

POST-QUANTUM CRYPTOGRAPHY: TRANSITION STRATEGIES, CHALLENGES, AND FUTURE DIRECTIONS

Anjali DV,
Department of Computer Science and Engineering
C Byre Gowda Institute of Technology,
Kolar, Karnataka
anjalicbictse21@gmail.com

Dr. Deepika Lokesh
Department of AI & ML
C Byre Gowda Institute of Technology,
Kolar, Karnataka
ushalokesh@gmail.com

Abstract: *The rapid evolution of quantum computing is expected to significantly disrupt the security assumptions of current cryptographic systems. Most important widely used encryption methods depend on mathematical problems that are computationally intractable for classical machines but solvable via quantum algorithms like Shor's and Grover's ones. This new risk has triggered the advancement in Post-Quantum Cryptography (PQC), which aims to create cryptographic systems that can be effective against both classical and quantum attacks while being suitable for existing digital infrastructures.*

This paper presents a detailed study of prominent PQC approaches, including lattice-based, hash-based, and code-based techniques, along with their underlying principles, strengths, and limitations. It further examines global standardization efforts, particularly those initiated by NIST, and discusses practical considerations involved in transitioning from traditional cryptographic systems to quantum-resistant solutions. Key challenges such as increased computational cost, larger key sizes, and integration with legacy systems are critically analyzed. In addition, the paper highlights ongoing research trends and identifies areas that require further investigation to achieve efficient and scalable deployment of PQC in real-world environments.

Keywords: *Post-Quantum Cryptography, Quantum Computing, Cybersecurity, NIST, Cryptographic Transition, Quantum Attacks, Hybrid Cryptography*

I. INTRODUCTION

The continuous advancement of quantum computing is redefining the boundaries of computational capability and, in doing so, challenging the security assumptions of modern cryptographic systems. Techniques that have long been considered secure in classical computing environments are now facing potential obsolescence due to the emerging power

of quantum algorithms. As research transitions from theoretical exploration to practical implementation, concerns regarding the long-term confidentiality and integrity of digital information are becoming increasingly urgent [1], [2].

Traditional cryptographic mechanisms rely chiefly on mathematical problems like integer factorization and discrete logarithms, whose solution is computationally infeasible for classical computers. These assumptions form the backbone of many of the public-key algorithms in use today, such as RSA and Elliptic Curve Cryptography (ECC). Yet quantum algorithms such as Shor's algorithm, significantly alters this landscape by enabling these problems to be solved in polynomial time, thereby undermining the security of widely used encryption protocols [3]. In addition to public-key systems, symmetric cryptographic techniques are also affected by quantum advancements. Although they are comparatively more resistant, Grover's algorithm introduces a quadratic speedup in brute-force search, effectively reducing the strength of symmetric keys. This implies that existing key sizes may no longer provide adequate security, necessitating modifications such as increasing key lengths to maintain resilience against quantum attacks [4].

A particularly critical concern associated with quantum computing is the possibility of delayed decryption attacks, often described as the —harvest now, decrypt later! model. In this scenario, adversaries collect encrypted data in the present and store it for future decryption when sufficiently powerful quantum systems become available. This threat is especially relevant for sensitive information that requires long-term protection, including financial records, healthcare data, and government communications [5], [6].

To address these emerging risks, the research community has increasingly focused on the development of Post-Quantum Cryptography (PQC). Unlike quantum cryptographic techniques that require specialized hardware, PQC solutions are designed to operate within existing computing environments while providing resistance against both classical and quantum adversaries. This makes PQC a practical and scalable approach for securing current and future digital systems [7].

Recent developments indicate a growing effort to integrate PQC into real-world applications, including cloud computing platforms, Internet of Things (IoT) ecosystems, and secure communication protocols. At the same time, global standardization initiatives led by organizations such as the National Institute of Standards and Technology (NIST) are playing a crucial role in evaluating and recommending quantum-resistant algorithms for widespread adoption [8]–[10]. Despite the promising progress in this domain, transitioning from classical cryptographic systems to PQC presents several technical and operational challenges. Issues such as increased key sizes, higher computational requirements, and compatibility with legacy infrastructure complicate the deployment process. Furthermore, ensuring cryptographic agility—where systems can adapt to evolving standards—has become a critical requirement for long-term security [11].

