TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52046

Post Quantum Cryptography in the Era of 6G and IoT: A Comprehensive Review

Vishal Kumar
School of Computer Science and Engineering, Galgotias University, Greater Noida, India
vishuv3466@gmail.com

KEYWORD

Post-Quantum Cryptography (PQC); Quantum Key Distribution (QKD); Internet of Things (IoT); Elliptic Curve Cryptography (ECC); Number Theoretic Transform (NTT)

ABSTRACT

The emergence of quantum computers presents a serious challenge to the widely used public-key cryptographic algorithms, including RSA and Elliptic Curve Cryptography (ECC), that are currently central to the digital security landscape. Meanwhile, new technologies such as Sixth Generation(6G) communication networks, the Internet of Things (IoT), blockchain platforms, and cloud computing infrastructures must also be equipped with strong and scalable security measures to safeguard sensitive information and communications. Post-Quantum Cryptography (PQC) has been one of the solutions that has been suggested as a strong potential solution that offers cryptographic algorithms that are secure against quantum attacks as well as classical attacks and is compatible with current digital systems. This review paper provides a detailed survey of recent advances in PQC that include the most important cryptographic families including lattice-based, code-based, and hash-based cryptography. The National Institute of Standards and Technology (NIST) standardization efforts are discussed in detail, such as ML-KEM (Kyber), ML-DSA (Dilithium), Falcon, and SPHINCS+. Over two dozen recent research papers are evaluated to test the security, performance, implementation and practicality of PQC algorithms in limited resource settings.

1. Introduction

The fast development of digital infrastructure, which is characterized by the transition to 6G mobile networks, and the exponential rise in the number of devices in the Internet of Things (IoT), has transformed global connectivity. Nonetheless, this growth has also led to the increase in the susceptibility of critical systems to the emerging cyber threats. The most important aspect of those worries is that quantum computing is poised to overturn the cryptographic principles of contemporary security. Classical public-key cryptosystems, such as RSA and Elliptic Curve Cryptography (ECC), are based on mathematical problems, such as integer factorization and discrete logarithms, which quantum algorithms, in particular Shor's algorithm, can solve in a time proportional to the ciphertext length. According to the recent industry indications, this so-called Q-Day, at which the quantum computers will be able to break the current standards, may happen within the next three to five years, which will be an imminent systemic risk to the digital infrastructures of countries [Hoque et al., 2024]. Three main pillars of quantum secure defense to deal with these vulnerabilities, researchers are concentrating on three key pillars of quantum-secure defense: Post-Quantum Cryptography (PQC): These are mathematical algorithms, including lattice-based, code-based, and hash-based algorithms, designed to be quantum-secure and resistant to both classical and quantum attacks. NIST is now on the forefront of global standardization of PQC, with candidate primary standards such as CRYSTALS-Kyber and CRYSTALS-Dilithium [Oliva del Moral et al., 2024].

Corresponding Author: Vishal Kumar, Galgotias University, Greater Noida, India
Email: vishuv3466@gmail.com

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52046

Quantum Key Distribution (QKD): In contrast to PQC, which is based on mathematical complexity, QKD uses the laws of quantum physics to achieve unconditionally secure exchange of keys. By incorporating QKD into the enabling Software-Defined Networking (SDN) architectures, 6G networks will be able to provide long-term security to important backbone infrastructure [Hoque et al., 2024]. Blockchain Technology: Blockchain provides decentralized trust and unalterable ledger. However, its current dependence on classical signatures makes it extremely vulnerable. In more modern constructions, a blockchain whose structure resists quantum attacks is proposed, using PQC compatible structures, such as lattice-based signatures and PQC-compatible Merkle trees, to secure transactions and identity [Oliva del Moral et al., 2024]. This is critical in ensuring that low-cost IoT devices can be acquired at low costs and which in most cases has a drastic energy and memory limitation. Studies have shown that it is possible to deploy advanced PQC-signatures, including Dilithium-5, on low-power microcontrollers, which can provide a scalable roadmap towards securing decentralized IoT ecosystems. It reviews the present state of affairs in these domains, and discusses the practical trade-offs among security, energy consumption, and network performance in the 6G era [Mahdi & Abdullah, 2025]. In order to tackle these challenges, Post-Quantum Cryptography (PQC) was introduced as a potential solution to create cryptographic schemes that are quantum-resistant. Compared to quantum key distribution (QKD), that requires a special quantum communication infrastructure, PQC algorithms can be implemented on the existing hardware and software systems and hence can be easily put into practice and widely adopted in the future [Shim et al., 2024; Garms et al., 2024; Liu & Moody, 2024]. The National Institute of Standards and Technology (NIST) recently has moved to increased standardization of quantum resistant algorithms, with CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, and SPHINCS+ being chosen as the most promising candidates for future quantum-resistant cryptographic systems [Xie et al., 2024; Aydeger et al., 2024; Hekkala et al., 2023]. The recent interest in PQC has stimulated a considerable amount of research in various application areas. The complexity of implementing PQC algorithms in resource limited embedded systems has been studied in several works, where computational load, memory usage and energy efficiency have been reported as obstacles [Alnaseri et al., 2025; Xie et al., 2024]. Some researchers have considered how PQC can be combined with newly developed technologies like IoT, mobile communication networks, blockchain systems and cloud computing infrastructures to ensure security for future use [Sanon & Schotten, 2025; Garms et al., 2024; Hekkala et al., 2023]. In addition, hybrid solutions of PQC and Quantum Key Distribution (QKD) have been proposed to further strengthen cryptographic resilience and offer further protection from future threats [Shim et al., 2024; Garms et al., 2024; Deshpande et al., 2024]. Recent studies also have highlighted the need to move from classical cryptography to quantum-safe cryptography. However, the so-called “Harvest Now, Decrypt Later” (HNDL) attacks have emerged as a concern as they could be conducted today with the hope of decrypting encrypted information once (in the future) quantum computers are powerful enough [Sanon & Schotten, 2025; Aydeger et al., 2024; Liu & Moody, 2024]. In response, the research and industry communities have been interested in migration frameworks, deployment strategies, measurement of adoption, and risk assessment methodologies to transition to a quantum-resilient cybersecurity infrastructure [Sowa et al., 2024; Shakil et al., 2024; Aydeger et al., 2024]. Although huge progress has been made, there are still a number of issues to be addressed. Traditionally, the PQC algorithms need a bigger key size, more computation power and harder to implement architectures than classic crypto graphic algorithms [Alnaseri et al., 2025; Xie et al., 2024; Borges et al., 2020]. Furthermore, interoperability, standardization, implementation and large-scale deployment issues remain barriers to broadscale deployment [Sowa et al., 2024; Aydeger et al., 2024; Hekkala et al., 2023]. It is thus crucial to conduct a backward glance to see how things have been evolving in the recent past, where the gaps in research were found and what steps are required in the future to make quantum-safe communication systems a reality. The present paper aims to conduct a systematic literature review of post quantum cryptography, focusing on its applications in the fields of 6G networks, Internet of Things (IoT), Blockchain Systems and embedded systems. The review covers recent research advances, reviews against the current PQC approaches, discusses challenges in implementation, and outlines future directions in quantum resilient cybersecurity. Furthermore, the paper highlights research gaps and opportunities for building secure and scalable post-quantum infrastructures for next generation digital ecosystems.

