Post-Quantum Cryptography: Current Developments, Challenges and Future Directions

Prageeth Fernando [1]

[1] *Sri Lanka Institute of Information Technology*
SLIIT Malabe Campus, New Kandy Road, Malabe, 10115, Sri Lanka

DOI: 10.22178/pos.119-4

LCC Subject Category: T1-995

Received 26.05.2025
Accepted 25.06.2025
Published online 30.06.2025

Corresponding Author:
prageethfndo@gmail.com

Abstract: Quantum computing poses a significant threat to existing cryptosystems, as Shor's and Grover's algorithms efficiently solve the underlying mathematical problems of classical cryptographic algorithms. Post-Quantum Cryptography (PQC) provides a proactive response to this emerging threat, enabling resilience against quantum attacks. Researchers have extensively explored various mathematical structures believed to be resilient against quantum attacks across several PQC families. The NIST PQC standardisation project demonstrates the global need to integrate PQC into existing digital systems, even before the quantum era. Practical use cases of PQC schemes in various areas, along with the associated challenges, have been thoroughly studied to understand future research directions that must be followed for the better optimisation of real-world PQC implementation in a quantum-safe future.

Keywords: Post-quantum cryptography; NIST standardisation; Classical cryptography; Digital signatures; Quantum Computing Threats

INTRODUCTION

Quantum computing represents a paradigm shift in computational power and problem-solving capabilities. It leverages the principles of quantum mechanics to perform calculations at speeds unachievable by classical computers [1]. However, this revolutionary technology poses significant threats to classical cryptography. The secure foundations of modern cryptographic algorithms rely on the computational difficulty of specific mathematical problems and are vulnerable to the immense processing capabilities of quantum computers [2].

The motivation for Post-Quantum Cryptography (PQC) is primarily based on the potential impacts of Shor's algorithm in efficiently solving trapdoor mathematical problems, such as integer factorisation complexity and elliptic curve discrete logarithm problems [3, 4]. These problems provide the security foundation of widely used public key cryptographic systems such as Diffie-Hellman (DH), Rivest-Shamir-Adleman (RSA), ElGamal, and Elliptic Curve Cryptography (ECC) [5]. Classical public-key algorithms for these problems typically require exponential time [3], where the time complexity increases exponentially with the input size. It makes them impenetrable to significant inputs. In contrast, Shor's algorithm on an adequately powerful quantum computer can solve these problems in polynomial time [4], where the time complexity grows at a quadratic rate. It makes these mathematical problems more penetrable, even with larger inputs. This capability would make these classical cryptosystems obsolete [6] and necessitate the development of quantum-resistant alternatives.

Symmetric cryptography is more resilient against quantum attacks, but not entirely immune [5]. Grover's algorithm can search unsorted databases quadratically faster [3] than classical algorithms, effectively reducing the security level of symmetric cryptographic systems, such as the Advanced Encryption Standard (AES). Grover's algorithm on a quantum computer can search for the secret key of AES-128 in 2^64 steps, compared to 2^128 steps on a classical computer [7]. Consequently, doubling key sizes (e.g., from AES-128 to AES-256) becomes necessary to maintain the desired security levels against quantum adversaries [5].

Table 1 – Impact of Quantum Computing on Classical Cryptographic Algorithms

Algorithm	Purpose	Impact
RSA	Encryption, key exchange	Shor's algorithm can factor large numbers efficiently
ECC	Encryption, digital signatures	Shor's algorithm can solve discrete logarithm problems efficiently
DH	Key exchange	Shor's algorithm can break digital signatures
AES	Symmetric encryption	Grover's algorithm reduces the adequate key size by half.
SHA	Hashing	Grover's algorithm reduces the security level.

RESULTS AND DISCUSSION

PQC algorithms have distinct differences in design and security foundations compared to classical algorithms. PQC algorithms are based on mathematical problems believed to be secure against quantum attacks [8], including high-dimensional lattices, nonlinear multivariate polynomial equations, syndrome decoding, and supersingular isogeny problems [9]. These PQC algorithms aim to provide robust security in a post-quantum era.

Core Families of PQC

Post-quantum cryptography comprises several cryptographic algorithm families that provide a range of solutions to security threats posed by quantum computing. Each family has its strengths and weaknesses, making them suitable for different use cases. This section discusses five key post-quantum cryptography families and provides a comparative analysis of their advantages, limitations, and trade-offs.

Lattice-Based Cryptography. Lattice-based cryptography is the most popular algorithm family in PQC [1]. It is based on the mathematical properties of higher-dimensional lattice problems [8, 10]. A lattice is a network of infinite points, where each point corresponds to a vector. In lattice-based cryptography, a message is represented as vectors, and the public key is a matrix that multiplies these vectors to generate the ciphertext [1]. This family is inherently versatile and can perform multiple cryptographic functions such as encryption (LWE, NTRU), digital signatures (Falcon, Dilithium), and KEM – Key Encapsulation Mechanisms (Kyber, Sabre) [8, 11]. While most other cryptosystems rely on their security in the average case, this algorithm family relies on worst-case problems, making it highly quantum resilient [9]. Lattice-based cryptographic algorithms provide strong protection against both classical and quantum attacks. They are also more favourable for resource-constrained and high-performance systems [6]. However, they require optimisation to address larger key sizes and ciphertexts compared to classical algorithms [11]. The practical adoption of these algorithms demands specialised implementation techniques, particularly in resource-constrained environments [12].

