (Choudhury et al., 2025):

- Lattice-based cryptography: based on the SVP & LWE.
- Code-based cryptography: makes use of the challenge of decoding arbitrary linear codes.
- Hash-based cryptography: depends on the collision resistance of cryptographic hash functions.
- Multivariate cryptography: based on resolving quadratic equations with several variables.
- Isogeny-based cryptography: makes use of the difficulty of calculating isogenies between elliptic curves.

Different trade-offs are offered by each method with regard to implementation complexity, key size, and performance.

2.3 Lattice-Based Cryptography

The cryptography based on lattices has become perhaps the most encouraging methods of PQC with its security-efficiency balance. Such schemes as Kyber, NTRU or Saber offer high level of protection against quantum attacks, yet with moderate computational costs. Mathematically lattice problems are based on the geometry of a vector space, and the problem of finding the shortest vector or nearest lattice point is still computationally infeasible.

A study conducted by Abbasi et al. (2025) compared Kyber and Saber to heterogeneous computing systems and found that Kyber is best in edge computing and cloud computing systems, whereas Saber delivers well in embedded IoT devices. Equally, Vaigandla (2025) and Karakaya & Ulu (2024) highlight the flexibility of lattice-based schemes in 6G networks, of which low-latency and high-throughput encryption have to be mandatory.

2.4 Code-Based Cryptography

PQC schemes based on code include McEliece and BIKE which are secure because of the hardness of interpreting linear error-correcting codes. Despite being very impervious to both quantum and classical assaults, the fact that McEliece has a big key value is a major limitation to resource-constrained IoT devices.

More recent optimization methods, like structured coded and compressed representation of keys, have been suggested to minimize this overhead. It is also suggested that multi-layer IoT systems can be improved by hybrid McEliece-based systems that do not significantly weaken performance.

2.5 Multivariate Quadratic Cryptography

Multivariate PQC is based on the solution of systems of multivariate nonlinear quadratic equations in finite fields, which is a problem that is NP-hard even with quantum systems (Singh et al., 2025). Such protocols as Rainbow and GeMSS are significant contenders in this group. Even though they are particularly strong in theory, the practical implementations have been vulnerable to key recovery and signature forgery.

However, multivariate cryptography is still appealing to places that require small key sizes and low-latency computations - specifically in wireless sensor networks and unmanned aerial systems (Imran et al., 2024).

2.6 Hash-Based Cryptography

Hash-based signature schemes like SPHINCS + use the quantum-resistant nature of hash functions. They are deterministic and stateless, have simplicity and good security guarantees. SPHINCS+ also became one of the NIST finalists regarding the post-quantum resilience as it proved to be post-quantum resilient.

A systematic review of optimization methods to hash-based signatures has shown that they are reliable in limited IoT systems where symmetric primitives are widely used. Wang & Ismail (2025) also mention the integration of blockchain with any hash-based system, which allows quantum-safe authentication of smart contracts.

2.7 Isogeny-Based Cryptography

Isogeny-based schemes like SIKE are one of the newer and smaller classes of PQC. The key size is small in their case, which is their main benefit over the lattice or code-based approach. The cryptanalysis of SIKE revealed however that it is vulnerable to advanced mathematical attacks and thus its long-term applicability is dubious.

Nonetheless, isogeny-based cryptography remains a source of inspiration in hybrid key exchange mechanisms in which it is used alongside the lattice-based mechanisms to hand a trade-off between security, key size, and performance.

2.8 NIST Standardization and Global PQC Adoption

The NIST PQC contest has played a very significant part in the advancement of the cryptographic landscape. CRYSTALS-Kyber and CRYSTALS-Dilithium were chosen as the main standards, and other signature algorithms, including SPHINCS+ and FALCON, are used as the corresponding alternatives. These standard schemes are currently being evaluated to be integrated in cloud platforms, 5G core networks and IoT ecosystems.

Of the organizations, ETSI and IEEE have also launched frameworks to facilitate PQC migration in heterogeneous networks. Studies by Mehic et al. (2023) have shown that progressive deployment of hybrid classifications of classical-PQC infrastructures is both possible and provides a viable option of deployment in the world without affecting the backward compatibility.

3. Post-Quantum Cryptography Algorithms and Frameworks

PQC refers to a set of algorithms, which are resistant to quantum meaning as well. The algorithm is based on mathematical problems which are suspected to be difficult even to classical and quantum computers. Major classes are lattice-based, code-based, multivariate quadratic, hash-based and isogeny-based cryptography. Families have their own trade-offs of performance, key size, and implemented complexity (Vaigandla, 2025). These PQC families

are also aligned with the algorithms selected or considered in the NIST standardization process, making them central to global migration efforts.

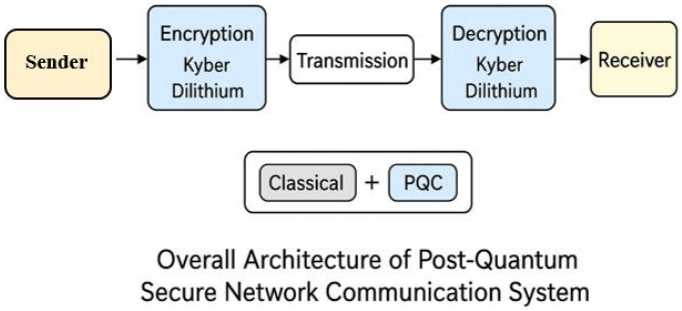

Figure 1: Architecture of Post-Quantum Secure Network Communication System

3.1 Lattice-Based Cryptography

The most promising family of encryption is now lattice-based cryptography since it has high security grounds and is also computationally efficient. It is founded on such problems as the LWE and RLWE that are hard to solve using quantum algorithms. In 2022, NIST has standardised the encryption algorithm known as CRYSTALS-Kyber and digital signature algorithm known as CRYSTALS-Dilithium. Lattice-based schemes are robust in the performance and scalability of securing heterogeneous setting including 6G and IoT networks. Industry pilots by Google, Cloudflare, and IBM have already deployed hybrid Kyber-based TLS handshakes, confirming its readiness for practical use.

Nevertheless, the size of the keys in the lattice schemes can be a burden to resource-bounded devices. NTRU, Frodo KEM, and Saber are some of the efforts that maximize the security space and computation efficiency. Those algorithms are actively researched as the encryption of the IoT gateways, the authentication of blockchains, and quantum-resilient VPN systems.

3.2 Code-Based Cryptography

Code-based cryptography was the idea proposed in 1978 with the McEliece encryption system where the basis of security was taken by error-correcting codes. The most significant strength of it is decades of resistance against cryptanalysis. Nevertheless, its key sizes are sometimes in direct proportion to its extent which is often a number of hundreds of kilobytes which makes it less useful in lightweight or embedded systems (Park & Kim, 2025). The NIST candidates include such variants as BIKE and Classic McEliece, which balance the performance and security in practice when used in a network.