Corresponding Author: Vishal Kumar, Galgotias University
Email: vishuv3466@gmail.com

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52046

2. Literature Overview

2.1. Research Status on PQC

In recent years, quantum computation has been an area where research has been ongoing in the field of Post Quantum Cryptography (PQC) in various fields such as Internet of Things (IoT), blockchain systems, intelligent transportation systems (ITS), unmanned aerial vehicles (UAVs), cloud computing, and next generation communication networks. The security solutions that are now required, particularly in the context of large-scale quantum computers, can help break the public-key security algorithms that are widely used including RSA, ECC and Diffie–Hellman [Sanon & Schotten, 2025; Aydeger et al., 2024; Liu & Moody, 2024]. PQC has proven to be an essential technology for the intelligent transportation systems to safeguard Vehicle-to Everything (V2X) communications. They rely on the ability to exchange data reliably and securely between vehicles, roadside infrastructure, and cloud services, which can facilitate traffic flow and enhance road safety. The use of PQC is crucial for the long-term security of transportation data, as it could be vulnerable to quantum attacks against traditional cryptographic methods [Al Mamun et al., 2026]. Likewise, the growing number of IoT ecosystems has brought with it considerable security concerns because of the limited resources of many of these connected devices. Traditional public-key cryptographic schemes are susceptible to quantum attacks and can be quite expensive in terms of processing power, so lightweight PQC schemes that are efficient in memory, energy, and processing under stringent constraints have been studied recently [Mahdi & Abdullah, 2025; Alnaseri et al., 2025]. These activities are especially important in the context of smart healthcare, smart city infrastructures and industrial automation. The use of PQC in communication networks is also a strong research focus. There have been several works that explored the deployment of quantum-resistant cryptographic mechanisms for Transport Layer Security (TLS) [Chang & Khan, 2026] and web security protocols [Sanon & Schotten, 2025] as well as for new 5G/6G communication architectures. Lattice-based schemes like ML KEM(Kyber) and ML-DSA(Dilithium) also show promising security and performance properties, but some issues with key size, computational burden, and integration with the existing infrastructure still remain. The use of PQC in UAV systems has another line of research since secure wireless communication is critical for mission-critical operations. UAVs are especially susceptible to cyber-attacks because of their onboard limited computational resources and the openness of the communication channels. Quantum-resistant cryptographic mechanisms can increase the degree of confidentiality, integrity, and authenticity of the information transmitted, which will provide security for the information transmitted for the purposes of surveillance, military, and disaster response. [Oliva del Moral et al., 2024] Blockchain technology is yet another crucial sector of application for PQC. Blockchains have been heavily relying on classical public-key cryptography for authenticating transactions and achieving consensus. The arrival of non-imaginary quantum computers could throw this foundation of security into disarray, allowing for the creation of forged transactions and unauthorized access to digital assets. To achieve long term security and trustworthiness in decentralized systems, researchers have suggested multiple PQC-based blockchain frameworks [Wang & Ismail, 2025]. In addition to specific application areas, researchers have also studied the general deployment issues related to PQC adoption. These encompass performance overhead, optimization of hardware, interfacing with legacy systems, migration planning and standardization requirements [Alnaseri et al., 2025; Sowa et al., 2024; Aydeger et al., 2024]. The increasing number of publications has shown that PQC has become a research field of action from theory to reality and has become essential for the protection of future digital infrastructures against new quantum threats [Liu & Moody, 2024]. In summary, the state of the art shows that in the field of Post-Quantum Cryptography, this theoretical concept has turned into a practical cybersecurity solution for the protection of future digital infrastructures from the threats of quantum computers. There is great development in algorithm design, standardization, optimization and implementation in application-specific fields. The continued standardization activities of NIST and the growing number of uses in the real-world deployment studies also suggest the rising maturity of PQC technologies. However, issues of computational burden, key and signature size, interoperability with current systems and large-scale deployment are still under investigation. Therefore, continued research is needed to realize efficient, scalable and secure solutions for quantum-resistant

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52046

cryptography which can fulfill the long-term security needs of next generation of communication networks, cloud platforms, IoT systems and critical infrastructures [NIST, 2024; Alnaseri et al., 2025; Liu & Moody, 2024].

3. Theoretical Basis of PQC

The security of Post-Quantum Cryptography (PQC) is based on mathematical challenges that are believed to be intractable for classical and quantum computers. Contrary to public-key cryptography, which utilizes integer factorization and discrete logarithm problems, PQC will rely on other hard problems such as lattices, codes, hashes, multivariate polynomials and isogenies. The mathematics on which these quantum-resistant algorithms rely is the basis of current NIST standardization efforts and is integral to modern cryptographic algorithms. CRYSTALS-Kyber and CRYSTALS Dilithium are the chosen PQC algorithms, and lattice-based cryptography has become the most promising among the many candidates mentioned above, because it has improved security guarantees and is efficient to implement [Alnaseri et al., 2025; Xie et al., 2024; Liu & Moody, 2024]. As shown in Figure 1, post-quantum cryptography comprises lattice-based, code-based, hash-based, multivariate, isogeny-based, and hybrid cryptographic approaches.