In this context, a comprehensive understanding of PQC techniques, transition strategies, and implementation challenges is essential. This paper aims to provide a detailed survey of post-quantum cryptographic approaches, analyze the practical difficulties associated with their adoption, and explore future research directions that can facilitate the development of secure and efficient cryptographic systems in the quantum era.

II. BACKGROUND OF CLASSICAL CRYPTOGRAPHY

Classical cryptography forms the backbone of modern digital security systems and has been extensively used for decades to protect sensitive information across communication networks. Its primary objective is to ensure confidentiality, integrity, authentication, and non-repudiation of data. These systems rely on mathematically complex problems that are computationally infeasible to solve using classical computers within a reasonable time frame [1], [2]. However, the emergence of quantum computing challenges the assumptions underlying these cryptographic foundations.

A. Public-Key Cryptography

Public-key cryptography, often referred to as asymmetric encryption, is a fundamental method used to secure communication across untrusted networks. It is based on a pair of interconnected keys: a public key that can be freely distributed and a private key that remains confidential with its owner. This approach supports essential security functions such as data encryption, authentication through digital signatures, and secure key exchange.

Well-known asymmetric algorithms like RSA and Elliptic Curve Cryptography (ECC) derive their security from the complexity of solving certain mathematical problems, including integer factorization and the discrete logarithm problem. In classical computing environments, solving these problems requires exponential time, making them secure for practical use [3]. These cryptographic systems are extensively deployed in secure web communication (SSL/TLS), email encryption, and authentication systems.

However, their heavy reliance on mathematical hardness assumptions makes them highly vulnerable in the presence of quantum computing, where these problems can be solved efficiently.

B. Symmetric Cryptography

Symmetric cryptography involves the use of a single shared key for both encryption and decryption. Unlike public-key systems, symmetric algorithms are computationally efficient and suitable for encrypting large volumes of data. The Advanced Encryption Standard (AES) is one of the most widely used symmetric encryption algorithms due to its high performance and strong security guarantees.

Symmetric encryption is commonly used in applications such as file encryption, secure communication channels, and database protection. Its security primarily depends on key size and resistance to brute-force attacks. For example, AES-

128 and AES-256 are considered secure under classical assumptions [4].

Despite being more resilient than public-key cryptography, symmetric systems are still affected by quantum advancements. Quantum algorithms like Grover's algorithm reduce the effective key strength, requiring longer keys to maintain equivalent security levels.

C. Cryptographic Hash Functions

Cryptographic hash functions are fundamental components used for data integrity verification, authentication, and digital signatures. These functions take an input of arbitrary size and produce a fixed-length output known as a hash value or message digest.

Well-known hash functions such as SHA-2 and SHA-3 are designed to satisfy properties like pre-image resistance, second pre-image resistance, and collision resistance. These properties ensure that it is computationally infeasible to reverse the hash or find two different inputs that produce the same output [5].

Hash functions are widely used in password storage, blockchain technologies, and integrity verification systems. Their role becomes even more significant in post-quantum cryptography, as many PQC schemes rely on hash-based constructions.

D. Applications of Classical Cryptography

Classical cryptographic techniques are deeply embedded in modern digital infrastructures. They are used in various applications, including secure communication protocols such as HTTPS, Virtual Private Networks (VPNs), and secure shell (SSH). In financial systems, cryptography ensures secure transactions and protects sensitive user information.

Additionally, cryptographic mechanisms are essential in cloud computing, where they protect stored and transmitted data, and in blockchain systems, where they ensure transparency and immutability of transactions [6], [7]. Despite their effectiveness in classical environments, these systems face significant challenges in the quantum era, necessitating the exploration of quantum-resistant alternatives.

III. QUANTUM THREATS TO CRYPTOGRAPHY

The emergence of quantum computing represents a paradigm shift in computational capabilities, posing a direct threat to traditional cryptographic systems. Unlike classical computers, quantum computers leverage principles

such as superposition and entanglement to perform parallel computations, significantly reducing the time required to solve complex problems [8], [9].

A. Impact on Public-Key Cryptography

Public-key cryptographic systems are particularly vulnerable to quantum attacks due to their reliance on mathematical problems that can be efficiently solved using quantum algorithms. Shor's algorithm is one of the most significant breakthroughs in this domain, as it can factor large integers and compute discrete logarithms in polynomial time [3].