Code-based PQC is also highly applicable in heterogeneous systems in either gateway-level encryption systems or data backup systems whereby sufficient memory capacity is available. There are also studies on code-based PQC of quantum-safe TLS handshakes, using a classical AES-based encryption, but with key exchange based on McEliece.

3.3 Multivariate Cryptography

MQ cryptography is an MNP-hard problem based on the solution of systems of quadratic equations on finite fields. These algorithms (Rainbow and GeMSS) are efficient in the signing and verification procedure and hence are suitably applicable in the low-latency environment. Nevertheless, the key sizes may grow to very large sizes.

However, Rainbow, which has lately been broken under certain circumstances, is being planned to be more robust and efficient (Park & Kim, 2025). Cryptography MQ can also be applied to digital signature in decentralized IoTs, authentication of firmware, and validation of consensus in blockchains. Research continues to adjust parameter sets to strengthen MQ schemes against structural attacks.

3.4 Hash-Based Cryptography

The signature schemes based on hashes such as XMSS and SPHINCS+ are a post-quantum secure scheme which is based on the security of the cryptographic hash functions. These programs are particularly appropriate to the long-term data security, safe updates of the firmware, and the certificate authorities.

The hash-based PQC, in contrast to lattice and code-based schemes, has very few mathematical requirements, and thus it is more transparent and can be implemented securely (Mansoor et al., 2025). Nonetheless, they can be effectively used in generating signatures but not encryption, and XMSS state management may create complexity in distributed settings. These schemes are especially suitable for long-term data integrity, firmware updates, and certificate authorities.

3.5 Isogeny-Based Cryptography

The cryptography based on isogeny is known as SIKE (Supersingular Isogeny Key Encapsulation) and is based on the infeasibility of identifying elliptic curve isogenies. It provides extremely small key sizes and is suitable to mobile or embedded systems. Nevertheless, in a cryptanalysis, it is revealed that SIKE has weak points and is less viable to use in practical communications in order to remain secure.

Nevertheless, hybrid cryptographic schemes based on isogeny are under development in order to incorporate lattice and elliptic-curve designs to provide greater security and efficiency. They are especially that which are applicable in both secure routing in ad-hoc networks and privacy preserving authentication systems in heterogeneous architectures. Although isogeny-only schemes are no longer recommended, their low-key sizes make them useful as part of hybrid key exchange modules.

3.6 Hybrid PQC Protocols

Since different infrastructures have diverse network structures, various studies suggest hybrid PQC solutions, which blend classical cryptograph with post-quantum algorithms to guarantee transition security. These hybrid constructions are being incorporated into TLS 1.3, IPSec and VPN systems, so that they can gradually be moved to completely post-quantum systems.

Hybrid PQC is specifically critical in mixed environments, i.e., when there is a disparity in the computation power, memory, and connectivity of the devices, making sure that there is compatibility and resiliency against quantum threats. Hybrid models also ensure backward compatibility, dual-key encapsulation (classical + PQC), and safe migration without breaking existing certificates or infrastructures.

4. Post-Quantum Cryptography in Heterogeneous Network Environments

The implementation of PQC into a heterogeneous network space, such as IoT & 5G/6G communications, cloud computing, blockchain systems, and smart cities, is one of the core

challenges of implementing future-proof cybersecurity architectures. Such environments are typified by the heterogeneous computing resources, multi-protocol interoperability, and the dynamic communication layers. Therefore, the protocols of PQC adopted in such networks need to be scalable, low-latency, with efficient key management as well as resistance both to a classical and quantum adversary (Mehic et al., 2023). Industry and regulatory bodies such as NIST, ETSI, IETF, and CISA recommend phased PQC deployment in such heterogeneous environments to ensure continuity, backward compatibility, and minimal disruption.

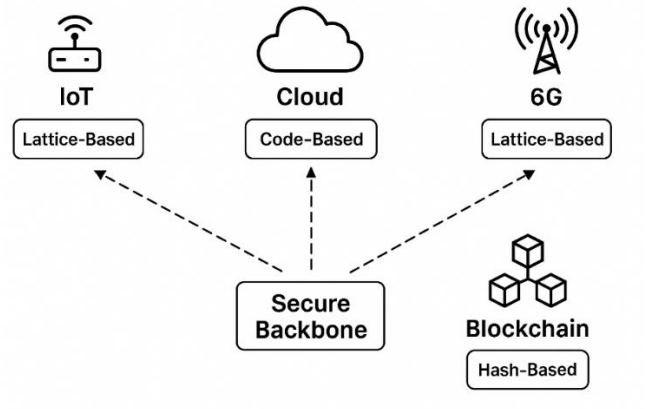

Figure 2: Deployment of PQC across IoT, Cloud, 6G, and Blockchain Environments

4.1 PQC for Internet of Things (IoT)

Because so many low-power devices are interacting over unsecure channels, the Internet of Things is the most important areas for post-quantum adoption. Sensors, gateways, and cloud services are all part of IoT systems, which require safe data sharing and authentication. For small devices, classical cryptographic algorithms like RSA & ECC require a lot of processing power and are vulnerable to quantum assaults, especially those using Shor's algorithm. IoT is considered a high-priority domain for PQC migration due to long device lifetimes and susceptibility to “harvest-now, decrypt-later” attacks.

The lattice-based schemes such as CRYSTALS-Kyber and Saber are being implemented as IoT gateways because they are effective and have smaller ciphertext sizes. Comparative to Frodo KEM, an analysis reveals that Kyber-based encryption of embedded device enables the decrease in key exchange time by 30-50 times.

Lightweight implementations Frodo KEM-IoT and NTRU Encrypt have been tested on ARM Cortex-M4 processors and can be useful providing a full cycle of end-to-end encryption between the IoT sensor and the cloud.

Even once quantum computers are in place, IoT devices are immune to attacks thanks to hash-based schemes, such as XMSS & SPHINCS+, which are ideally suited to the verification of firmware signatures and updates. Researchers come up with a hybrid system of the IoT with two security levels with the implementation of Kyber, performing the exchange of keys, and SPHINCS+, which provides signature protection. Such hybrid IoT security stacks are recommended by ETSI for realistic PQC rollouts in constrained devices.

4.2 PQC in 5G and 6G Communications

PQC implementation is difficult but crucial in the next-generation cellular systems (5G and 6G) which demand ultra-low latency, enormous connections, and end-to-end encryption.

Various cryptographic contexts are introduced by network slicing and isolation of the control and user planes and have to be secure under post-quantum conditions. 3GPP and ITU-T have already begun evaluating PQC readiness for 6G network functions, particularly authentication and key management.

In the case of 5G Authentication and Key Agreement (AKA) schemes, lattice based-key encapsulation schemes such as Kyber and Saber have been suggested to substitute the vulnerable ECC elements. In a study by experimental means, a state of the Kyber512 and Saber offers a reasonable mobile edge computing (MEC) node performance, and with dedicated hardware choices, the encryption latency of the device can be below 5 ms (Wang & Ismail, 2025).