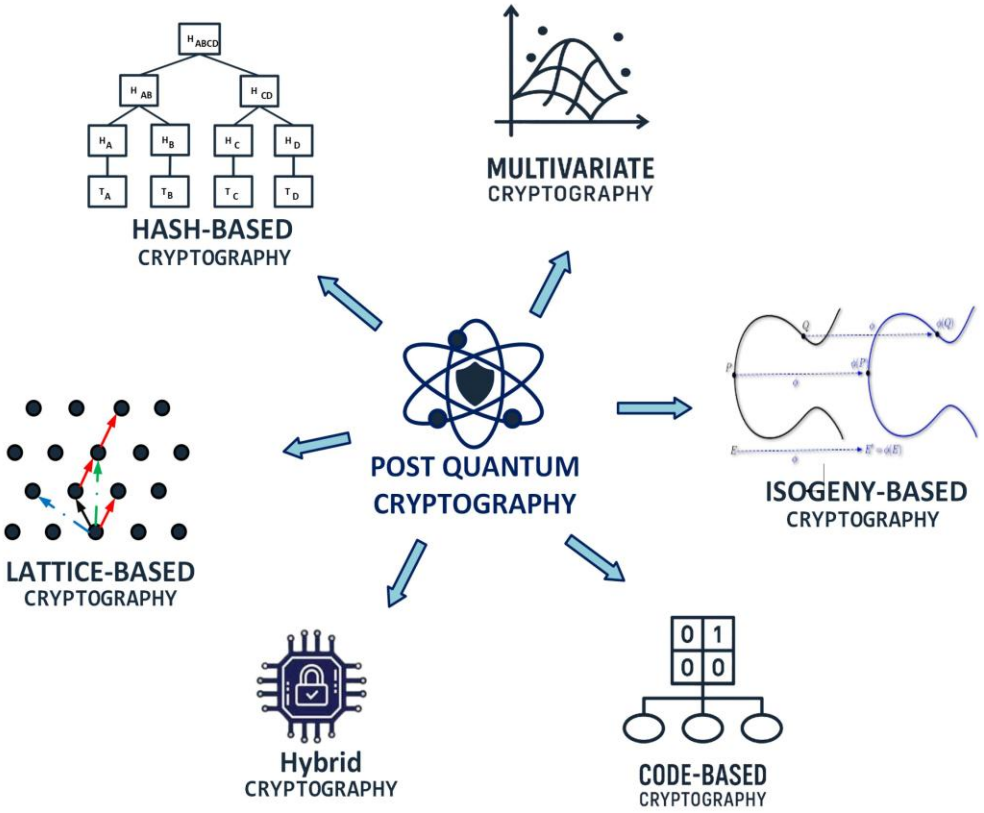

Fig. 1. Post-Quantum Cryptography Ecosystem

3.1.1. Lattice-based cryptography:

Lattice-based cryptography is the most studied and promising method for general purpose PQC; a result of this was that it dominated the NIST standardization process. The security is normally based on the hardness of finding short vectors in a high-dimensional lattice, and it is the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). Most modern lattice-based schemes are based on the Learning With Errors (LWE) problem, which was introduced by Oded Regev in 2005. Now, the LWE problem is of the recovery of a secret vector. $s \in Z_q^n$ From a series of approximate random linear equations. The LWE distribution $A_{s,x}$ is generated by random selection of a vector A from a distribution x over Z_q for some $s \geq 2$ (dimension) and $q \geq 2$ (modulus). $a \in Z_q^n$ At random uniformly and an error term $e \in Z_q$ according to x . The output is the tuple (a, b) where:

$$b = \langle a, s \rangle + e(mod q) \quad (1)$$

For most cryptographic uses, x is a normal distribution with standard deviation αq rounded to the nearest integers and reduced modulo q with standard deviation α usually of the order of 10^{-30}, or less. $\frac{1}{\text{poly}(n)}$. The hardness of LWE is guaranteed by a reduction to a worst-case lattice problem like the decision version of the Shortest Vector Problem (SVP), and the Shortest Independent Vectors Problem (SIVP). For better efficiency, structured lattices are employed which results in extensions like Ring-LWE and Module-LWE (M-LWE). These are variants where operations are performed in a polynomial ring:

$$Rq = Zq[x]/(xn + 1) \quad (2)$$

Here n is usually taken to be a power of 2, to ensure that the polynomial $x_n + 1$ is not easily factored into rational numbers.

Both these structured methods enable significantly smaller key sizes and faster calculations with the help of the Number Theoretic Transform (NTT), a technique that speeds up polynomial multiplication and enhances overall cryptographic efficiency. Importance of lattice-based cryptography can be seen in the standardization process by NIST, such as algorithms are chosen as standards: CRYSTALS-Kyber for key encapsulation, and CRYSTALS-Dilithium for digital signatures. The algorithms use polynomial arithmetic and Number Theoretic Transform (NTT) to perform efficient encryption and decryption as well as signature generation operations [Alnaseri et al., 2025; Xie et al., 2024; Liu & Moody, 2024].

3.1.2. Hash-Based Cryptography:

Hash-based cryptography is a well-established approach that relies on the security of cryptographic hash functions to generate digital sig natures. Unlike other cryptographic methods, its security does not depend on complex mathematical structures but instead on the fundamental properties of hash functions, such as collision resistance and preimage resistance [Opiłka et al., 2024]. This makes hash-based cryptography highly secure and resistant to quantum attacks. One of the most widely recognized hash-based signature schemes is SPHINCS+, which has been selected as a candidate in the NIST standardization process. SPHINCS+ provides strong security guarantees without re lying on structured mathematical assumptions, making it a reliable option for long-term data protection [Wang & Ismail, 2025]. However, a major drawback of hash-based cryptography is its large signature size and relatively slower performance compared to other PQC approaches. Despite these limitations, it remains an important and dependable method for ensuring secure digital signatures in quantum-resistant systems.

3.1.3. Code-Based Cryptography:

Code-based cryptography is based on the computational difficulty of decoding random linear error-correcting codes, a problem that has been studied for several decades and is still considered secure against both classical and quantum attacks [Oliva del Moral et al., 2024]. This long-standing security makes it one of the most trusted approaches in Post Quantum Cryptography. A well-known example of a code-based cryptographic scheme is Classic McEliece, which has demonstrated strong resistance to various cryptographic attacks. Due to its proven reliability and robustness, it is considered a strong candidate for quantum-resistant encryption systems [Ricci et al., 2024]. However, one of the major challenges associated with code-based cryptography is its extremely large public key size, which can create issues in storage and communication efficiency. Despite this limitation, its high level of security makes it suitable for applications where security is more critical than performance, such as military and high-security communication systems. A code-based approach to cryptography is based on the intractability of the problem of decoding a random linear code, which is known to be NP-hard in general [Hoque et al., 2024]. The McEliece cryptosystem, which was first introduced in 1978, is one of the most popular candidates for Post-Quantum Cryptography (PQC) as it has been very resistant to both classical and quantum cryptanalysis over the years [Al Mamun et al., 2026]. The difficulty in this family is the Syndrome Decoding Problem (SDP) [Opiłka et al., 2024]. Let n, k, w be integers such that $k \leq n$ and w ≤ n. An instance of the problem $SD(n, k, w)$ is a parity-check matrix $H(n, k, w)$.

$$H = F_2^{(n-k)\cdot n}$$

and a vector

$$s \in F_2^{n-k}$$

called the syndrome.
A solution is a vector

$$e \in F_2^n$$

Let $wt(e) \leq w$ be the Hamming distance of e for which:

$$He^\top = s^\top \quad (3)$$

This is an equation that is still exponential in the size of the error vector w. In general, random linear codes are the most difficult to solve when the code rate

$$R = \frac{k}{n}$$

The value of is about 0.5 and the value of w is slightly larger than the $Gilbert - Varshamov\ bound\ d_{GV}$. Let C be a binary code, the Gilbert-Varshamov distance d_{GV} is the smallest integer d such that:

$$\sum_{j=0}^{d-1} n_j \geq 2^{n-k} \quad (4)$$

Structured codes are commonly employed in crypto graphic applications in order to attain reasonably sized key lengths. For instance, Classic McEliece is based on binary Goppa codes, and the more recent codes include Quasi Cyclic Moderate Density Parity-Check (QC-MDPC) codes and Hamming Quasi-Cyclic codes. These structured methods then enable legitimate users to decode efficiently with a private trapdoor, whilst the public code looks random to an outside observer, thus keeping cryptographic security.