This capability directly undermines the security of widely used cryptographic schemes such as RSA and ECC. As a result, encrypted communications, digital signatures, and authentication mechanisms that rely on these algorithms become susceptible to compromise in a quantum computing environment.

B. Impact on Symmetric Cryptography

While symmetric cryptography is generally more resistant to quantum attacks, it is not completely immune. Grover's algorithm provides a quadratic speedup for brute-force key search attacks, effectively reducing the security strength of symmetric encryption algorithms [4].

For instance, a 128-bit key would offer only 64 bits of security against a quantum adversary. To counter this, it is necessary to increase key sizes (e.g., using AES-256 instead of AES-128) to maintain acceptable security levels in the quantum era.

C. Harvest Now, Decrypt Later Threat

One of the most concerning implications of quantum computing is the —harvest now, decrypt later! attack model. In this scenario, adversaries collect encrypted data today and store it with the intention of decrypting it in the future when quantum computing capabilities become sufficiently advanced [5], [6].

This is particularly dangerous for data that requires long-term confidentiality, such as government communications, healthcare records, and financial transactions. This threat highlights the urgency of transitioning to quantum-resistant cryptographic systems before large-scale quantum computers become operational.

D. Broader Implications for Cybersecurity

The impact of quantum computing extends beyond individual algorithms to the entire cybersecurity ecosystem. Current infrastructures—including cloud platforms, IoT networks, and communication protocols—are heavily dependent on classical cryptographic primitives.

A successful quantum attack could compromise these systems at scale, leading to widespread security breaches. Therefore, it is essential to adopt proactive measures and transition strategies to ensure resilience against future quantum threats [10], [11].

IV. POST-QUANTUM CRYPTOGRAPHY TECHNIQUES

The limitations of classical cryptographic systems in the presence of quantum computing have led to the development of alternative security mechanisms collectively known as Post-Quantum Cryptography (PQC). As mentioned in the Table I, these techniques are specifically engineered to withstand attacks from both conventional and quantum computers while remaining deployable on existing digital infrastructure. Unlike quantum key distribution, which requires specialized communication channels, PQC focuses on software-compatible solutions that can be integrated into current systems with minimal architectural changes [8], [10].

Rather than relying on a single mathematical principle, PQC consists of multiple algorithmic families, each grounded in different hard computational problems. This diversity is essential, as it reduces the risk of a universal failure if one approach becomes vulnerable.

A. Lattice-Based Cryptography

Among the various PQC approaches, lattice-based cryptography has emerged as a leading candidate due to its combination of efficiency, scalability, and strong security assumptions. These schemes are constructed on the difficulty of solving lattice problems such as the Shortest Vector Problem and Learning With Errors, both of which remain resistant even under quantum computation models.

A notable strength of lattice-based methods is their adaptability across multiple cryptographic functions, including encryption, key exchange, and digital signatures. Algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium demonstrate practical performance while maintaining high security, which has led to their selection in standardization efforts [10], [11].

However, despite their advantages, these methods still introduce moderate increases in key sizes compared to classical systems, which must be considered during implementation.

B. Hash-Based Cryptography

Hash-based cryptographic schemes take a fundamentally different approach by deriving their security solely from the properties of cryptographic hash functions. Because hash functions are well-studied and relatively resistant to quantum attacks, these schemes offer a high level of confidence in terms of long-term security.

Signature schemes such as XMSS and SPHINCS+ are prominent examples, providing strong guarantees without relying on complex algebraic structures. However, this simplicity comes at the cost of efficiency, as hash-based signatures

tend to be significantly larger and may introduce performance limitations in bandwidth-sensitive environments [5].

C. Code-Based Cryptography

Code-based cryptography is one of the oldest approaches in PQC and is based on the computational difficulty of decoding linear error-correcting codes. The McEliece cryptosystem, in particular, has withstood extensive cryptanalysis over several decades, making it a strong candidate for long-term security.

Despite its robustness, the primary limitation of this approach lies in its extremely large public key sizes. This characteristic poses challenges for systems where memory and transmission efficiency are critical, thereby limiting its practical applicability in certain scenarios [7].

D. Multivariate Cryptography

Multivariate cryptographic systems rely on solving systems of nonlinear polynomial equations, a problem that is computationally intensive and difficult to reverse. These schemes are attractive due to their fast execution times, especially in signature generation.