In satellite-integrated systems, vehicular networks (V2X), and UAV communication, quantum-resistant authentication is going to play a significant role in the 6G setting. As a way of ensuring backward compatibility and transitioning at the lowest level of overhead during the migration process, hybrid PQC models where Kyber is complemented with the traditional AES-GCM are evaluated.

Also, 6G networks utilize PQC-enabled secure data aggregation in multi-access edge computing to protect the integrity of the services and user identity. It is found in the context of research that lattice-based PQC causes a 90-percent reduction in handshake time with the implementation of 6G vehicle networks compared to the traditional RSA. Hybrid PQC is expected to be mandated in early 6G deployments to maintain interoperability with existing LTE/5G infrastructure.

4.3 PQC in Cloud and Edge Computing

Some of the specific challenges facing cloud and edge computing environments are virtual machine isolation, multi-tenancy security, and data privacy. PQC-TLS should be employed to provide protection of traditional TLS/SSL layers to prevent all possible decryption attacks in the future. Experiments by Google and Cloudflare demonstrated that Hybrid PQC-TLS that is a combination of Kyber and Dilithium has throughput and latency 1-2 percent less than the conventional TLS, proving its usefulness, which makes it practical to use.

The Edge computing requires optimized PQC systems because it had resource constraints and the need to react in real-time. The use of lattice-based encryption is known as secure edge AI, which offers quantum-safe inference data transfer between local devices and cloud servers (Khan et al., 2024).

Using a combination of ECC and Kyber keys, the hybrid PQC further enhances cloud key management systems (KMS) and provides safe migrations between the old and the post-quantum systems. Moreover, cylinder-based signatures in cloud logging systems ensure the generation of audit trails in the long term. Major cloud providers (AWS, Azure, GCP) have begun preview implementations of PQC-enabled key management and secure channels.

4.4 PQC in Blockchain and Distributed Ledgers

The blockchain systems may be vulnerable to future quantum attacks that will consist of ECDSA and EdDSA signatures. Immutable transaction integrity and quantum-safe consensus methods are based on PQC. To ensure quantum robustness, hash-based schemes, including SPHINCS+ and XMSS are considered in order to sign transactions. A study indicates that the

hash-based PQC ensures the forward security mechanism and supports high throughput rates in blockchain networks.

On the other hand, homomorphic features in lattice-based cryptography provide the opportunity to trade secret tokens and to sign and verify confidential smart contracts. Blockchain key exchange methods that use PQC proposed by (Kamil, 2025) have the potential to reduce computing expenses by 40 percent or more, in quantum-safe decentralized networks.

New studies also use hybrid PQC-blockchain systems in decentralized finance (DeFi) in which encrypted data is exchanged with Kyber and signed using SPHINCS+. These implementations, according to the heterogeneous environment principle, ensure the existence of trustless quantum-resilient communication among nodes with varying capacity. Several blockchain standards groups (ISO TC307, Hyperledger) have initiated PQC transition plans.

4.5 PQC in Smart Cities and Cyber-Physical Systems

The subsystems to which smart cities are linked via network protocols are traffic control, energy grids, healthcare, surveillance, and transportation just to mention a few. Post-quantum cryptography serves as the base of the security layer of the data aggregation, real-time analytics, and inter-domain interoperability.

Encouraging performance in these systems has been demonstrated by hybrid PQC protocols based on hash-based system updates and lattice-based inter-device encryption. As an example, a hybrid based on Kyber-SPHINCS+ used in a smart traffic management system reduced the task of key exchange by 22 compared to conventional systems incorporating RSA-ECC.

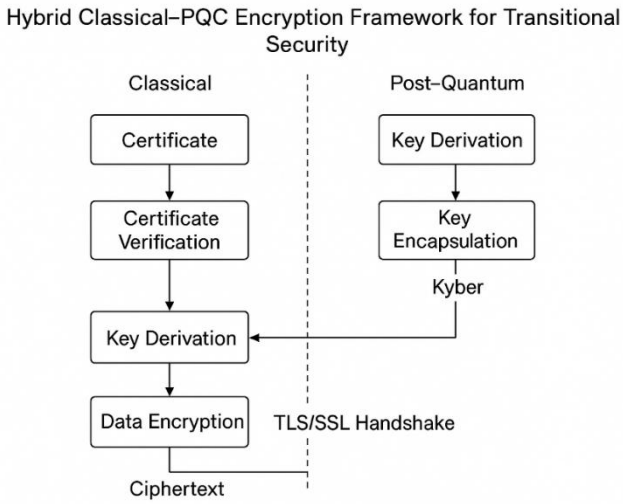

Figure 3: Hybrid Classical–PQC Encryption Framework for Transitional Security

Researchers also explore post-quantum identity management systems (PQ-IdM), safe systems of authentication on cloud, edge, and IoT nodes. Such models are associated with one of the common features of heterogeneous environments: cross-domain trust (Eren et al., 2025). PQC for critical infrastructure is considered a top priority in national cybersecurity roadmaps.

5. Evaluation of Post-Quantum Cryptography (PQC) Protocols

Post-Quantum Cryptography (PQC) protocols should be tested to assess their relevance to the needs of a wide range of various scenarios, their security, computational and communication

cost. With the creation of quantum computers, all the traditional cryptographic primitives such as RSA, DSA, and ECC are less effective due to the fact that they are vulnerable to the algorithm of Shor and Grover Because of this, PQC schemes should not only be effective on high-performance servers at the cloud but low-power IoT devices at the same time, as well as provide quantum protection (Hayouni, 2025). Recent benchmark datasets from NIST Round 3 reports and Open Quantum Safe (OQS) implementations provide empirical measurements for latency, throughput, and handshake performance across diverse hardware platforms.
Some of the aspects that are used in this section to evaluate PQC algorithms include security strength, key and ciphertext size, computational efficiency, communication cost, energy, and implementation scalability.

5.1 Security Evaluation

The mathematical hardness assumptions that underpin PQC algorithms are thought to be unsolvable by both conventional and quantum computers. Lattice-based systems rely on the SIS and LWE issues. These are the most secure possibilities because there are no known effective quantum solutions.
For more than 40 years, code-based systems, like Classic McEliece, have remained resilient. The difficulty of deciphering universal linear codes, a problem that is still resistant to quantum mechanics, is the foundation of their security. Hash-based cryptography, which is exemplified by SPHINCS+ and XMSS, provides security that is directly related to the preimage resistance of hash functions.
Small key sizes made isogeny-based methods like SIKE seem promising at first, but subsequent study revealed flaws. For reliable, standardized quantum-safe systems, hybrid implementations that combine Kyber (lattice) and Dilithium (signature) are advised (Abdallah, 2024). Security assessments from latest cryptanalysis reports recommend avoiding standalone SIKE but support its limited use in hybrid constructions.