4. Current Implementation Status

4.1. Public Key Encryption

3.1.1. CRYSTALS-kyber:

The National Institute of Standards and Technology (NIST) has chosen CRYSTALS-Kyber as one of the lattice-based Key Encapsulation Mechanisms (KEM) of the standards project for post-quantum public key encryption (PQKE). It is based on the hardness of some lattice problems, such as the Learning With Errors (LWE) problem, which is believed to be hard against both classical and quantum attacks [Hasan et al., 2024]. With its emphasis on security and performance, Kyber is poised to become a valuable asset in modern communication systems, offering robust protection and efficient performance. The major advantage of Kyber is its efficient computation and high level of security. Kyber is also less susceptible to the computational overhead typically incurred by standard cryptographic schemes like RSA, providing faster key generation, encryption and decryption times in numerous contexts [Al Mamun et al., 2026]. Moreover, it has relatively small key sizes as compared to other PQC schemes, making it more convenient for use in resource-limited settings. This makes Kyber a top contender for future communication systems in the post quantum world.

3.1.2. BIKE:

BIKE (Bit Flipping Key Encapsulation) is one of the code-based Post-Quantum Cryptography (PQC) algorithms that offers efficient and secure encryption mechanisms. Built on the hardness of decoding random linear codes that are believed to be quantum adversarial resistant as well as classical adversarial resistant [Hasan et al., 2024)]. As a result of its solid security foundation and practical performance properties, BIKE is suggested as a candidate in the NIST post-quantum standardization procedure. The relatively smaller key size is one of the important merits of the BIKE, as it is more appropriate for practical use in communication systems than other code-based schemes like classic McEliece [Al Mamun et al., 2026]. Also, BIKE is developed to accomplish effective key generation and encryption processes. But despite all these advantages, it still needs to be optimized in terms of performance and efficiency of implementation particularly in environments with limited resources. Current efforts are directed towards enhancing its computational efficiency and minimizing overhead to better enable its use in practical applications.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52046

3.1.3. Classic McEliece:

One of the earliest and best established Post-Quantum Cryptography (PQC) algorithms, Classic McEliece was proposed in 1978. It is based on the code-based cryptography and the hardness of decoding random linear error-correcting codes, which is known to be secure against classical and quantum attacks during last 10 years [Hasan et al., 2024]. Classic McEliece is one of the most secure PQC schemes for use today, because it has a long history of use and it is known to be resistant to the many cryptographic attacks. A significant benefit of Classic McEliece is its high level of security and proven robustness making it appropriate for applications that call for long term data protection [Al Mamun et al., 2026]. One major limitation to this algorithm is the sheer size of the public key, which could make it difficult to store and transmit or to implement in a practical way. However, it is a promising choice for secure communication networks in the post-quantum era due to its robust security features.

3.1.4. HQC (Hamming Quasi-Cyclic):

A code-based Post Quantum Cryptography (PQC) scheme, currently being assessed by NIST, is called HQC (Hamming Quasi-Cyclic). Based on the hardness of decoding random linear codes, especially quasi-cyclic (QC) linear codes that can be made efficient and still provide excellent security against classical and quantum attacks [Hasan et al., 2024]. HQC is a Key Encapsulation Mechanism (KEM), which is designed to deliver secure key exchange in post-quantum communication systems. One of the key strengths of HQC is its ability to achieve a balance between security and performance. The key size in HQC is relatively small as compared to traditional code-based schemes like Classic McEliece, and it is also more practical for implementation in modern communication network [Al Mamun et al., 2026]. Further, HQC is resilient to several attack models, providing an extra level of assurance. But like other PQC algorithms, it has yet to be optimized for widespread use. Current studies are directed towards making it more efficient and reducing the computation load to make it more viable to be used in real life.

3.2. Digital Signature Schemes

Digital signature schemes are being widely used in digital communication systems to provide authentication, data integrity and non-repudiation. From a Post Quantum Cryptography (PQC) point of view, these schemes are security schemes that are guaranteed to be secure against classical and quantum attacks. Classical digital signature schemes like RSA and ECDSA can be attacked by quantum algorithms such as Shor's that are capable of compromising the under lying mathematical issues [Hasan et al., 2024]. To overcome the above limitation, a number of digital signature schemes based on PQC have been developed based on different mathematical basis other than lattices and hash functions. Examples of notable ones include CRYSTALS Dilithium, Falcon, and SPHINCS+, which are in the NIST standardization process [Al Mamun et al., 2026]. The primary goal of these schemes is to strike the balance between security, efficiency, and simplicity while also tackling the challenges posed by quantum computing. With the advent of research, PQC-based digital signatures will become an alternative to classical-based digital signatures for future communication systems.

3.2.1. Crystal- DIlithium:

CRYSTALS-Dilithium is a lattice-based digital signature scheme that was chosen by the National Institute of Standards and Technology (NIST) to be standardized in the future. It is based on the hardness of lattice problems, especially the Learning With Errors (LWE) and Module-LWE problems, which are believed to be quantumly secure [Opiłka et al., 2024]. The aim of the Dilithium is to offer robust security without sacrificing performance, allowing it to be used in practical applications like secure communication and authentication systems. The efficient key generation, signing, and verification are one of the major benefits of the Dilithium. The performance analysis reveals that it has a reasonable computational efficiency and security and can be applied to various systems [Wang & Ismail, 2025]. Also, it provides moderate key and signature size, compared to other PQC schemes. CRYSTALS-Dilithium is considered one of the best candidates for future digital signature standards in the post-quantum era, thanks to its reliability and efficiency.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52046

3.2.2. SPHINICS+:

SPHINCS+ is a stateless hash-based variant of the digital signature scheme, based on the security of cryptographic hash functions and not on complex mathematical structures. It is also very secure and is secure based on properties which are well known like collision resistance and preimage resistance [Oliva del Moral et al., 2024]. Unlike stateful hash-based schemes, SPHINCS+ does not need to store any state information, making the implementation much easier as well as decreasing the chance of misuse. A major benefit of SPHINCS+ is that it guarantees high level security and does not rely on any structured assumption, guaranteeing a reliable option for long-term data protection [Ricci et al., 2024]. However, it is not without its drawbacks such as fairly large signatures and slower performance than lattice-based schemes. However, because of these disadvantages, SPHINCS+ is still an important PQC solution because of its robustness and simplicity, particularly when security is more important than performance.

3.2.3. Falcon:

Falcon is a digital signature scheme based on lattices which uses small signatures and is very efficient, ideal for applications such as those with limited bandwidth or storage. It is based on the NTRU lattice problem which is believed to be quantum and classical secure [Chang & Khan, 2026]. Falcon has been selected as one of the candidates in the NIST post quantum standardization process due to its strong performance characteristics. The smaller signatures sizes that Falcon can produce than other PQC schemes allows for more efficient communication and less storage space, which is one of its main benefits [Wang & Ismail, 2025]. Additionally, it provides fast verification and competitive performance. But, because of the complexity of the mathematical structure and the need for floating-point computations, Falcon is subject to potential vulnerability if not implemented correctly [Chang & Khan, 2026]. However, Falcon is a promising option for efficient and secure digital signatures in the post-quantum world, overcoming these obstacles.

4. Comparative Analysis of Reviewed Studies:

A comparative analysis of the studies reviewed is presented in terms of the main research domain, the application domain, main contributions, and limitations. The comparison illustrates the disparity in the ongoing research in Post Quantum Cryptography and also shows some of the areas where practical deployment, computational efficiency and wide-scale adoption of the new technologies come with some challenges. The analysis also points to the growing need for quantum safe and standardized cryptographic solutions in securing future digital infrastructures.