However, the security of multivariate approaches has been inconsistent, with several proposed schemes being broken over time. This has led to cautious adoption, where only carefully analyzed constructions are considered viable for real-world deployment [9].

E. Isogeny-Based Cryptography

Isogeny-based cryptography explores the use of mappings between elliptic curves to construct secure cryptographic systems. Initially, this approach gained attention due to its relatively compact key sizes, which offered an advantage over other PQC methods.

However, recent breakthroughs in cryptanalysis have exposed weaknesses in certain isogeny-based protocols, significantly reducing their reliability. As a result, their role in the future PQC landscape remains uncertain [10].

F. Comparative Analysis of PQC Techniques

From a broader perspective, no single PQC technique satisfies all performance and security requirements. Lattice-based methods currently offer the best balance between efficiency and security, while hash-based systems provide strong theoretical assurance at the cost of size. Code-based cryptography ensures durability but struggles with scalability, whereas multivariate and isogeny-based approaches remain under active evaluation.

Table 1: Evaluation of Post-Quantum Cryptographic Algorithms

Technique	Security Basis	Advantages	Limitations
Lattice-Based	SVP, LWE	Efficient, widely adopted	Moderate key sizes
Hash-Based	Hash functions	Very strong security	Large signatures
Code-Based	Error-correcting codes	Proven long-term security	Very large keys
Multivariate	Polynomial equations	Fast computation	Security concerns
Isogeny-Based	Elliptic curve isogenies	Small key sizes	Recently broken / less secure

V. TRANSITION STRATEGIES TO POST-QUANTUM CRYPTOGRAPHY

The transition from classical cryptographic systems to Post-Quantum Cryptography (PQC) is a complex and multi-dimensional process that requires careful planning, implementation, and standardization. Unlike previous cryptographic upgrades, the shift to PQC must address not only security concerns but also compatibility, scalability, and long-term sustainability. Recent studies emphasize that a well-structured transition strategy is essential to mitigate risks associated with quantum threats while ensuring continuity of existing systems [8], [10].

A. Cryptographic Agility

Cryptographic agility refers to the ability of systems to dynamically switch between different cryptographic algorithms without significant disruption. This capability is critical in the context of PQC, as organizations must be prepared to replace vulnerable algorithms with quantum-resistant alternatives as standards evolve. Research highlights that systems lacking agility face significant challenges in adapting to new cryptographic requirements, leading to increased security risks and operational inefficiencies [10], [11].

B. Hybrid Cryptographic Approaches

One of the most practical strategies for transitioning to PQC is the adoption of hybrid cryptographic systems, which combine classical and post-quantum algorithms. In this approach, both classical and PQC-based encryption or signature mechanisms are applied simultaneously, ensuring security even if one of the algorithms is compromised. Hybrid solutions are particularly useful during the transition phase, as they provide backward compatibility while enabling gradual adoption of PQC technologies [7], [9].

C. Incremental Migration Strategies

A phased or incremental migration approach is widely recommended for deploying PQC in real-world systems. This involves gradually replacing classical cryptographic components with quantum-resistant alternatives rather than performing a complete system overhaul. Key steps include identifying critical assets, prioritizing high-risk systems, and implementing PQC in stages. Such an approach minimizes operational disruptions and allows organizations to evaluate performance and security impacts during the transition [8].

D. Standardization and Policy Frameworks

Standardization plays a crucial role in ensuring interoperability and widespread adoption of PQC algorithms. Efforts led by the National Institute of Standards and Technology have accelerated the development and evaluation of quantum-resistant cryptographic standards. In addition to technical standards, policy frameworks and regulatory guidelines are essential for guiding organizations in adopting PQC solutions, particularly in critical sectors such as finance, healthcare, and government systems [10].

E. Infrastructure and Implementation Considerations

The successful deployment of PQC requires significant changes to existing infrastructure, including hardware, software, and network protocols. A significant number of post-quantum cryptographic (PQC) schemes require comparatively large key sizes and increased computational effort, which may affect overall performance and system efficiency. These demands become more problematic in environments with limited resources, such as Internet of Things (IoT) devices and embedded platforms. [9], [11].