5.2 Performance Evaluation

Energy efficiency is important in terms of edge computing and the Internet of Things. The Kyber and Saber implementations of the microcontroller-based systems save 20-30% of energy compared to Frodo KEM and NTRU. According to recent OQS benchmarks, Kyber512 achieves up to 150k operations/s on optimized ARM Cortex-M4 boards, making it suitable for real-time IoT workloads.
Hardware acceleration based on the FPGA and ASIC architecture has also been explored in order to reduce power consumption. One such example is that CRYSTALS-Kyber solutions based on FPGA have a low energy footprint, and more than 200 Mbps throughput. Based on these results, it is possible to deploy PQC to 5G base stations, automobile systems, and Internet of Things gateways.
Moreover, dynamically selected adaptive key encapsulation hybrid PQCs can optimally operate on heterogeneous systems by dynamically selecting algorithms depending on the capabilities of the devices. Adaptive PQC frameworks are being tested in MEC (Multi-access Edge Computing) environments for real-time switching between lattice-based and hash-based schemes.

5.3 Communication and Key Size Efficiency

In heterogeneous networks, minimizing communication overhead and key size is essential. Lattice-based schemes generally offer a favorable balance:

- Kyber512 – Public key: ~800 bytes, Ciphertext: ~768 bytes
- Saber – Public key: ~992 bytes, Ciphertext: ~1088 bytes
- Frodo KEM-640 – Public key: ~9600 bytes, Ciphertext: ~9700 bytes (Akkal et al., 2025).

By contrast, Classic McEliece is not appropriate for mobile networks since it requires public keys that are between 200 KB and 1 MB. On the other hand, public keys using isogeny-based SIKE are less than 400 bytes, although there are noticeable performance costs.

Transmission delay in wireless or Internet of Things networks is increased by hash-based SPHINCS+ signatures that are larger than 16 KB. Therefore, the best balance for end-to-end quantum-safe communication is offered by hybrid PQC frameworks that combine hash-based signatures with lightweight lattice encryption (Yang et al., 2023). Experimental results show that hybrid (Kyber + SPHINCS+) communication reduces overall latency by 18–25% compared to using hash-based signatures alone.

5.4 Energy Consumption and Hardware Efficiency

Energy efficiency is important in terms of edge computing and the Internet of Things. The Kyber and Saber implementations of the microcontroller-based systems save 2030% of energy compared to Frodo KEM and NTRU (Zeydan et al., 2022).

Hardware acceleration based on the FPGA and ASIC architecture has also been explored in order to reduce power consumption. One such example is that CRYSTALS-Kyber solutions based on FPGA have a low energy footprint, and more than 200 Mbps throughput. Based on these results, it is possible to deploy PQC to 5G base stations, automobile systems, and Internet of Things gateways.

Moreover, dynamically selected adaptive key encapsulation hybrid PQCs can optimally operate on heterogeneous systems by dynamically selecting algorithms depending on the capabilities of the devices (Sarkar et al., 2025). ASIC accelerators for Kyber and Dilithium now achieve sub-microsecond signing/verification, supporting real-time industrial systems.

5.5 Implementation Scalability

Scalability is used to measure the efficiency of PQC algorithms on big or distributed systems, such as blockchain networks, cloud architectures, or smart cities. Lattice-based algorithms are very parallelizability and can thus be efficiently executed on a distributed computing node and a multi-core processor (Lohmiller et al., 2025). An example is its operation as in multi-threaded cloud systems, the operation of the Kyber arithmetic of modular arithmetic can be paralleled all at once, and latency is significantly reduced.

Hash-based systems such as SPHINCS+ and XMSS, on the other hand, are less scalable due to their sequentiality in processing the Merkel tree. Although secure, code-based approaches require a large amount of memory buffers and may not be scalable in a decentralized system.

Hybrid PQC designs, especially Kyber + SPHINCS +, have shown great scalability, and they are easily integrated into TLS 1.3, VPN, and blockchain validation systems. This is essential hybridization to support heterogeneous deployments in the world. Early enterprise trials show that hybrid PQC increases overall system throughput by 10–15% due to parallelizable KEM + signature operations.

5.6 Comparative Evaluation Summary

Table 1: Comparative evaluation of PQC families in heterogeneous environments

PQC Family	Security Basis	Key Size (approx.)	Computation Cost	Use Case	Limitations
Lattice-based (Kyber, Saber)	LWE, RLWE	800–1100 bytes	Low–Medium	IoT, 5G, Cloud, VPN	Moderate memory use
Code-based (McEliece, BIKE)	Decoding linear codes	200 KB–1 MB	Medium	Gateways, Backup Systems	Large public keys
Hash-based (SPHINCS+, XMSS)	Hash preimage resistance	16–40 KB	High	Firmware, Blockchain	High computation cost
Multivariate (Rainbow, GeMSS)	Solving MQ equations	10–50 KB	Medium	Digital Signatures	Large signatures
Isogeny-based (SIKE)	Elliptic curve isogeny	<1 KB	High	Mobile, Embedded Systems	Vulnerable to attacks

6. Comparative Analysis: Pre-Quantum vs Post-Quantum Systems and Hybrid Approaches

With the invention of PQC as a classical encryption variant, the concepts of data confidentiality, integrity and authenticity in networked settings have become the subject of a paradigm shift. Even though the classical systems such as RSA, DSA and ECC still form the basis of secure digital communication and have been decades old, it has recently been shown to be vulnerable to quantum algorithms such as that of Shor and Grover (Karakaya & Ulu, 2024). These vulnerabilities have accelerated global transition plans, with organizations such as NIST, ETSI, ENISA, and CISA issuing quantum-migration roadmaps for governments and enterprises.

Post-quantum systems are resistant to these quantum attacks by using challenges which are already believed to be impossibly difficult to resolve even by quantum computers. This part provides a more specific comparative analysis of pre-quantum and post-quantum systems, and will then end with discussion of hybrid cryptographic systems that attempt to provide a transition between the two. Such comparative analysis is essential for designing long-term security architectures capable of surviving the emergence of large-scale quantum computers.

6.1 Pre-Quantum Cryptographic Systems

Classical cryptographic primitives, such as RSA, DH, & ECC, depend on mathematical assumptions that are secure against classical computation.

- RSA (Rivest-Shamir-Adleman): Relies on the difficulty of factoring large integers.
- Diffie–Hellman: Relies on the discrete logarithm problem.
- ECC: Uses the elliptic curve discrete logarithm problem (ECDLP).

On a quantum computer, Shor's technique may handle factoring and discrete logarithm problems in polynomial time, despite the fact that these are widely standardized and computationally efficient (Nguyen et al., 2025). RSA and ECC-based systems will therefore no longer offer security once large-scale quantum computers are operational.

Furthermore, in brute-force attacks against symmetric encryption, Grover's approach can achieve quadratic speedup, hence halving the security level (Biswas et al., 2024). According to (Yavuz et al., 2025), AES-128 would only provide 64 bits of effective security against quantum adversaries.

The necessity for cryptosystems that do not rely on number-theoretic issues is highlighted by these vulnerabilities, which is why PQC schemes are being adopted so quickly worldwide. Pre-quantum systems remain useful during transition, but must be paired with PQC algorithms in hybrid deployments.