Table 1. Comparative Analysis of Reviewed Studies

References	Research Focus	Application Domain	Major Contribution	Limitation
Hoque et al. (2024)	PQC+QKD Integration	6G Networks	Hybrid quantum-safe architecture	Deployment complexity
Al Mamun et al. (2026)	PQC for ITS	Intelligent Transportation Systems	Secure V2X communication	Performance overhead
Opiłka et al. (2024)	PQC Digital Signatures	General Security Systems	Signature performance analysis	Large signature sizes
Wang and Ismail (2025)	PQC in Blockchain and IoT	Blockchain, IoT	Comprehensive application review	Limited deployment studies
Oliva del Moral et al. (2024)	PQC for Critical Infrastructure	Industrial Systems	Quantum-resilient	High implementation cost

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52046

			cybersecurity framework	
Ricci et al. (2024)	Hybrid Cryptography	Secure Communications	Classical-PQC-QKD integration	Interoperability issues
Chang and Khan (2026)	PQC Networking Protocols	Communication Networks	Migration strategies for networking systems	Standardization challenges
Demir et al. (2025)	Industry Deployment Analysis	Enterprise Systems	Real-world implementation assessment	Limited industrial adoption
Mahdi and Abdullah (2025)	PQC for IoT Devices	IoT	Lightweight security solutions	Resource constraints
Hasan et al. (2024)	Migration Framework	Enterprise Security	Security dependency analysis	Complexity of migration
Alnaseri et al. (2025)	Embedded PQC Optimization	Embedded Systems	Hardware optimization techniques	Memory overhead
Shim et al. (2024)	PQC-QKD Protocols	Web Security	Secure key exchange mechanisms	Infrastructure requirements
Sanon and Schotten (2025)	PQC in Mobile Networks	5G/6G Networks	Quantum-secure communication framework	Performance trade-offs
Sowa et al. (2024)	PQC Adoption Measurement	Network Infrastructure	Migration pathway analysis	Early deployment stage
Garms et al. (2024)	Hybrid Quantum-Safe Systems	Communication Networks	Experimental hybrid architecture	Scalability concerns
Xie et al. (2024)	PQC Hardware Design	Hardware Security	Efficient circuit implementation	Hardware complexity
Shakil et al. (2024)	AI-Assisted PQC Migration	Cybersecurity Analytics	Quantum vulnerability assessment	Limited datasets
Deshpande et al. (2024)	Classical vs PQC Comparison	Secure Communication	Security-performance evaluation	Computational cost
Borges et al. (2020)	PQC Key Agreement	Cryptographic Protocols	Security-performance comparison	Large key sizes
Aydeger et al. (2024)	PQC Transition Strategies	Enterprise Security	Migration framework development	Adoption barriers
Hekkala et al. (2023)	PQC Development Practices	Software Engineering	Practical implementation guidance	Limited large-scale validation
Liu and Moody (2024)	Future of PQC	Cybersecurity	Comprehensive PQC overview	Generalized discussion

Comparing the two reveals that the lattice-based cryptography is the preferred approach of the current research in PQC due to its secure certifications, low computation and successful NIST standardization. The focus of most of the studies is on the implementation difficulties in resource constrained environments like IoT devices, embedded systems and next-generation communication networks. Moreover, hybrid quantum-safe architectures that integrate PQC and QKD are also becoming a research hotspot to tackle long-term security. Although great

progress has been made, few studies have assessed PQC algorithms in large-scale operational environments. The majority of previous research works are centered on the theoretical analysis, simulation or prototype implementation. This is an indication that more deployment studies, performance benchmarking and interoperability testing is needed before this can be widely adopted in industry.

5. Research Gaps

While Post-Quantum Cryptography (PQC) has made great progress, there are still some challenges in the research community that have yet to be solved, hindering the broad adoption of PQC in real-world applications. Most existing literature is dedicated to algorithm design and the theoretical security analysis, and the deployment, optimization and interoperability aspects still need to be explored further. The main research gaps revealed by the studies reviewed are discussed below.

5.1. Optimization for Resource-Constrained Devices

The computational resources, memory and energy most NIST-standardized PQC algorithms demand is greater than existing cryptographic algorithms, especially lattice-based schemes like ML-KEM (Kyber) and ML-DSA (Dilithium). The requirements are very difficult to satisfy in resource poor environments such as IoT devices, wireless sensor networks, embedded systems, and edge computing systems. While some optimization methods have been suggested, some additional research efforts are needed to implement lightweight methods, develop hardware–software co-design methodologies and design energy-efficient architectures for low-power devices [Alnaseri et al., 2025; Xie et al., 2024].

5.2. Large Key and Signature Sizes

Compared to more traditional public-key cryptographic methods like RSA and ECC, many PQC algorithms can produce significantly larger public keys, ciphertexts and digital signatures. In code-based or hash-based cryptographic systems, for instance, the physical memory needed and the overhead in communication could be a challenge for systems with limited bandwidth. The key and signature length reduction as well as maintaining the same guarantees and computational efficiency is an interesting area for further research [Vidakovic & Milicevic, 2023; Deshpande et al., 2024; Borges et al., 2020].

5.3. Limited Large-Scale Deployment Studies

The majority of PQC research has been done theoretically, in simulations, in the laboratory or with a prototype system. Large-scale operational systems like cloud infrastructures, industrial systems, blockchain networks, IoT ecosystems and next generation communication networks are not well supported by comprehensive evaluations. Therefore, further real-world deployments should be conducted to evaluate scalability, reliability, interoperability and long-term performance in realistic deployments [Sanon & Schotten, 2025; Sowa et al., 2024; Aydeger et al., 2024].

5.4. Integration of PQC and Quantum Key Distribution

It has been recently shown that PQC can be used in combi nation with Quantum Key Distribution (QKD) to implement hybrid Quantum-safe communication architectures. The goal of such approaches is to take advantage of scalability of PQC and the information theoretic security of QKD. But, interoperability, standardization, deployment complexity and cost effectiveness issues are yet not completely addressed. More research is needed to establish standardized frameworks for the actual implementation of PQC and QKD technologies [Shim et al., 2024; Garms et al., 2024].

5.5. Migration and Interoperability Challenges

The shift from classical cryptographic systems to PQC based systems is extremely complex, both from an operational and technical perspective. Compatibility with legacy systems, cryptographic agility, risk management, and deployment planning are all critical areas that organizations need to tackle when dealing with legacy systems.

Some migration frameworks have been suggested, but there are currently no standardized migrations methodologies, automated migration tools, and interoperability testing mechanisms that can assist in large-scale cryptographic migrations in heterogeneous environments [Sowa et al., 2024; Aydeger et al., 2024; Hekkala et al., 2023].

5.6. Resistance to Hardware-Level Attacks

Most of the existing research into PQC focuses on algorithmic security with respect to classical and quantum attackers. Vulnerabilities at the level of implementation (side channel attacks, fault injection attacks, power analysis attacks, timing attacks, and electromagnetic leakage) have been given less attention so far. The construction of secure hardware architectures and the implementation of attacks is one of the key research areas to guarantee real-world security in practice [Alnaseri et al., 2025; Garms et al., 2024; Xie et al., 2024].