Code-Based Cryptography. Code-based cryptography relies on error-correcting codes to ensure secure communication by making it difficult to decode a general linear code, thereby providing robust security. The McEliece cryptosystem is the most well-known code-based scheme, which has remained unbroken since its introduction in 1978 [13]. It relies on the difficulty of decoding random linear error correction codes. A strong error correction code serves as the private key, combined with two blinding matrices to create a public key with reduced error correction capabilities. The message is encrypted using the public key matrix with random errors. The decryption utilises the private key matrices to reverse the scrambling and correct errors using the Goppa code [9, 14]. Despite its robust security, it suffers from time-consuming key generation, with encapsulation and decapsulation times that increase correspondingly [15]. This presents a challenge for practical implementation, given the large public key size of ~ 1MB [13], which makes it less suitable for resource-constrained environments [16]. Researchers have recently explored several variants of the McEliece cryptosystem to address this trade-off. The Niederreiter variant produces more compact ciphertexts and slightly smaller keys with minimal performance loss [6]. LDPC-based and quasi-cyclic variants reduce key sizes through sparsely connected or cyclic structures [13]. The f-variant introduces semi-systematic matrices to optimise the key size [15]. Researchers discovered that these variants are vulnerable to quantum attacks, while the original binary Goppa codes remain quantum resilient to date [13].

Hash-Based Cryptography. Hash-based cryptography focuses on the security of hash functions to provide digital signatures and authentication. Hash functions are irreversible mathematical functions that take arbitrary-length inputs and scramble them into fixed-size outputs [17]. Hash-

based algorithms are considered quantum-resistant as they leverage the difficulty of finding collisions or pre-images within a cryptographic hash function [18]. In this scheme, the one-time signature (OTS) is a fundamental concept, allowing each private key to sign only one message. Due to their large key and signature sizes, Merkle trees were later introduced to reduce key management overhead by organising multiple OTS in a binary tree structure [1, 19]. The Merkle tree root node is the public key, and the secret key becomes the private key of all one-time signatures in the tree [20]. SPHINCS+ is a prominent hash-based signature scheme with a stateless design [10]. It addresses the key management challenges associated with stateful schemes, such as XMSS [18]. The stateful schemes require maintaining and tracking the signature state, posing a risk of accidental state reuse. However, SPHINCS+ leverages techniques such as one-time signatures, few-time signatures, Merkle trees, and hyper-trees to generate secure, quantum-resistant signatures without requiring state tracking, making it ideal for distributed systems [9, 10].

Multivariate Polynomial Cryptography. Multivariate polynomial cryptography (MPC) is based on the difficulty of solving systems of multivariate quadratic equations over finite fields [21]. This algorithm family forms the public key using quadratic polynomial equations, and the private key is used to solve these equations. These cryptosystems are easy to construct, but due to their highly nonlinear nature, it is infeasible to solve these equations without knowledge of the private key [18]. This feature makes these schemes resistant to both classical and quantum attacks. MPC is primarily focused on public key cryptosystems and digital signatures, utilising schemes such as Rainbow and Unbalanced Oil and Vinegar (UOV). UOV divides variables into two sets: oil and vinegar. The vinegar variables are chosen randomly, and the equations involve interactions between these two sets. The "unbalanced" nature refers to having more vinegar than oil variables, which enhances the security of the scheme by making it harder to reverse-engineer the private key [8]. Rainbow is an advanced variant of UOV by using multiple sequential layers built upon one another with a distinct set of equations [6, 8]. This design offers faster generation and verification of compact signatures, making it suitable for resource-constrained environments, such as IoT [16]. However, Rainbow has been discovered to be vulnerable to algebraic key recovery attacks. These attacks exploit the mathematical structure of polynomial systems, allowing attackers to solve these equations more efficiently [10, 22].

Isogeny-Based Cryptography. Isogeny-based cryptography is based on supersingular isogeny problems – the difficulty of finding a mapping between two supersingular elliptic curves with the same structure [19]. This cryptographic family is notable for its compact key size, which makes it practical for limited data transmission systems, such as embedded or mobile platforms [11]. A major algorithm in this family is the Supersingular Isogeny Diffie-Hellman (SIDH), which was designed as a secure key exchange alternative for classical DH through the complex isogenies of supersingular elliptic curves [1]. It also demonstrates the potential for combining classical and quantum cryptographic algorithms to form hybrid cryptographic systems. SIKE is another prominent isogeny-based KEM that is implemented on pseudo-random walks in supersingular isogeny graphs [19]. Despite the strengths of isogeny-based cryptography, the computational complexity of isogeny generation and validation can bottleneck the system's performance [23]. SIKE has the smallest public key size but is also one of the slowest. Later, it was discovered to be vulnerable to the Castryck-Decru classical computer attack and removed from the NIST candidate algorithms [1], raising concerns about the long-term viability of isogeny-based schemes.

NIST PQC Project

In 2016, NIST initiated its PQC competition to address the risks posed by quantum computers to classical cryptographic systems. The competition consisted of several rounds to evaluate various algorithms for public-key encryption, KEM, and digital signatures. It began with 82 submissions [1] from cryptographers worldwide and was narrowed down to the first three finalised algorithms as standards for PQC for real-world deployments [24]. NIST aimed to select PQC algorithms that would secure both current and future systems from both classical and quantum computing attacks. Therefore, each round focused on different aspects of security, practicality, and efficiency.