VI. CHALLENGES IN POST-QUANTUM CRYPTOGRAPHY ADOPTION

Despite significant advancements in Post-Quantum Cryptography (PQC), its widespread adoption presents numerous technical, operational, and security challenges. While PQC algorithms are designed to resist quantum attacks, their integration into existing systems is far from straightforward. Recent research highlights that these challenges must be carefully addressed to ensure a secure and efficient transition to quantum-resistant cryptographic infrastructures [8], [11].

A. Increased Key Sizes and Storage Overhead

One of the primary challenges associated with PQC algorithms is the significantly larger key sizes compared to classical cryptographic schemes. For example, code-based and lattice-based cryptographic systems often require keys that are several times larger than those used in RSA or ECC. This increase in key size leads to higher storage requirements and increased bandwidth consumption during transmission, which can be problematic for large-scale and resource-constrained systems [9].

B. Computational Complexity and Performance Overhead

PQC algorithms typically involve more complex mathematical operations, resulting in increased computational overhead. This can impact system performance, particularly in applications requiring real-time processing, such as secure communications and financial transactions. Studies indicate that while some PQC algorithms are optimized for performance, achieving a balance between security and efficiency remains a major challenge [11].

C. Compatibility with Legacy Systems

Integrating PQC into existing infrastructure poses significant compatibility challenges. Current systems, protocols, and applications are designed to work with classical cryptographic algorithms, and replacing them with PQC solutions may require extensive modifications. This is especially challenging in large-scale systems where backward compatibility and interoperability are critical requirements [10].

D. Challenges in Resource-Constrained Environments

The deployment of PQC in resource-constrained environments, such as Internet of Things (IoT) devices and embedded systems, presents additional difficulties. Limited processing power, memory, and energy resources make it challenging to implement PQC algorithms efficiently. Recent studies emphasize the need for lightweight PQC solutions tailored to such environments [9], [8].

E. Security Uncertainty and Cryptanalysis

Unlike classical cryptographic algorithms, which have been extensively analyzed over decades, many PQC schemes are relatively new and may not yet be fully

tested against all possible attack vectors. Recent cryptanalysis efforts have exposed vulnerabilities in certain candidate algorithms, raising concerns about their long-term security. This uncertainty necessitates continuous evaluation and validation of PQC algorithms before widespread adoption [10].

F. Standardization and Adoption Barriers

Although standardization efforts have made significant progress, global adoption of PQC is still in its early stages. Differences in regulatory policies, lack of awareness, and the absence of clear migration guidelines can slow down the transition process. Additionally, organizations may be hesitant to adopt new cryptographic systems due to concerns about cost, complexity, and potential risks associated with early implementation [8], [11].

VII. FUTURE DIRECTIONS IN POST-QUANTUM CRYPTOGRAPHY

As the field of Post-Quantum Cryptography (PQC) continues to evolve, several research directions have emerged to address existing limitations and enhance the practical deployment of quantum-resistant cryptographic systems. While current PQC algorithms provide a strong foundation, ongoing advancements are necessary to improve efficiency, scalability, and long-term security. Recent studies emphasize that future research must focus on optimizing implementations, strengthening security guarantees, and enabling seamless integration into modern digital infrastructures [8], [2].

A. Development of Lightweight PQC Algorithms

A major focus of current research is designing lightweight post-quantum cryptographic (PQC) methods that can operate effectively in constrained environments such as Internet of Things (IoT) devices, embedded hardware, and mobile systems. Many existing PQC approaches demand considerable processing power and memory, which limits their practicality in these resource-limited settings. Future work aims to design optimized algorithms that maintain strong security while reducing computational and storage overhead [9].

B. Integration with Emerging Technologies

The integration of PQC such as artificial intelligence (AI), blockchain, and cloud computing presents a promising research direction. Combining PQC with AI-driven cybersecurity solutions can enhance threat detection and response mechanisms. Similarly, developing quantum-resistant blockchain frameworks is essential to ensure the long-term security of decentralized systems. Research also focuses on incorporating PQC into cloud infrastructures to provide secure data storage and communication in the quantum era [9].

C. Hardware Acceleration and Optimization

To address performance challenges, future research is exploring hardware-based optimizations for PQC algorithms. This includes the use of specialized processors, field-programmable gate arrays (FPGAs), and application-specific integrated circuits (ASICs) to accelerate cryptographic operations. Efficient hardware implementations can significantly improve the feasibility of deploying PQC in high-performance and real-time applications [11].