5.7. Standardization and Compliance Issues

NIST has completed the first round of PQC standards, but there are more algorithms and implementation recommendations being evaluated and refined. There could be barriers in the form of regulatory standards, security policies, and implementation, which can be different across industries and make it difficult to get everyone to follow suit. Further work is needed to develop standards, certification processes and compliance regimes for the easy deployment of PQC in various application areas, ideally on the global scale [NIST, 2024; Aydeger et al., 2024].

6. NIST PQC Standardization and Comparative Analysis

6.1. NIST Standardized PQC Algorithms

As practical quantum computers come into the world, global activity has been unfolding to standardize quantum resistance cryptographic algorithms. To solve this problem, in 2016 the National Institute of Standards and Technology (NIST) launched the Post-Quantum Cryptography (PQC) Standardization Project, whose goal is to find and standardize secure cryptographic algorithms that are resistant to both classical and quantum attacks [NIST, 2024; Liu & Moody, 2024]. Following several rounds of analysis, comparison and testing, NIST selected a number of algorithms for standardization. In August 2024, NIST formally released the first Federal Information Processing Standards (FIPS) for PQC, namely the ML-KEM (formerly CRYSTALS-Kyber) and the ML-DSA (formerly CRYSTALS-Dilithium) standards [NIST, 2024]. The standardization process is a major step in the evolution towards quantum secure cybersecurity infrastructures. Such algorithms offer reliable security assurances while being still efficient in practical usage on various platforms and architectures like cloud-based systems, enterprise networks, embedded systems, and future communication architectures [Alnaseri et al., 2025; Aydeger et al., 2024; Liu & Moody, 2024]. Although the benefits of PQC algorithms are significant, their public keys, ciphertext and signatures are typically larger than those in classical cryptographic schemes such as RSA or Elliptic Curve Cryptography (ECC). In the deployment phase, one may need more computational power, storage capacity and bandwidth [Vidakovic & Milicevic, 2023].

6.2. Comparative Analysis of Standardized PQC Algorithms

TABLE II
SIZE COMPARISON OF NIST POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS

Algorithm	**Security Level**	**Public Key (Bytes)**	Signature/ Ciphertext (Bytes)
ML-KEM-512	Level 1 (AES-128)	800	768

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52046

ML-KEM-1024	Level 5 (AES-256)	1568	1568
ML-DSA-44	Level 2 (SHA3-256)	1312	2420
ML-DSA-87	Level 5 (AES-256)	2592	4627
FN-DSA-512	Level 1 (AES-128)	897	666
SLH-DSA-128f	Level 1 (AES-128)	32	17088

Based on the comparison it is observed that lattice-based algorithms like ML-KEM and ML-DSA offer a good compromise between security, computational efficiency and communication overhead. While hash-based schemes provide robust security guarantees, their signature size is much larger and potentially leads to greater network delays and storage space usage in schemes with limited bandwidth capacity, such as in cellular networks and the Internet of Things [Vidakovic & Milicevic, 2023; Liu & Moody, 2024]. FN-DSA (Falcon) has much smaller size signatures than ML-DSA, which makes it promising for applications with strict communication requirements. But it is more complicated to implement because of the use of floating-point arithmetic and gaussian sampling methods [Opiłka et al., 2024; Chang & Khan, 2026].

6.3. Performance in Resource-Constrained IoT Environments

IoT devices and embedded systems pose further challenges because of their limited processing power, memory and energy capacity when deploying PQC algorithms. The feasibility of using standardized PQC algorithms in ARM Cortex-M0+ is gained by recent benchmarking studies [Chhetri, 2026].

TABLE III
IoT Benchmarks (ARM Cortex-M0+ @ 133 MHz)

Algorithm	Handshake/Full Cycle	RAM (KB)	Flash (KB)
ML-KEM-512	35.7 ms	12.1	5.1
ML-KEM-1024	85.7 ms	24.9	6.7
ML-DSA-44	~1,115 ms	55.5	8.9
ML-DSA-87	~1,125 ms	128.9	8.7

Source: Adapted from Chhetri (2026) and Alnaseri et al. (2025).

The result shows that the memory usage and the computational complexity of ML-KEM variants are relatively small, which means they can be used in lightweight applications of cryptography. ML-DSA, on the other hand, needs much more computation power and memory storage and may not be applicable in highly constrained environments [Chhetri, 2026]. Experimental results also show that ML-KEM-512 sows significantly lower energy consumption as compared to classical Elliptic Curve Diffie–Hellman (ECDH) implementations with equivalent security levels. The results pave the way to lattice-based PQC algorithms for future generation IoT and embedded platforms [Chhetri, 2026; Alnaseri et al., 2025].

6.4. Comparison of Digital Signature Schemes

The digital signature algorithms form part of a major factor of PQC infrastructures as they offer authentication, integrity and non-repudiation services. While NIST standardized, ML-DSA (Dilithium), FN-DSA (Falcon), and SLH DSA (SPHINCS+) are all signature schemes based on NIST standard designs, they exhibit different performance trade offs and design philosophies.

TABLE IV
Comparison of ML-DSA (Dilithium) and FN-DSA (Falcon) on Microcontrollers

Feature	ML-DSA (Dilithium)	FN-DSA (Falcon)

Verification Speed	Good	Excellent (0.5M vs 2.7M cycles)
Key Generation	Excellent	Poor (171M cycles)
Implementation	Simple (Uniform Sampling)	Complex (64-bit Gaussian)
Signature Size	Moderate	Compact (2.3× smaller)

Source: Adapted from Vidaković and Miličević (2023) and related PQC benchmarking studies.

Table IV shows performance characteristics of ML-DSA (Dilithium) and FN-DSA (Falcon) for microcontroller-based platforms. The key generation is efficient, implementation is simpler and Dilithium has been chosen for use in resource-constrained environments.

It is an easier-to-implement solution that provides strong security assurances, making it applicable to a broad range of applications, including those found in ML-DSA. On the other hand, FN-DSA has smaller signature size and better verification speed, but it has more complex implementation methods. Consequently, the selection between such schemes is application-based and depends on the application-specific security, storage, computational efficiency and deployment complexity requirements [Opiłka et al., 2024; Chang & Khan, 2026; Chhetri, 2026]. Moreover, SLH-DSA has a different design method that uses hash-based cryptography, with excellent security assurances without structured mathematical assumptions. It is considered very resilient against both classical and quantum attacks, although its signature sizes are significantly bigger as compared to those of ML-DSA and FN-DSA. The comparative evaluation shows that none of the digital signature schemes is ideal in every context. Limited storage, limited bandwidth applications may choose FN-DSA, while systems which focus on better implementation simplicity and balanced performance may choose ML-DSA. While the communication overhead is higher, SLH-DSA is still a good candidate for long-term security-critical applications [Opiłka et al., 2024; Vidakovic & Milicevic, 2023].