In the first round, NIST evaluated theoretical security, performance, and implementation metrics. This initial screening filtered out proposals that did not meet the minimum requirements. In

the second stage, NIST thoroughly evaluated the strengths and weaknesses of each proposal and selected 17 KEM and nine signature schemes for the second round. During the second round, NIST assessed the software and hardware implementations of all 26 candidates and selected 15 algorithms for the next round [25]. By the end of the third round, NIST chose the CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, and SPHINCS+ algorithms for the fourth round. At the same time, it recognised BIKE, Classic McEliece, HQC, and SIKE as alternate candidate algorithms [26]. In the fourth round, NIST removed SIKE from the list of candidates, leaving only three alternate algorithms [1].

In August 2024, NIST published Module Lattice-Based Key Encapsulation Mechanism (ML-KEM) derived from CRYSTALS-Kyber, Module Lattice-Based Digital Signature (ML-DSA) derived from CRYSTALS-Dilithium and Stateless Hash-Based Digital Signature (SLH-DSA) derived from SPHINCS+ as the finalists of this PQC competition and the first set of PQC standards [24]. CRYSTALS-Kyber is a lattice-based cryptographic algorithm that leverages the LWE problem. NIST selected it for its efficiency in KEM and the combination of strong security with relatively small key sizes [27]. Its fast performance makes it ideal for resource-constrained environments as well [28, 29]. For digital signatures, CRYSTALS-Dilithium was identified as the primary candidate [30] due to its excellent speed and security, based on the same lattice-based foundations as Kyber [12, 31]. The SPHINCS+ is positioned as a backup solution in case other schemes encounter vulnerabilities [32]. It is well-recognised for its robust security properties, although it requires larger signatures and performs worse at higher security levels [31]. Additionally, the NTRU lattice-based Falcon algorithm has been drafted for the NIST PQC standardisation process and will be formally referred to as FN-DSA [24]. Although it has smaller signature sizes and faster verification, its implementation complexity requires careful management [10]. NIST also continues to evaluate the code-based Classic McEliece encryption scheme [33] due to its long track record of resilience, although its large key size presents deployment challenges.

Table 2 – Comparison Of Optimised NIST Standardised Algorithms

Algorithm	Public key size	Secret key size	Ciphertext size	Strengths	Weaknesses
ML-KEM-768	1,184 bytes	2,400 bytes	1,088 bytes	High-performance, efficient key exchange	Larger key sizes compared to classical
ML-DSA-65	1,952 bytes	4,032 bytes	3,309 bytes	High security, efficient signature generation	Higher computational cost
SLH-DSA-192	48 bytes	-	16,224 bytes	Very high security, stateless	Large key and signature sizes
FN-DSA-512	897 bytes	-	666 bytes	Fast signature generation, smaller key sizes	Lower security compared to Dilithium

Key Applications and Use Cases

The implementation of PQC spans various sectors, ensuring long-term security in the face of future quantum computing capabilities.

Public Key Infrastructure and Certificates. Public Key Infrastructure (PKI) relies on digital certificates to authenticate entities and encrypt data transmissions in modern-day client-server architecture. With the threat of quantum computing to the existing public key cryptosystems, PQC algorithms are essential for maintaining the integrity of PKI systems. NIST-finalised algorithms, such as ML-KEM and ML-DSA, are being incorporated into PKI to ensure that digital certificates issued today remain valid in the future [34]. Web service providers can implement PQC-enabled Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates to enable quantum-safe HTTPS communication. Email providers can apply the same approach to secure email communication [34]. During the transition period, system architects or organisations can combine classical cryptosystems with post-quantum cryptography (PQC) to enhance security and protect against Harvest Now, Decrypt Later (HNDL) attack [35]. Early PQC adoption in PKI ensures that current sensitive communications are quantum-ready and will not become vulnerable in a quantum era [2].

Secure Communication. Modern-day secure communication protocols are critical for protecting data exchanged over the internet. They are heavily relying on classical public key encryption and digital signature algorithms. To address future quantum attacks on these protocols, researchers are integrating PQC algorithms to ensure future-proof security [36]. They have extensively studied ML-KEM and ML-DSA for integration into TLS key exchange and authentication mechanisms [22]. ML-DSA provides up to 950 connections per second for level 3 security, while existing classical key exchange systems provide 400 connections per second. The ML-KEM and Falcon combination can provide 890 connections per second at level 5 security [31].

Similarly, PQC is also being integrated into Virtual Private Network (VPN) protocols to secure data transmission over potentially vulnerable communication channels [37]. ML-KEM is one of the promising approaches being explored for securing VPN tunnels. This approach is based on quantum-resistant key exchange, which encrypts the public key before exchanging it with the server [38]. Cisco has recently developed and tested quantum-safe VPN solutions combining classical and PQC algorithms [36]. Secure Shell (SSH) is the most common and safe protocol for remote system access, comprising TLS, authentication, and connection protocols. Adapting to existing encryption methods is a viable approach to making SSH quantum-safe [18]. Post-quantum KEM and signature schemes, such as ML-DSA, can provide strong authentication for SSH connections, protecting against both classical and quantum attacks [37].