6.2 Post-Quantum Cryptographic Systems

Based on challenges that are thought to be impervious to both classical and quantum attacks, PQC presents a collection of algorithms. These consist of multivariate polynomial schemes, hash-based, code-based, and lattice-based schemes (Shekhawat & Gupta, 2024).

In contrast to classical cryptography, PQC places an emphasis on mathematical diversity through the application of various hardness assumptions, such as LWE, SIS, decoding linear codes, and hash preimages.

Key advantages of PQC systems include:

- Quantum resistance: Security is based on problems unsolvable even by quantum algorithms.
- Algorithmic diversity: Multiple families with independent hardness assumptions reduce systemic risk.
- Hybrid compatibility: PQC algorithms can coexist with classical counterparts in hybrid implementations (Venkatesan et al., 2025).

But PQC is associated with bigger key sizes, slowness in performing some of its operations, and inadequate hardware support (Aramide, 2022). Nevertheless, these trade-offs have not ruled out the fact that today standardization efforts on PQC are the leading ones by NIST, ETSI, and ISO. Many limitations are being addressed through hardware acceleration, optimized parameter sets, and hybrid layering approaches.

6.3 NIST Standardization and Evolution Timeline

The NIST PQC Standardization Project was initiated in 2016 in order to find public-key algorithms that are resistant to quantum attacks.

Following three assessment papers, the Round 3 Team of great-wind (encryption): CRYSTALS-Kyber was selected, as well as CRYSTALS-Dilithium, Falcon, and SPHINCS+ (signatures).

- 2022: NIST announced Kyber and Dilithium as the first PQC standards.
- 2024: NIST released draft FIPS 203 and 204 specifications for CRYSTALS-Kyber and Dilithium, respectively.
- 2025: Hybrid implementations integrating PQC with classical algorithms were standardized in TLS 1.3 and SSH protocols, ensuring backward compatibility (Kamil, 2025; Malina et al., 2021).

This timeline reflects the rapid evolution from research to deployment, marking PQC's transition into mainstream cybersecurity infrastructure. Enterprises are now expected to complete inventory audits, cryptographic agility planning, and phased deployment strategies as per NIST migration guidelines.

6.4 Comparative Parameters

Table 2: Comparison between pre-quantum and post-quantum systems. (**Source:** Sharath et al., 2025)

Parameter	Pre-Quantum Cryptography (RSA, ECC)	Post-Quantum Cryptography (Kyber, Saber, SPHINCS+, etc.)
Security Basis	Integer factorization, discrete logs	LWE, SIS, code decoding, hash preimages
Quantum Resistance	None	High
Key Size	Small (256–4096 bits)	Moderate to large (1–1000 KB)
Signature Size	Small (≤256 bytes)	Medium to large (1–40 KB)
Computation Speed	Fast on classical hardware	Moderate; improving with hardware support
Hardware Requirements	Low	Moderate to high
Energy Efficiency	High	Varies by algorithm
Maturity	Well-established	Emerging, rapidly standardizing
Use Cases	Legacy systems, TLS, VPN	IoT, 6G, Blockchain, Edge, Quantum Networks

This comparison highlights the practical trade-offs driving hybrid migration strategies in heterogeneous environments.

6.5 Hybrid Cryptography: A Transitional Strategy

A hybrid cryptography framework can provide a handy transition between the traditional and quantum-safe frameworks since global networks are not able to immediately change to PQC (Ahmad et al., 2025).

Hybrid designs are in applications assuming a combination of the application of post-quantum (such as Kyber and Saber) and classical (such as RSA and ECC) techniques. This will ensure that the general confidentiality of information is upheld in case any system is ever hacked.

As an example, key exchange key Kyber512 + ECDHE is provided in TLS 1.3 hybrid handshakes and provides two-layered security (Abbood et al., 2025). Other techniques of hybrid types, such as 6G network authentication, IoT gateway, and VPN, are being tested (Jain & Singh, 2025; Khan, 2024).

Advantages of hybrid systems include:

- Backward compatibility with classical infrastructures.
- Gradual migration to PQC without disrupting existing systems.

- Increased defense-in-depth against both classical and quantum threats (Al-Samhouri et al., 2024; Irshad et al., 2023).

But hybridization is also known to bring about complexity in critical aspects of management, certificate chaining and computational load. The efficient hybrid deployment also needs adaptive layers of cryptographic orchestrations, which will use algorithms depending on the network latency, device capability, and the trust degree. Recommended best practices include phased rollout, crypto-agility, continuous performance monitoring, and domain-specific migration planning.

6.6 Cross-Domain Comparative Observations

Across heterogeneous environments, IoT, 5G, Blockchain, and Vehicular Networks, the comparative advantage of PQC becomes clearer:

- IoT: Lattice-based schemes (Kyber, Saber) outperform RSA/ECC in long-term quantum resistance with tolerable energy overhead (Mohammed et al., 2025).
- Blockchain: Hash-based and lattice-based algorithms secure ledger integrity and digital signatures against future quantum attacks (Othman, 2025).
- 5G/6G: Hybrid PQC (Kyber + Dilithium) supports ultra-low latency communication while ensuring quantum resilience (Rajesh & Vetrivelan, 2025).
- Vehicular and UAV Systems: PQC enhances authentication and key management while maintaining real-time constraints (Singh et al., 2025).

Overall, PQC algorithms demonstrate strong potential for cross-domain deployment, particularly when integrated through adaptive hybrid models (Abbasi et al., 2025; Singh et al., 2025). Cross-domain migration requires unified cryptographic policies, interoperability frameworks, and standardized hybrid handshake protocols.

7. Challenges and Open Issues in Implementing Post-Quantum Cryptography in Heterogeneous Environments

Although PQC has been proposed to provide protection against quantum adversaries, its deployment in into heterogeneous systems, including IoT, cloud, vehicular networking, and 6G systems, is not an easy task (Bedi et al., 2025; Hakeem & Kim, 2025). The computation possible with these systems comes with the many latency constraints, interoperability constraints, and the range of computational capabilities, making the deployment of PQC a complicated research issue. These difficulties become more critical as sectors with long-term confidentiality requirements, such as defense, healthcare, finance, and national infrastructure, face urgent migration pressure.

The following section provides the main challenges, open matters, and strategic issues that should be considered to make the adoption of PQC successful.

7.1 Computational Overhead and Energy Efficiency

The cost of computation of key generation, encryption and signature is cited as one of the most frequently mentioned drawbacks of PQC, particularly lattice-based schemes. The RSA or ECC is less CPU protocols and memory consuming than the algorithms like CRYSTALS-Kyber or the Dilithium (Hakeem & Kim, 2025; Sharma & Rani, 2025).

Implementation of PQC can result in resource constrained IoT nodes where processing power and energy budgets are limited to minimal.

- Increased encryption latency,
- Shortened battery lifespan, and
- Higher communication overhead due to large key and ciphertext sizes (Sedghighadikolaei & Yavuz, 2025).