6.5. Discussion

Comparative analysis shows that the most practical way for the deployment of PQC in the large-scale is the lattice based cryptographic schemes. Because of their selection by NIST, good performance, and excellent security guarantees, they have emerged as favorite contenders for future crypto graphic infrastructures [Alnaseri et al., 2025; Xie et al., 2024; Liu & Moody, 2024]. However, issues of memory usage, complexity of computation, limitations on interoperability and complexity of deployment are still major issues. Further study and optimization of algorithms, hardware acceleration, lightweight implementations, and standardized migration solutions will be crucial to ensure smooth adoption of PQC within the future of communication systems, cloud infrastructures, and IoT ecosystems [Sanon & Schotten, 2025; Aydeger et al., 2024].

7. Discussion and Future Work

Post-Quantum Cryptography (PQC) has many technical and practical challenges that need to be resolved before it can be deployed at scale. Despite PQC algorithms being constructed to be secure against quantum attacks, real life implementation of these algorithms brings forth new complexities previously unseen in traditional cryptographic systems.

7.1. Key Challenges

The huge key and signature sizes of many algorithms is one of the main challenges of PQC. PQC schemes may demand much larger keys, which may in turn raise storage costs and communication overhead compared to classical cryptographic schemes (such as RSA and ECC) [Hasan et al., 2024]. This is of great concern in a system with low bandwidth or memory. Another important issue is the high computational overhead. PQC algorithms: PQC algorithms are more complex and involve more mathematical operations, which demand more processing power. This may cause a higher latency and low system performance, particularly in real-time applications like communication networks and embedded systems [Al Mamun et al., 2026]. The other challenge that is critical is the integration with the legacy systems. The majority of the current digital infrastructures are designed with the

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52046

help of classical cryptographic algorithms, and the replacement of these algorithms with PQC is not possible in the short term. Hence, compatibility and interoperability between the classical and post-quantum systems should be guaranteed in the transition stage [Opiłka et al., 2024]. Another problem is that the actual data of real-life deployment of PQC is lacking. Although a number of algorithms have been tested in controlled environments, their performance, reliability and security in large-scale real-world applications is however still not fully comprehended. This poses a challenge to organizations that intend to implement PQC technologies [Wang & Ismail, 2025]. In industrial environments, the implementation of PQC must be carefully balanced between security and performance, especially in resource-limited systems, such as IoT devices and industrial control systems [Oliva del Moral et al., 2024].

7.2. Research Gaps and Open Challenges

However, there are some areas that require further research and development; they are identified as research gaps and open challenges. While there have been great strides made in PQC, there are still a number of research gaps that need to be resolved. The high key and signature sizes of many PQC algorithms are one of the main difficulties, as they lead to higher communication costs and storage demands in resource-limited settings like IoT devices and embedded systems. Another challenge is related to computational complexity. However, many PQC schemes demand more processing power and memory usage than classical cryptographic methods, so it is hard to implement them in low-power devices. Moreover, interoperability with the legacy cryptographic infrastructure is still a significant problem in the migration stage from classical cryptography to PQC. Efficient hybrid cryptographic frameworks and light implementations are still on the research horizon. In addition, there are not many real-world deployment data points, and hardware optimization is still a bit lacking. The development of lightweight PQC solutions, hardware acceleration and scalable deployment strategies to support next generation communication systems is thus of great interest for future research.

7.3. Hybrid Cryptography

Hybrid cryptography as shown in figure 2 has become a viable approach to overcome the issues related to the transition to PQC. It consists of integrating classical cryptographic algorithms with post-quantum algorithms in order to offer higher security and at the same time be compatible with existing systems. This is so that in the event of a break into one cryptographic scheme, the entire system will be safe as there is another scheme. Hybrid cryptographic models are especially applicable when transitioning to a quantum-resistant cryptographic model, in such a way that existing operations are not disrupted [Opiłka et al., 2024]. Recent studies have revealed that hybrid cryptography can enhance security as well as be flexible in deployment. It enables systems to be backwards compatible and gradually add PQC algorithms to existing protocols like TLS and secure communication models [Ricci et al., 2024].

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52046

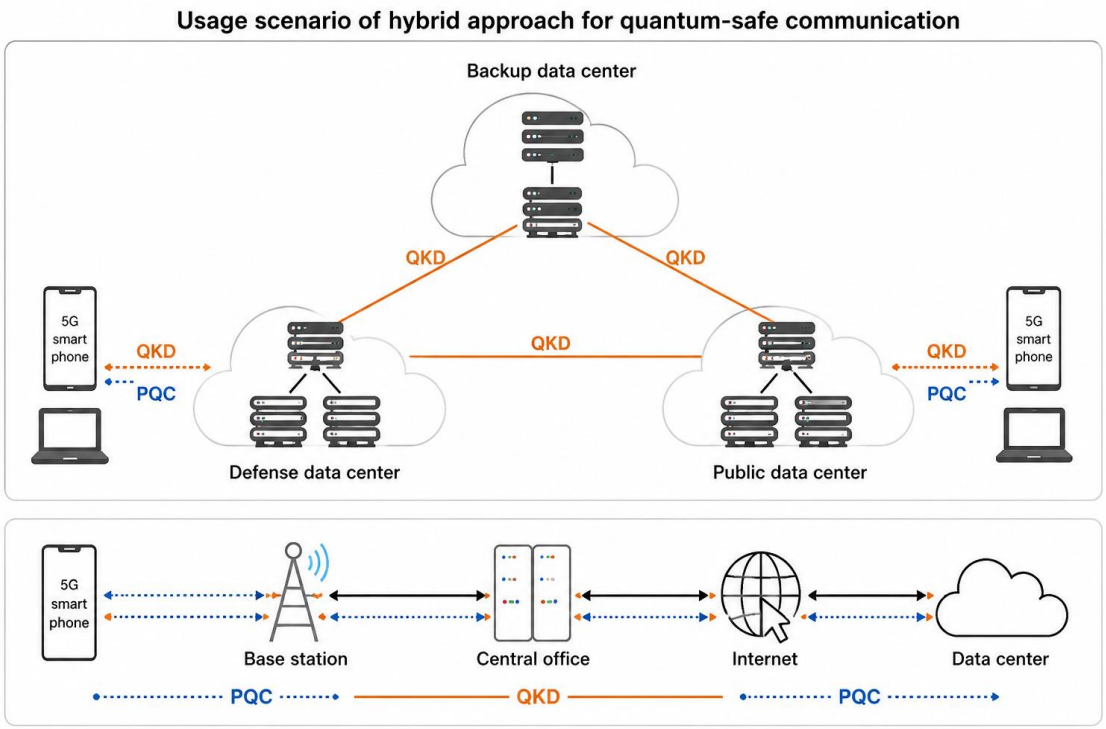

Fig. 2. Hybrid approach for quantum-safe communication.