Blockchain. Blockchain security relies on cryptographic algorithms to ensure data privacy, authenticity, and resistance to unauthorised changes. One approach for quantum-safe blockchain is to replace classical digital signature algorithms with ML-DSA and Falcon algorithms [39]. These algorithms provide more secure digital signatures, ensuring that data transactions and smart contracts cannot be tampered with by quantum computing. Ethereum-based Hyperledger Besu is currently experimenting with the integration of lattice-based and hash-based signature schemes for the seamless execution of smart contracts on quantum-resistant distributed ledgers [40]. PQC can further enhance blockchain security by either modifying an existing consensus algorithm, such as Proof of Work (PoW), or proposing a new consensus technique [41]. A hybrid blockchain approach enables a smooth, quantum-safe transition and maintains compatibility with existing cryptocurrency infrastructure [42]. This approach highlights the flexibility and adaptability in blockchain evolution and remains resilient against future technological threats.

IOT & Embedded Systems. Internet of Things (IoT) and embedded systems are devices that operate with limited computational power, memory, and battery life. The integration of PQC into these systems requires optimised protocols and architectural adjustments to ensure efficiency. Lattice-based lightweight algorithms, such as Kyber, Sabre, LightSaber-KEM, and Dilithium2, demonstrate higher performance on IoT hardware due to their relatively low computational demands. They can significantly preserve battery life and execution time, making these lattice-based PQC algorithms ideal for constrained devices [29]. Additionally, the use of efficient communication protocols, such as MQTT alongside PQC, ensures secure and lightweight data exchange. This integration helps IoT systems maintain a balance between security and performance without compromising resource efficiency [28]. Studies on PQC implementations in constrained devices have focused on both performance and feasibility. Key generation benchmark experiments involving Kyber KEM and signature schemes on platforms such as Arduino Uno, Raspberry Pi 4, and ESP32 indicated that Kyber-512 was the fastest, while Kyber-768 was the most stable, with minimal variance across multiple executions. Kyber-768 can offer the best trade-off between performance, stability, and security for any IoT application [28].

Cloud Security. Cloud providers rely heavily on cryptosystems to protect data at rest, in transit, and during processing [36]. PQC can provide a viable path forward by offering quantum-resilient algorithms to ensure the continued confidentiality, integrity, and availability of cloud resources. Tech giants like Amazon, Google, Microsoft, and IBM have already implemented commercial quantum computing cloud services [43]. ML-KEM is integrated into cloud encryption and quantum-safe key exchange mechanisms to ensure secure communication between cloud clients and servers. ML-DSA and SLH-DSA are integrated, quantum-resistant authentication mechanisms for users, services, and applications in the cloud [36, 44]. Since 2014, Microsoft has invested heavily in PQC through Azure, providing secure quantum computing capabilities. Azure

adaptive quantum solutions and hybrid schemes ensure a smooth transition for migration to the hyperscale cloud, promoting quantum-safe readiness and the implementation of quantum-safe technologies across the Microsoft ecosystem [45]. IBM has introduced IBM z16, the industry's first quantum-safe hybrid cloud system targeting the finance and insurance sectors [46]. Google replaced ECC with the NewHope key exchange algorithm in Google Chrome as part of its transition to a quantum-safe cloud service [36]. Furthermore, PQC algorithms are integrated into identity and access management (IAM) systems for identity-based encryption and attribute-based encryption within the cloud, ensuring trusted authentication and authorisation processes [4]. Additionally, the adoption of ML-DSA into cryptographic libraries, such as Crypto++, enables seamless API authentication, providing more robust cloud security, even in scenarios involving machine-to-machine communication [47].

Challenges in PQC Adoption

Researchers and industry leaders must address several challenges and limitations to ensure the successful adoption of PQC for securing information systems in the quantum era.

Performance Trade-offs. One of the most significant challenges in adopting PQC is the performance trade-off compared to classical cryptographic algorithms. Lattice-based Kyber and Sabre exhibit larger key sizes and ciphertexts than traditional algorithms, such as RSA and ECC. This results in increased memory and bandwidth requirements. For instance, ML-KEM-768 requires 2,400 bytes per private key and produces ciphertexts of 1,088 bytes [27], in contrast to RSA-2048's 256 bytes and ECC-256's 32 bytes private keys and their relatively more minor ciphertexts [17]. This difference can adversely impact network performance, particularly in resource-constrained environments.

Furthermore, the signature sizes of ML-DSA-65 and SLH-DSA-192, at 3,309 bytes and 16,224 bytes, respectively [10], introduce additional latency in the digital signing and verification process. Classic McEliece requires keys of approximately 1 MB, which also presents significant challenges for storage and transmission. Such factors render them less efficient for real-time applications such as TLS handshakes, compared to SHA-256 [15, 18]. Balancing security with speed and resource consumption remains a critical challenge, especially for high-performance systems that demand low latency and high throughput.

Implementation Challenges. The transition to PQC presents several challenges across hardware and software platforms. Implementation of NIST's PQC algorithms on various hardware platforms requires significant modifications due to their larger key sizes and more complex operations compared to classical algorithms; this leads to increased memory, processing power, bandwidth, and storage needs, which can be both time-consuming and resource costly to accommodate [9, 15, 20]. Hardware accelerators, such as Field Programmable Gate Arrays (FPGAs) and Advanced Encryption Standard New Instructions (AES-NI), can enhance the performance of cryptographic algorithms across various hardware platforms. However, PQC implementation often requires meeting performance benchmarks, adding to the complexity of deployment [1, 37, 48, 49]. On the software side, integrating these algorithms poses challenges in optimising performance to avoid degrading system efficiency; this is particularly critical for real-time applications where latency is a significant issue. Existing cryptographic libraries and protocols must be updated or replaced, necessitating substantial changes to the codebase [25, 47].