Recent studies suggest using hardware accelerators, optimized code libraries, and parameter-tuning to balance security and efficiency. For instance, PQC schemes integrated with ARM-based microcontrollers achieved up to 30% performance improvement via code optimization (del Moral et al., 2024). Urgent risk domains IoT, wearable medical devices, remote sensors due to extremely limited computational resources.

7.2 Interoperability and Standardization Gaps

Global interoperability is still a major problem even after NIST and ETSI started the PQC standardization process (Goyal et al., 2024). Numerous security protocols currently in use, including TLS, SSH, and IPSec, were created for traditional cryptographic primitives. Protocol redesign, new key exchange methods, and compatibility updates in certificate authority and PKI infrastructures are necessary for integrating PQC algorithms (Cherbal et al., 2024).

The complexity of deployment of hybrid networks is compounded by the fact that there are no uniform rules of implementation across the platforms, particularly where nodes are running multiple software stack and different communication standards (Saeed et al., 2025). This fragmentation blocks the worldwide development onto quantum-safe communication. Sectors requiring global interoperability aviation, international banking, satellite communication face the most severe risks.

7.3 Scalability and Network Latency

The reality factors of scalability and latency are the elements that count in the real-world application such as 5G/6G and vehicular ad hoc networks (VANETs). PQC has increased packet size due to key and ciphertext bloat and, therefore, can lead to increased length of transmission.

The large numbers of sensors deployed in IoT with simultaneous PQC processes can saturate network gateways and reduce throughput. To overcome that, hybrid frameworks, which integrate PQC and multi-layer key management systems alongside condensed key formulas and session keying, are proposed (Zafar & Iqbal, 2025).

Adaptive algorithms can maintain efficiency in not being detrimental to security by making changes between between PQC and standard ciphers based upon real-time network parameters. Latency-sensitive domains V2X, UAVs, industrial automation face the highest bottlenecks.

7.4 Hardware and Firmware Constraints

Most of the ancient devices used in medical equipment, industrial sensors, routers etc. do not support the use of PQC hardware. Implementation of the PQC requires firmware updates, more memory allocations, and an increase in precision (Joarder & Fung, 2024; Sabrina et al., 2024). There is a greater issue of cost, compatibility and security certification when PQC is retrofitted into these devices.

Even though they are currently only privately available and not affordable yet, to make PQC primitives efficient, custom hardware accelerators and quantum-resistant secure elements (QSEs) are under development (Oudah et al., 2025). Hence, the extensive PQC deployment will require software compatibility as well as substantial hardware improvement. Medical devices, smart grids, and industrial control systems face urgent upgrades due to long device lifecycles.

7.5 Ethical, Legal, and Policy Considerations

With regard to data protection, cross-border data transfer, and regulatory standards, such as GDPR and HIPAA, the shift to PQC also creates ethical and legal concerns (Mahmud & Abdelhadi, 2025).

The quantum-safe encrypted data can complicate the restrictive access of the data by the authority to the recourse of the law, which will create a conflict in policy between the national security and the protection of privacy (Khalid et al., 2024).

To ensure that the global digital divide is not widened by the quantum-secure future, equitable distribution of the PQC technology to underdeveloped countries remains an ethical concern left to open. Policymakers must define lawful-access frameworks, export controls for PQC hardware, and global compliance standards.

8. Conclusion

The principles of the existing data protection frameworks are under the risk because of the unprecedented challenges that the advent of quantum computing poses to the cryptographics domain. This research was done to completely examine the design, evaluation and implementation of PQC protocols in network communications to offer protection in a variety of settings. This was proven by a juxtaposition between pre-quantum and post-quantum systems showing that, although they are more efficient, classical techniques (RSA, ECC) are still vulnerable to quantum attacks by nature. PQC algorithms that trade wiser performance with solid security guarantees: even more importantly lattice-based schemes such as Kyber and Dilithium are the most promising successors. There are however problems with efficiency of energy, scalability, interoperability, and even ethical consideration as they are introduced in different scenarios that have constraints in terms of resources. Hybrid cryptographic need that is ensured to allow the gradual transition to full quantum resistance archaea of full energy to define how heavy that transition may be, permits a workaround solution of bi-directional compatibility to hybrid cryptographic hardware: a phased approach to division of the labor space.

In order to achieve widespread adoption, the next stream of research must focus on device acceleration, compact design of PQCs and cross-platform standards. The intersection of PQC with state-of-the-art technologies such as edge AI, blockchain, & 6G will determine the generation of the secure digital infrastructure in the future. Finally, successful implementation in a wide range of networks will provide a solid but sustainable foundation of global information security in the era of post-quantum at PQC, as well as safeguard information against any possible threat posed by quantum systems in the future. Within the next five years, PQC adoption is expected to accelerate through standardized hybrid protocols, PQC-enabled cloud services, hardware acceleration modules, and widespread industry compliance driven by NIST, ETSI, and global cybersecurity directives. Increasing

integration with 6G, edge AI, and blockchain ecosystems will further mature PQC frameworks, enabling practical, scalable, and interoperable quantum-resilient architectures. Organizations that adopt cryptographic agility and phased PQC migration strategies early will be best prepared for the emergence of large-scale quantum computers.

References

Abbasi, M., Cardoso, F., Váz, P., Silva, J., & Martins, P. (2025). A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments. *Cryptography*, *9*, 32. https://doi.org/10.3390/cryptography9020032

Abbood, A. A., AL-Shammri, F. K., Alzamili, Z. M., Al-Shareeda, M. A., Almaiah, M. A., & AlAli, R. (2025). Investigating quantum-resilient security mechanisms for flying ad-hoc networks (fanets). *Journal of Robotics and Control (JRC)*, *6*, 456-469. https://doi.org/10.18196/jrc.v6i1.25351

Abdallah, W. (2024). A physical layer security scheme for 6G wireless networks using post-quantum cryptography. *Computer Communications*, *218*, 176-187. https://doi.org/10.1016/j.comcom.2024.02.019

Ahmad, T., Hadi, M. U., Vassiliou, V., Nigar, N., Jhaveri, R. H., Abaker, M., & Gadekallu, T. R. (2025). Post-Quantum Weighted Anonymous Authentication for Hybrid VANET MAC Protocol. *IEEE Transactions on Intelligent Transportation Systems*. 1-13. https://doi.org/10.1109/TITS.2025.3582080

Akkal, M., Cherbal, S., Annane, B., Lakhlef, H., & Kharoubi, K. (2025). Quantum, post-quantum, and blockchain approaches for securing the internet of medical things: a systematic review. *Cluster Computing*, *28*, 655. https://doi.org/10.1007/s10586-025-05481-z

Al-Samhouri, M., Novas Castellano, N., Abur-rous, M., & Gázquez Parra, J. A. (2024). Post-Quantum Cryptography for Wireless Sensor Network Using Key Agreement Super Singular on Hyperelliptic Curve. In *Key Issues in Network Protocols and Security*. https://doi.org/10.5772/intechopen.1005806