7.4 Future Directions

To enable these algorithms to be applicable in real-world applications, future research in PQC must aim at enhancing efficiency and lowering computational overhead to make them applicable in real-world applications. It is paramount to develop optimized implementations that need less processing power and memory to be used widely [Al Mamun et al., 2026]. Another valuable field of research is hardware acceleration. Specialized hardware, including GPUs, FPGAs, and dedicated cryptographic processors can greatly enhance the performance of PQC algorithms and make them more practical to implement in high-speed systems [Hasan et al., 2024]. The global and standardization is also the key to the success of PQC. Other organizations like NIST are busy in standardizing PQC algorithms that will offer a common platform in secure communication across industries [Chang & Khan, 2026]. Lastly, secure migration models will need to be established and used to help organizations transition out of classical cryptography to PQC. Such frameworks ought to incorporate risk assessment, system evaluation, the strategies of phased implementation to facilitate a smooth and secure transition [Wang & Ismail, 2025]. Altogether, although PQC has a number of limitations, the current research and development efforts are likely to address these concerns and allow deploying secure and quantum-resistant systems in the nearest future.

8. Conclusion

As quantum computers become increasingly powerful, Post-Quantum Cryptography (PQC) has risen to become one of the groundbreaking cybersecurity solutions to ensure the security of digital infrastructures. The current review was conducted to explore the recent developments of PQC, such as the theoretical underpinning, the key families of cryptographic functions, the status of the implementation, the standardization process, and its applications in the 6G network, IoT, blockchain and embedded systems. The studies reviewed indicate that there is a tradeoff between security and performance of the lattice-based and hash-based/coded-based schemes, and currently the lattice-based schemes are the most practically viable options with security guarantees in the quantum regime. The NIST standardization and prototypes in the field have made great strides, but computational burden, memory constraints, key size, interoperability and scalability issues are still not yet answered. In conclusion, PQC is not just a concept but a practical solution that is essential for maintaining cybersecurity in the future. Scalable

and resilient quantum-safe communication systems will only be possible if carried out in the context of the continued research into lightweight implementations, optimization of hardware, hybrid cryptographic architectures and secure migration strategies. With the development of quantum technologies, PQC is poised to serve as the backbone of more secure digital infrastructure in the future.

References

[1]. Al Mamun, A. A., Abrar, A., Rahman, M., Salek, M. S., & Chowdhury, M. (2026). *Post-quantum cryptography for intelligent transportation systems: An implementation-focused review*. *Vehicular Communications*.

[2]. Alnaseri, O., Himeur, Y., Atalla, S., & Mansoor, W. (2025, May). Complexity of post-quantum cryptography in embedded systems and its optimization strategies. In *2025 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 776–781). IEEE.

[3]. Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024, October). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In *2024 15th International Conference on Network of the Future (NoF)* (pp. 195–203). IEEE.

[4]. Borges, F., Reis, P. R., & Pereira, D. (2020). A comparison of security and its performance for key agreements in post-quantum cryptography. *IEEE Access, 8*, 142413–142422.

[5]. Chang, S.-Y., & Khan, Q. (2026). Post-quantum cryptography in networking protocols: Challenges, solutions, and future directions. *Cryptography, 10*(1), 12.

[6]. Chhetri, R. (2026). *Benchmarking NIST-standardized ML-KEM and ML-DSA on ARM Cortex-M0+: Performance, memory, and energy on the RP2040* (arXiv:2603.19340). arXiv.

[7]. Demir, E. D., Bilgin, B., & Onbasli, M. C. (2025). *Performance analysis and industry deployment of post-quantum cryptography algorithms* (arXiv:2503.12952). arXiv.

[8]. Deshpande, A., Nalwade, A., Gutte, V. S., & Patil, D. R. (2024, October). Journeying through securing digital communication: A comparative analysis from classical to post-quantum cryptography. In *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)* (pp. 1–7). IEEE.

[9]. Garms, L., Paraíso, T. K., Hanley, N., Khalid, A., Rafferty, C., Grant, J., ... & O'Neill, M. (2024). Experimental integration of quantum key distribution and post-quantum cryptography in a hybrid quantum-safe cryptosystem. *Advanced Quantum Technologies, 7*(4), 2300304.

[10]. Hasan, K. F., Simpson, L., Baee, M. A. R., Islam, C., Rahman, Z., Armstrong, W., Gauravaram, P., & McKague, M. (2024). A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies. *IEEE Access, 12*, 23427–23450.

[11]. Hekkala, J., Muurman, M., Halunen, K., & Vallivaara, V. (2023). Implementing post-quantum cryptography for developers. *SN Computer Science, 4*(4), 365.

[12]. Hoque, S., Aydeger, A., & Zeydan, E. (2024). Exploring post-quantum cryptography with quantum key distribution for sustainable mobile network architecture design. In *Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems*.

[13]. Liu, Y.-K., & Moody, D. (2024). Post-quantum cryptography and the quantum future of cybersecurity. *Physical Review Applied, 21*(4), 040501.

[14]. Mahdi, L. H., & Abdullah, A. A. (2025). Post-quantum cryptography for IoT devices. *IEEE Transactions on Industrial Informatics*.

[15]. National Institute of Standards and Technology. (2024). *Module lattice-based key-encapsulation mechanism standard (FIPS 203)*. U.S. Department of Commerce.

[16]. Oliva del Moral, J., de Marti i Olius, A., Vidal, G., Crespo, P. M., & Etxezarreta Martinez, J. (2024). Cybersecurity in critical infrastructures: A post-quantum cryptography perspective. *IEEE Internet of Things Journal*.

[17]. Opiłka, F., Niemiec, M., Gagliardi, M., & Kourtis, M. A. (2024). Performance analysis of post-quantum cryptography algorithms for digital signature. *Applied Sciences, 14*(12), 4994.

[18]. Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid keys in practice: Combining classical, quantum and post-quantum cryptography. *IEEE Access, 12*, 23206–23219.

[19]. Sanon, S. P., & Schotten, H. D. (2025). Securing mobile networks in the quantum era: Imperative role of post-quantum cryptography. In *2025 Joint European Conference on Networks and Communications and 6G Summit (EuCNC/6G Summit)*. IEEE.

[20]. Shakil, N. A. F., Ahmed, I., & Mia, R. (2024). Data science approaches to quantum vulnerability assessment and post-quantum cryptography schemes. *Sage Science Review of Applied Machine Learning, 7*, 144–161.

[21]. Shim, K.-S., Kim, B., & Lee, W. (2024). Research on quantum key, distribution key and post-quantum cryptography key applied protocols for data science and web security. *Journal of Web Engineering, 23*(6), 813–830.

[22]. Sowa, J., Hoang, B., Yeluru, A., Qie, S., Nikolich, A., Iyer, R., & Cao, P. (2024, September). Post-quantum cryptography (PQC) network instrument: Measuring PQC adoption rates and identifying migration pathways. In *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)* (Vol. 1, pp. 1835–1846). IEEE.

[23]. Vidaković, M., & Miličević, K. (2023). Performance and applicability of post-quantum digital signature algorithms in resource-constrained environments. *Algorithms, 16*(11), 518.

[24]. Wang, Y., & Ismail, E. S. (2025). A review on the advances, applications, and future prospects of post-quantum cryptography in blockchain and IoT. *IEEE Access, 13*.

[25]. Xie, J., Zhao, W., Lee, H., Roy, D. B., & Zhang, X. (2024). Hardware circuits and systems design for post-quantum cryptography—A tutorial brief. *IEEE Transactions on Circuits and Systems II: Express Briefs, 71*(3), 1670–1676.