Key Management and Distribution Complexities. The adoption of PQC introduces new key management and distribution complexities due to the larger key sizes and more frequent key rotations required [5]. Traditional key distribution methods prove inadequate for PQC due to the larger key sizes and the necessity for secure channels. Ensuring that keys are generated, exchanged, and stored securely without compromising performance remains a formidable challenge. Moreover, the lifecycle management of cryptographic keys – encompassing creation, distribution, rotation, and revocation – becomes increasingly complex with the use of PQC. The substantial key sizes and the need for frequent updates to maintain security place considerable strain on key management systems and protocols.

Additionally, the larger key sizes and ciphertexts characteristic of PQC algorithms can adversely impact network bandwidth. Efficient key distribution over networks—without causing significant delays or bottlenecks—presents a critical challenge. Additionally, the increased storage requirements for keys and certificates raise concerns about scalability, particularly in PKI sys-

tems that must issue and manage millions of certificates. [34]. Integrating PQC algorithms into existing cryptographic systems and protocols necessitates meticulous consideration of compatibility issues [36]. Ensuring that PQC algorithms function seamlessly alongside legacy systems is essential for a smooth transition. As the adoption of PQC algorithms increases, the scalability of key management and distribution systems becomes a pertinent concern. Systems must adeptly handle a growing number of keys and cryptographic operations without compromising security or performance.

Backward Compatibility. Transitioning to PQC presents significant challenges in maintaining backwards compatibility with existing cryptographic systems. The current cryptographic infrastructure is heavily reliant on classical algorithms and deeply integrated into various systems, including PKI, secure communication protocols, and software applications. Replacing these with PQC algorithms requires ensuring that new systems remain compatible with legacy systems to avoid disruptions. During the transition period, systems using classical algorithms must be able to communicate securely with systems using PQC; this requires hybrid solutions that support both classical and PQC algorithms [25]. However, these hybrid systems should not introduce new vulnerabilities. Rigorous testing and validation are required to ensure that backwards compatibility does not compromise overall security. PQC algorithms often require more computational resources, and updating existing infrastructure to support PQC is a resource-intensive process. Ensuring that these impacts do not degrade user experience or system efficiency is a significant challenge. Organisations must allocate substantial time and financial resources to re-engineer systems, update software, and retrain personnel [2]. Balancing these costs with the need to maintain backwards compatibility adds another layer of complexity to the transition process.

Implementation-specific Vulnerabilities. PQC algorithms are not immune to side-channel attacks that exploit information leaked through physical or timing characteristics during computation [50]. Timing attacks, power analysis, and fault injection attacks have indeed been identified as potential threats to PQC implementations. For instance, lattice-based algorithms like Kyber can leak information through timing variations if not implemented securely [51]. Similarly, code-based and hash-based algorithms are vulnerable to fault injections that can corrupt key generation processes, compromising the entire encryption scheme [52]. Ensuring that implementations are side-channel resistant requires additional engineering effort, including the use of constant-time algorithms and side-channel mitigation techniques, further complicating the deployment of PQC [43]. Vulnerabilities due to coding errors, hardware design flaws, or inadequate security practices can arise as implementation-specific vulnerabilities. For instance, a poorly implemented PQC algorithm might be vulnerable to fault attacks [52], where an attacker induces errors to extract sensitive information. Ensuring robust and secure implementations requires rigorous testing, validation, and adherence to the best practices in cryptographic engineering.

Future Research

As PQC continues to develop, researchers are exploring possibilities to address the remaining challenges and extend the capabilities of quantum-resistant systems.

Hybrid Approaches. A complete transition to PQC is a gradual process due to the involved complexities. As a result, combining classical and quantum-resistant algorithms to form hybrid approaches is a current research focus [25].

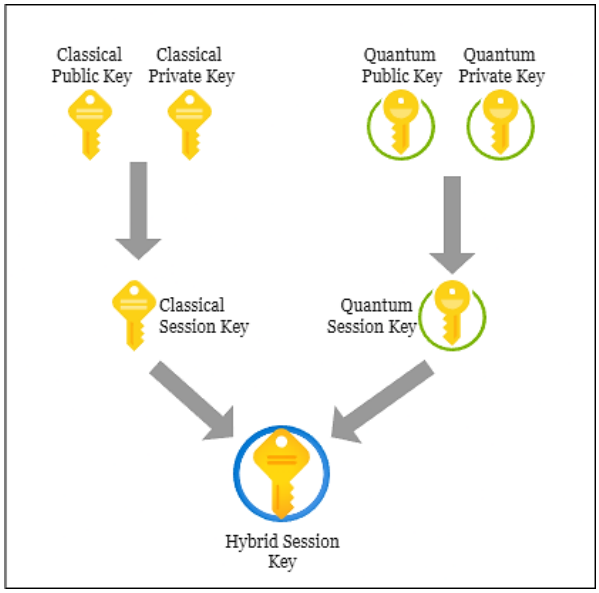

Figure 1 – Overview of a Hybrid Cryptographic Protocol Combining Classical and Post-Quantum Cryptography

Hybrid cryptosystems ensure interoperability with existing infrastructure, providing seamless integration while offering long-term security

against emerging quantum threats [43]. One main challenge with hybrid systems is the operational complexity of maintaining dual cryptographic frameworks simultaneously; this involves addressing potential computational overheads and ensuring the system's efficiency and security [49]. Future research must address these concerns to optimise hybrid protocols for robust performance in key exchanges and authentication processes, especially for services like TLS and VPNs, where secure and efficient data transmission is paramount.