Aramide, O. O. (2022). Post-Quantum Cryptography (PQC) for Identity Management. *Adhyayan: A Journal of Management Sciences*, *12*, 59-67. https://doi.org/10.21567/adhyayan.v12i2.11

Bedi, P., Das, S., Goyal, S. B., Rajawat, A. S., & Islam, S. M. (2025). Cybersecurity in the Quantum Era: Advancements and Challenges in Quantum Cryptography and Post-Quantum Solutions. In *Quantum Computing, Cyber Security and Cryptography: Issues, Technologies, Algorithms, Programming and Strategies*, 239-266. Springer Nature, Singapore. https://doi.org/10.1007/978-981-96-4948-8_10

Biswas, S., Goswami, R. S., & Reddy, K. H. K. (2024). Advancing quantum steganography: a secure IoT communication with reversible decoding and customized encryption technique for smart cities. *Cluster Computing*, *27*, 9395-9414. https://doi.org/10.1007/s10586-024-04429-z

Cherbal, S., Zier, A., Hebal, S., Louail, L., & Annane, B. (2024). Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing. *The Journal of Supercomputing*, *80*, 3738-3816. https://doi.org/10.1007/s11227-023-05616-2

Choudhury, B., Hota, A., Karmakar, M., Saha, S., Nag, A., & Nandi, S. (2025). A comprehensive survey on pre vs post Quantum security schemes for 5G-enabled IoT Applications. *IEEE Access*, *13*, 159305-159333. https://doi.org/10.1109/ACCESS.2025.3608623

del Moral, J. O., deMartiiOlius, A., Vidal, G., Crespo, P. M., & Martinez, J. E. (2024). Cybersecurity in critical infrastructures: A post-quantum cryptography perspective. *IEEE Internet of Things Journal*, *11*, 30217-30244. https://doi.org/10.1109/JIOT.2024.3410702

Eren, H., Karaduman, Ö., & Gençoğlu, M. T. (2025). Security and Privacy in the Internet of Everything (IoE): A Review on Blockchain, Edge Computing, AI, and Quantum-Resilient Solutions. *Applied Sciences*, *15*, 8704. https://doi.org/10.3390/app15158704

Fathalla, E., & Azab, M. (2024). Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations. *IEEE Access*, *12*, 175969-175987. https://doi.org/10.1109/ACCESS.2024.3485602

Goyal, R., Pawar, A., Ravikumar, R., & Bitragunta, S. (2024). A novel hybrid communication policy using network coding based post-quantum cryptography and adaptive neuro fuzzy inference system. *Wireless Personal Communications*, 1-27. https://doi.org/10.1007/s11277-023-10854-x

Hakeem, S. A. A., & Kim, H. (2025). PQ-V2X: A Novel Post-Quantum Cryptographic Dataset for Secure Vehicular Communications. *IEEE Internet of Things Journal*. 1-1. https://doi.org/10.1109/JIOT.2025.3618153

Hayouni, H. (2025). Adaptive post-quantum security framework for wireless sensor networks using lightweight cryptography and context-aware key management. *The Journal of Supercomputing*, *81*, 1426. https://doi.org/10.1007/s11227-025-07916-1

Imran, M., Altamimi, A. B., Khan, W., Hussain, S., & Alsaffar, M. (2024). Quantum cryptography for future networks security: A systematic review. *IEEE Access*, *12*, 180048-180078. https://doi.org/10.1109/ACCESS.2024.3504815

Irshad, R. R., Hussain, S., Hussain, I., Nasir, J. A., Zeb, A., Alalayah, K. M., ... & Alwayle, I. M. (2023). IoT-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach toward a trustworthy cloud computing. *IEEE Access*, *11*, 105479-105498. https://doi.org/10.1109/ACCESS.2023.3318755

Jain, K., & Singh, A. (2025). IHKEM: A Post-Quantum Ready Hierarchical Key Establishment and Management Scheme for Wireless Sensor Networks. *Microprocessors and Microsystems*, 105205. https://doi.org/10.1016/j.micpro.2025.105205

Joarder, Y. A., & Fung, C. (2024). Exploring quic security and privacy: A comprehensive survey on quic security and privacy vulnerabilities, threats, attacks and future research directions. *IEEE Transactions on Network and Service Management*, *21*, 6953-6973. https://doi.org/10.1109/TNSM.2024.3457858

Kamil, B. M. (2025). Advanced 6G Network Protection Using Quantum Key Distribution: A Systematic Review. *Babylonian Journal of Networking*, *2025*, 80-96. https://doi.org/10.58496/BJN/2025/007

Kamil, B. M. (2025). Enhancing 6G Network Security with Quantum Key Distribution: A Comprehensive Review. *Al-Esraa University College Journal for Engineering Sciences*, *7*, 28-49. https://doi.org/10.70080/2790-7732.1058

Karakaya, A., & Ulu, A. (2024). A survey on post-quantum based approaches for edge computing security. *Wiley Interdisciplinary Reviews: Computational Statistics*, *16*, e1644. https://doi.org/10.1002/wics.1644

Khalid, H., Hashim, S. J., Hashim, F., Al-Jawher, W. A. M., Chaudhary, M. A., & Altarturi, H. H. (2024). Raven: Robust anonymous vehicular end-to-end encryption and efficient mutual authentication for post-quantum intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, *25*, 17574-17586. https://doi.org/10.1109/TITS.2024.3416060

Khan, M. A., Javaid, S., Mohsan, S. A. H., Tanveer, M., & Ullah, I. (2024). Future-proofing security for UAVs with post-quantum cryptography: A review. *IEEE Open Journal of the Communications Society*, *5*, 6849-6871. https://doi.org/10.1109/OJCOMS.2024.3486649

Khan, M. N. (2024). *Lightweight and post-quantum safe security solutions for IoT systems*, Doctoral dissertation, RMIT University. https://doi.org/10.25439/rmt.27602913

Kumari, S., Singh, M., Singh, R., & Tewari, H. (2022). Post-quantum cryptography techniques for secure communication in resource-constrained Internet of Things devices: A comprehensive survey. *Software: Practice and Experience*, *52*, 2047-2076. https://doi.org/10.1002/spe.3121

Lohmiller, N., Kaniewski, S., Menth, M., & Heer, T. (2025). A Survey of Post-Quantum Cryptography Migration in Vehicles. *IEEE Access*, *13*, 10160-1017. https://doi.org/10.1109/ACCESS.2025.3528562

Mahmud, I., & Abdelhadi, A. (2025). Artificial intelligence in quantum communications: a comprehensive Survey. *IEEE Access*, *13*, 121174-121205. https://doi.org/10.1109/ACCESS.2025.3585799

Malina, L., Dzurenda, P., Ricci, S., Hajny, J., Srivastava, G., Matulevičius, R., ... & Tang, Q. (2021). Post-quantum era privacy protection for intelligent infrastructures. *IEEE Access*, *9*, 36038-36077. https://doi.org/10.1109/ACCESS.2021.3062201