D. Cryptographic Agility and Automated Migration

Enhancing cryptographic agility remains a critical area of focus for future systems. Research is directed toward developing automated tools and frameworks that enable dynamic switching between cryptographic algorithms without disrupting system operations. Such solutions will facilitate seamless migration from classical to post-quantum cryptography and ensure adaptability to evolving security requirements [10], [6].

E. Global Standardization and Policy Development

While standardization efforts have made significant progress, achieving global consensus on PQC adoption remains an ongoing challenge. Future work must focus on harmonizing international standards, developing clear migration guidelines, and promoting awareness among stakeholders. Collaboration between governments, industry, and academia is essential to establish robust policy frameworks that support secure and efficient PQC deployment [8], [2].

F. Long-Term Security and Cryptanalysis

Ensuring the long-term security of PQC algorithms is a fundamental research challenge. Continuous cryptanalysis is required to evaluate the resilience of these algorithms against both classical and quantum attacks. Future research must focus on identifying potential vulnerabilities, improving security proofs, and developing adaptive cryptographic schemes that can withstand evolving threat landscapes [10].

VIII. CONCLUSION

The rapid advancement of quantum computing presents a significant challenge to the security of classical cryptographic systems that underpin modern digital infrastructure. As demonstrated in this paper, widely used cryptographic algorithms are vulnerable to quantum attacks, particularly due to the capabilities of Shor's Algorithm and Grover's Algorithm, which threaten both public-key and symmetric encryption schemes. These developments highlight the urgent need for transitioning toward quantum-resistant security mechanisms.

This paper has provided a comprehensive review of Post-Quantum Cryptography (PQC), covering its fundamental techniques, including lattice-based, hash-based, code-based, and multivariate cryptographic approaches. It also examined the critical role of standardization initiatives led by the National Institute of Standards and Technology in guiding the development and adoption of secure PQC algorithms. Furthermore, the study analyzed various transition strategies, such as cryptographic agility, hybrid cryptographic systems, and phased migration approaches, which are essential for enabling a smooth transition from classical to quantum-resistant infrastructures.

Despite the promising advancements in PQC, several challenges remain, including increased key sizes, computational overhead, compatibility issues, and security uncertainties. These challenges indicate that the transition to PQC is not merely a technological upgrade but a complex transformation that requires coordinated efforts across multiple domains. Addressing these issues is critical to ensuring the successful deployment of PQC in real-world applications.

Looking forward, future research must focus on developing efficient, scalable, and lightweight PQC solutions, particularly for resource-constrained environments.

Additionally, advancements in hardware optimization, integration with emerging technologies, and continuous cryptanalysis will play a vital role in strengthening the security and practicality of PQC systems. Global collaboration among academia, industry, and regulatory bodies will be essential to establish unified standards and accelerate adoption.

In conclusion, Post-Quantum Cryptography represents a crucial step toward securing digital systems in the quantum era. Proactive adoption of PQC, supported by robust transition strategies and ongoing research, is necessary to safeguard sensitive information against emerging quantum threats and to ensure the long-term resilience of cybersecurity infrastructures.

REFERENCES

- [1] N. Lohmiller et al., —A Survey of Post-Quantum Cryptography Migration in Vehicles,| IEEE Access, 2025.
- [2] C. O. Sakwa, —Survey on Post-Quantum Cryptography Implementations and Deployment Challenges,| Future Generation Computer Systems, 2026.
- [3] P. W. Shor, —Algorithms for quantum computation: discrete logarithms and factoring,| 694.
- [4] L. K. Grover, —A fast quantum mechanical algorithm for database search,| 696.
- [5] O. Egbuagha et al., —Post-Quantum Cryptography in Practice: A Literature

Review, IACR, 2025.

[6] S. Y. Chang, —Post-Quantum Cryptography in Networking Protocols, I 2026.

[7] M. A. Khan et al., —Implementation of PQC in Consumer Electronics, I 2025.

[8] Y. Hanna et al., —Performance Evaluation of PQC for IoT Devices, I 2025.

[9] A. Al Mamun et al., —PQC for Intelligent Transportation Systems, I 2026.

[10] National Institute of Standards and Technology (NIST), —PQC Standardization, I 2022–2025.

[11] S. Ahmadunnisa et al., —Hardware Implementations of PQC, I 2025.