Decentralised Protocols. Future research must focus on developing quantum-resistant blockchains by integrating PQC algorithms like ML-DSA and SLH-DSA to replace vulnerable ECDSA signatures [40]. Researchers should explore new cryptographic approaches to secure blockchain systems against emerging quantum attack vectors. Developers can utilise self-sovereign identity (SSI) systems based on PQC to safeguard blockchains against identity theft and unauthorised access to personal data [39]. Individuals can maintain high control over their identities with enhanced security through these secure SSI systems. Research is also needed to design consensus protocols that can efficiently operate with quantum-resistant algorithms, as these protocols typically require intensive communication and computation [41]. Furthermore, exploring hybrid blockchains [42] that use both classical and PQC algorithms can provide a practical transition path, maintaining security and performance during the migration phase.

Hardware Acceleration. One of the key challenges in adopting PQC is the increased computational load, making hardware acceleration a vital research focus. FPGA-based implementations of PQC algorithms, such as Kyber and Sabre, are being explored to improve performance by offloading intensive operations to dedicated hardware [48]. Future research should examine ways to optimise these FPGA implementations for different application environments, including cloud data centres and edge devices [43]. Additionally, further research into designing crypto accelerators that can support both classical and PQC algorithms will be essential to ensure seamless transitions without sacrificing performance.

Constrained Environments. IoT devices and mobile platforms face unique challenges in adopting PQC due to limited computational resources, memory, and power. Research is needed to develop lightweight PQC algorithms, such as optimised versions of Kyber and Sabre, and efficient key management solutions for frequent rotations [9, 29]. Future research should also focus on interoperability frameworks for seamless PQC integration across various IoT platforms and mobile networks [36].

Crypto-agility. Crypto-agility is the capability of systems to rapidly adapt to new cryptographic algorithms as threats evolve [34]. As PQC algorithms become standardised and implemented, agile frameworks are crucial for seamlessly transitioning between classical, hybrid, and quantum-safe algorithms [18]. Research focuses on developing systems that support dynamic cryptographic updates without service disruption, ensuring continuous security despite the emergence of new vulnerabilities or advancements in technology. This approach enables organisations to gradually integrate PQC while staying responsive to emerging quantum threats and advancements in cryptography [35].

QKD. While PQC focuses on developing mathematical algorithms to withstand quantum attacks, Quantum Key Distribution (QKD) focuses on the principles of quantum mechanics to ensure secure key exchange [53]. Integrating QKD with PQC can create hybrid systems that leverage the benefits of both approaches [13]. Future research will need to focus on developing efficient protocols to combine these technologies and infrastructure solutions, thereby supporting the deployment of QKD networks alongside classical and quantum-resistant systems.

CONCLUSIONS

The advancement of PQC is crucial as it fortifies the digital realm from emerging quantum threats. It involves efforts to identify and analyse mathematical problems that stay resilient in the face of quantum capabilities and standardising algorithms for robust security in the quantum era. This journey has witnessed significant milestones in the NIST's PQC standardisation project. The cryptographic community anticipates a gradual yet determined shift toward the adoption of these PQC standards across various sectors, ensuring the quantum readiness of existing infrastructures to handle the challenges of the quantum era. Future research is expected to refine these algorithms for better performance and efficiency by addressing the existing challenges, complexities, and trade-offs.

REFERENCES

1. Dam, D., Tran, T., Hoang, V., Pham, C., & Hoang, T. (2023). A survey of Post-Quantum Cryptography: Start of a new race. *Cryptography, 7*(3), 40. doi: 10.3390/cryptography7030040

2. Käppler, S. A., & Schneider, B. (2022). Post-Quantum Cryptography: An Introductory overview and implementation challenges of Quantum-Resistant Algorithms. *EPiC Series in Computing, 8*4, 61–49. doi: 10.29007/2tpw

3. Hegde, S. B., Jamuar, A., & Kulkarni, R. (2023). Post Quantum Implications on Private and Public Key Cryptography. *International Conference on Smart Systems for Applications in Electrical Sciences (ICSSES)*, 1–6. doi: 10.1109/icsses58299.2023.10199503

4. Ott, D., Peikert, C., & Participants, O. W. (2019). Identifying research challenges in post-quantum cryptography migration and cryptographic agility. *arXiv (Cornell University)*. doi: 10.48550/arxiv.1909.07353

5. Lella, E., Gatto, A., Pazienza, A., Romano, D., Noviello, P., Vitulano, F., & Schmid, G. (2022). Cryptography in the Quantum Era. *IEEE 15th Workshop on Low Temperature Electronics (WOLTE)*, 1–4. doi: 10.1109/wolte55422.2022.9882585

6. Roy, K. S., & Kalita, H. K. (2019). A Survey on Post-Quantum Cryptography for Constrained Devices. *International Journal of Applied Engineering Research, 14*(11), 2608–2615.