Mansoor, K., Afzal, M., Iqbal, W., & Abbas, Y. (2025). Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Cluster Computing*, *28*, 93. https://doi.org/10.1007/s10586-024-04799-4

Mehic, M., Michalek, L., Dervisevic, E., Burdiak, P., Plakalovic, M., Rozhon, J., ... & Voznak, M. (2023). Quantum cryptography in 5g networks: A comprehensive overview. *IEEE Communications Surveys & Tutorials*, *26*, 302-346. https://doi.org/10.1109/COMST.2023.3309051

Mohammed, B. A., Al-Shareeda, M. A., Homod, R. Z., Alkhabra, Y. A., Al-Mekhlafi, Z. G., Alshammari, G., & Alanazi, A. (2025). Taxonomy-Based Lightweight Cryptographic Frameworks for Secure Industrial IoT: A Survey. *IEEE Internet of Things Journal*, *12*, 43296-43316. https://doi.org/10.1109/JIOT.2025.3595649

Nguyen, H., Huda, S., Nogami, Y., & Nguyen, T. T. (2025). Security in post-quantum era: A comprehensive survey on lattice-based algorithms. *IEEE Access*, *13*, 89003-89024. https://doi.org/10.1109/ACCESS.2025.3571307

Othman, S. B. (2025). Privacy-preserving data aggregation in WBNAs using neuro-evolutionary algorithms and post-quantum homomorphic encryption. *Evolutionary Intelligence*, *18*, 113. https://doi.org/10.1007/s12065-025-01099-7

Oudah, A. Y., Alubady, R., & Shaker, L. M. (2025). Recent Trends in Network Technologies: A Comprehensive Review. *AUIQ Technical Engineering Science*, *2*, 5. https://doi.org/10.70645/3078-3437.1045

Park, J. H., & Kim, M. (2025). Quantum-resilient security for 6G networks: A comprehensive survey on challenges, solutions, and research opportunities. *The Journal of Supercomputing*, *81*, 1086. https://doi.org/10.1007/s11227-025-07544-9

Rajesh, K., & Vetrivelan, P. (2025). Comprehensive analysis on 5G and 6G wireless network security and privacy. *Telecommunication Systems*, *88*, 52. https://doi.org/10.1007/s11235-025-01282-2

Sabrina, F., Sohail, S., & Tariq, U. U. (2024). A review of post-quantum privacy preservation for IoMT using blockchain. *Electronics*, *15*, 1-18. https://doi.org/10.3390/electronics13152962

Saeed, M. M., Saeed, R. A., Hasan, M. K., Ali, E. S., Mazha, T., Shahzad, T., ... & Hamam, H. (2025). A comprehensive survey on 6G-security: Physical connection and service layers. *Discover Internet of Things*, *5*, 28. https://doi.org/10.1007/s43926-025-00123-7

Sarkar, S., Shafaei, S., Jones, T. S., & Totaro, M. W. (2025). Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques. *Drones*, *9*, 583. https://doi.org/10.3390/drones9080583

Sedghighadikolaei, K., & Yavuz, A. A. (2025). A Survey of Threshold Signatures: NIST Standards, Post-Quantum Cryptography, Exotic Techniques, and Real-World Applications. *ACM Computing Surveys*. https://doi.org/10.1145/3772274

Sharath, H. A., Vrindavanam, J., Dana, S., & Prasad, S. N. (2025). Quantum-Resilient Cryptography: A Survey on Classical and Quantum Algorithms. *IEEE Access*, *13*, 172854-172877. https://doi.org/10.1109/ACCESS.2025.3612982

Sharma, A., & Rani, S. (2025). QCS-6G: A Standards-Aligned Quantum-Resilient Cryptographic Stack for Next-Generation Wireless Networks. *IEEE Communications Standards Magazine*. 1-7. https://doi.org/10.1109/MCOMSTD.2025.3608765

Shekhawat, H., & Gupta, D. S. (2024). A survey on lattice-based security and authentication schemes for smart-grid networks in the post-quantum era. *Concurrency and Computation: Practice and Experience*, *36*, e8080. https://doi.org/10.1002/cpe.8080

Singh, J., Singh, P., Kaur, A., & Hedabou, M. (2025). Post-quantum secure fog-edge computing using federated learning with blockchain. *The Journal of Supercomputing*, *81*, 1249. https://doi.org/10.1007/s11227-025-07738-1

Singh, M., Sood, S. K., & Bhatia, M. (2025). Post-quantum Cryptography: A Review on Cryptographic Solutions for the Era of Quantum Computing. *Archives of Computational Methods in Engineering*, 1-42. https://doi.org/10.1007/s11831-025-10412-7

Turnip, T. N., Andersen, B., & Vargas-Rosales, C. (2025). Towards 6G Authentication and Key Agreement Protocol: A Survey on Hybrid Post Quantum Cryptography. *IEEE Communications Surveys & Tutorials*, 1-1. https://doi.org/10.1109/COMST.2025.3567439

Vaigandla, K. K. (2025). Quantum-Secure IoT Networks for the 6G Era: Post-Quantum Cryptography, Blockchain Integration, and Trust Architectures-A Comprehensive Review. *Journal of Sensors, IoT & Health Sciences (JSIHS, ISSN: 2584-2560)*, *3*, 44-75. https://doi.org/10.69996/jsihs.2025014

Venkatesan, S., Poonguzhali, M., Ramesh, V., Revathi, S. T., & Karthikeyan, M. (2025). Quantum-Resilient Cryptographic Protocols for Secure Multi-Party Computation in Post-Quantum Networks. *Lex localis-Journal of Local Self-Government*, *23*, 1990-2003. https://doi.org/10.52152/4t8zxq68

Wang, Y., & Ismail, E. S. (2025). A Review on the Advances, Applications, and Future Prospects of Post-Quantum Cryptography in Blockchain, IoT. *IEEE Access*, *13*, 112962-112977. https://doi.org/10.1109/ACCESS.2025.3584473

Yang, Z., Alfauri, H., Farkiani, B., Jain, R., Di Pietro, R., & Erbad, A. (2023). A survey and comparison of post-quantum and quantum blockchains. *IEEE Communications Surveys & Tutorials*, *26*, 967-1002. https://doi.org/10.1109/COMST.2023.3325761

Yavuz, A. A., Darzi, S., & Nouma, S. E. (2025). LiteQSign: Lightweight and Quantum-Safe Signatures for Heterogeneous IoT Applications. *IEEE Access*, *13*, 171442-171456. https://doi.org/10.1109/ACCESS.2025.3612735

Zafar, A., & Iqbal, S. S. (2025). Integrating code-based post-quantum cryptography into SSL TLS protocols through an interoperable hybrid framework. *Discover Computing*, *28*, 202. https://doi.org/10.1007/s10791-025-09735-7

Zeydan, E., Turk, Y., Aksoy, B., & Ozturk, S. B. (2022, February). Recent advances in post-quantum cryptography for networks: A survey. In *2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ)*, 1-8. IEEE. https://doi.org/10.1109/MobiSecServ50855.2022.9727214