7. Gajbhiye, S., Karmakar, S., Sharma, M., & Sharma, S. (2017). Paradigm shift from classical cryptography to quantum cryptography. *International Conference on Intelligent Sustainable Systems (ICISS),* 548–555. doi: 10.1109/iss1.2017.8389231

8. Richter, M., Bertram, M., Seidensticker, J., & Tschache, A. (2022). A Mathematical Perspective on Post-Quantum Cryptography. *Mathematics, 10*(15), 2579. doi: 10.3390/math10152579

9. Bavdekar, R., Chopde, E. J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023). Post Quantum Cryptography: A review of techniques, challenges and standardisations. *2022 International Conference on Information Networking (ICOIN)*, 146–151. doi: 10.1109/icoin56518.2023.10048976

10. Pinto, J. (2022). Post-Quantum cryptography. *ARIS2 - Advanced Research on Information Systems Security, 2*(2), 4–16. doi: 10.56394/aris2.v2i2.17

11. Yalamuri, G., Honnavalli, P., & Eswaran, S. (2022). A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats. *Procedia Computer Science, 215*, 834–845. doi: 10.1016/j.procs.2022.12.086

12. Soni, D., Basu, K., Nabeel, M., & Karri, R. (2019). A Hardware Evaluation Study of NIST Post-Quantum Cryptographic Signature Schemes. *2nd PQC Standardisation Conference.*

13. Balamurugan, C., Singh, K., Ganesan, G., & Rajarajan, M. (2021). Post-Quantum and Code-Based Cryptography—Some prospective research directions. *Cryptography, 5*(4), 38. doi: 10.3390/cryptography5040038

14. Pratama, I. P. A. E., & Adhitya, I. G. N. A. K. (2022). Post Quantum Cryptography: Comparison between RSA and McEliece. *International Conference on ICT for Smart Society (ICISS)*, 01–05. doi: 10.1109/iciss55894.2022.9915232

15. Lingeshwaran, B., & Singh, A. (2022). Performance Evaluation of Classic McEliece Post Quantum Cryptography. *Algorithms, Computing and Mathematics Conference (ACM),* 90–94. doi: 10.1109/acm57404.2022.00022

16. Roma, C. A., Tai, C. A., & Hasan, M. A. (2021). Energy efficiency analysis of Post-Quantum Cryptographic Algorithms. *IEEE Access, 9*, 71295–71317. doi: 10.1109/access.2021.3077843

17. Sanon, S. P., Alzalam, I., & Schotten, H. D. (2023). Quantum and Post-Quantum Security in Future Networks. *IEEE Future Networks World Forum (FNWF)*, 1–6. doi: 10.1109/fnwf58287.2023.10520624

18. Grote, O., Ahrens, A., & Benavente-Peces, C. (2019). A Review of Post-quantum Cryptography and Crypto-agility Strategies. *International Interdisciplinary PhD Workshop (IIPhDW),* 115–120. doi: 10.1109/iiphdw.2019.8755433

19. Kumar, M. (2022). Post-Quantum Cryptography Algorithms' Standardisation and Performance Analysis. *Array, 15*, 100242. doi: 10.1016/j.array.2022.100242

20. Tiwari, A., Chauhan, R., Joshi, N., Devliyal, S., Aluvala, S., & Kumar, A. (2024). The Quantum Threat: Implications for data security and the rise of Post-Quantum cryptography. *IEEE 7th International Conference for Convergence in Technology (I2CT)*. doi: 10.1109/i2ct61223.2024.10543513

21. Giroti, I., & Malhotra, M. (2022). Quantum Cryptography: A Pathway to Secure Communication. *6th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS*), 1–6. doi: 10.1109/csitss57437.2022.10026388

22. Garcia, C. R., Aguilera, A. C., Olmos, J. J. V., Monroy, I. T., & Rommel, S. (2023). Quantum-Resistant TLS 1.3: A Hybrid Solution Combining Classical, Quantum and Post-Quantum Cryptography. *IEEE 28th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD),* 13895, 246–251. doi: 10.1109/camad59638.2023.10478407

23. Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., Liang, W., & Xiong, N. (2023). Post-Quantum Security: opportunities and challenges. *Sensors, 23*(21), 8744. doi: 10.3390/s23218744

24. NIST. (2024). *NIST Releases First 3 Finalised Post-Quantum Encryption Standards*. Retrieved from https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

25. Kan, K., & Une, M. (2021). Recent Trends on Research and Development of Quantum Computers and Standardisation of Post-Quantum Cryptography. *Monetary and Economic Studies.*

26. Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022). Status report on the third round of the NIST Post-Quantum Cryptography Standardisation process. *NIST.* doi: 10.6028/nist.ir.8413-upd1

27. NIST. (2024). Module-Lattice-Based Key-Encapsulation Mechanism Standard. *NIST*. doi: 10.6028/nist.fips.203

28. Ristov, R., & Koceski, S. (2023). Quantum resilient public key cryptography in the internet of things. *11th Mediterranean Conference on Embedded Computing (MECO),* 1–4. doi: 10.1109/meco58584.2023.10154994

29. Sajimon, P. C., Jain, K., & Krishnan, P. (2022). Analysis of Post-Quantum Cryptography for Internet of Things. *6th International Conference on Intelligent Computing and Control Systems (ICICCS),* 387–394. doi: 10.1109/iciccs53718.2022.9787987

30. FIPS 204 (2024). Module-Lattice-Based Digital Signature Standard. *NIST* doi: 10.6028/nist.fips.204

31. Doring, R., & Geitz, M. (2022). Post-Quantum Cryptography in Use: Empirical analysis of the TLS handshake performance. *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, 1–5. doi: 10.1109/noms54207.2022.9789913

32. FIPS 205 (2024). Stateless Hash-Based Digital Signature Standard. *NIST* doi: 10.6028/nist.fips.205

33. NIST. (2022). PQC Standardisation Process: Announcing Four Candidates to be Standardised, Plus Fourth Round Candidates. Retrieved from https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

34. Bene, F., & Kiss, A. (2023). Post-Quantum Security: An overview of the public key infrastructure. *System Theory Control And Computing Journal, 3*(2), 27–35. doi: 10.52846/stccj.2023.3.2.55

35. Thakur, M. S. D., Vidhani, K., Syed, H. B., & MA, R. (2024). Enterprise Post Quantum Cryptography Migration Tools. *16th International Conference on COMmunication Systems & NETworkS (COMSNETS),* 327–329. doi: 10.1109/comsnets59351.2024.10427442

36. Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024). Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography. *15th International Conference on Network of the Future (NoF)*, 195–203. doi: 10.1109/nof62948.2024.10741441

37. Mehic, M., Michalek, L., Dervisevic, E., Burdiak, P., Plakalovic, M., Rozhon, J., Mahovac, N., Richter, F., Kaljic, E., Lauterbach, F., Njemcevic, P., Maric, A., Hamza, M., Fazio, P., & Voznak, M. (2023). Quantum Cryptography in 5G Networks: A Comprehensive Overview. *IEEE Communications Surveys & Tutorials, 26*(1), 302–346. doi: 10.1109/comst.2023.3309051

38. Marrok, A., Boukhelef, S., & Chikouche, N. (2024). PQH-WireGuard: Post-Quantum Hybrid Cryptography-Based WireGuard VPN Protocol. In *Lecture Notes in Networks and Systems* (pp. 283–292). doi: 10.1007/978-981-99-8324-7_25

39. Moraes, D. H., Pereira, J. P. A., Grossi, B. E., Mirapalheta, G. C., Smetana, G. M. M. A., Rodrigues, W., Guimarães, N., Domingues, B., Saito, F., Simplício, M., & Guimarães, J. C. N. (2024). Applying Post-Quantum Cryptography Algorithms to a DLT-Based CBDC Infrastructure: Comparative and Feasibility Analysis. *Cryptology EPrint Archive.*

40. Chauhan, S., Ojha, V. P., Yarahmadian, S., & Carvalho, D. (2023). Towards building quantum-resistant blockchain. *International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 1–9. doi: 10.1109/icecet58911.2023.10389558

41. Jose, J. M., & V, P. (2022). A Survey on Consensus Algorithms in Blockchain Based on Post-Quantum Cryptosystems. *5th International Conference on Computational Intelligence and Networks (CINE),* 1–6. doi: 10.1109/cine56307.2022.10037353

42. 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*(2), 967–1002. doi: 10.1109/comst.2023.3325761

43. Zeydan, E., Turk, Y., Aksoy, B., & Ozturk, S. B. (2022). Recent Advances in Post-Quantum Cryptography for Networks: A Survey. *Seventh International Conference on Mobile and Secure Services (MobiSecServ),* 1–8. doi: 10.1109/mobisecserv50855.2022.9727214

44. Dhinakaran, D., Selvaraj, D., Dharini, N., Raja, S. E., & Priya, C. S. L. (2024). Towards a Novel Privacy-Preserving Distributed Multiparty Data Outsourcing Scheme for Cloud Computing with Quantum Key Distribution. *arXiv (Cornell University).* doi: 10.48550/arxiv.2407.18923

45. Bell, C. (2023). Building a quantum-safe future. Retrieved from https://blogs.microsoft.com/blog/2023/05/31/building-a-quantum-safe-future/

46. Meaney, P., Mishra, A., & Rao, R. (2024). Synchronous, Low-Latency, Off-Module Interface for the IBM z16TM Telum® Processor. *IEEE Micro*, 1–9. doi: 10.1109/mm.2024.3424506

47. Hekkala, J., Muurman, M., Halunen, K., & Vallivaara, V. (2023). Implementing post-quantum cryptography for developers. *SN Computer Science, 4*(4). doi: 10.1007/s42979-023-01724-1

48. Ni, Z., Khalid, A., & O'Neill, M. (2022). High Performance FPGA-based Post Quantum Cryptography Implementations. *32nd International Conference on Field-Programmable Logic and Applications (FPL),* 456–457. doi: 10.1109/fpl57034.2022.00076

49. 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. doi: 10.1109/access.2024.3364520

50. Fritzmann, T., Van Beirendonck, M., Roy, D. B., Karl, P., Schamberger, T., Verbauwhede, I., & Sigl, G. (2021). Masked accelerators and instruction set extensions for Post-Quantum cryptography. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 414–460. doi: 10.46586/tches.v2022.i1.414-460

51. Saarinen, M. O. (2022). WiP: Applicability of ISO Standard Side-Channel Leakage Tests to NIST Post-Quantum Cryptography. *IEEE International Symposium on Hardware Oriented Security and Trust (HOST),* 69–72. doi: 10.1109/host54066.2022.9839849

52. Bettale, L., Montoya, S., & Renault, G. (2021). Safe-Error Analysis of Post-Quantum Cryptography Mechanisms - Short Paper-. *Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, 39–44. doi: 10.1109/fdtc53659.2021.00015

53. Ahn, J., Kwon, H., Ahn, B., Park, K., Kim, T., Lee, M., Kim, J., & Chung, J. (2022). Toward quantum-secured distributed energy resources: adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). *Energies, 15*(3), 714. doi: 10.3390/en15030714