Fortifying Future IoT Security: A Comprehensive Review on Lightweight Post-Quantum Cryptography

Liyth H. Mahdi
College of Information Technology, Department of Information Networks, University of Babylon, Babil, Iraq
liythhaiderm.net@student.uobabylon.edu.iq (corresponding author)

Alharith A. Abdullah
College of Information Technology, Department of Information Network, University of Babylon, Babil, Iraq
alharith@uobabylon.edu.iq

Received: 6 January 2025 | Revised: 1 February 2025 | Accepted: 5 February 2025

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: https://doi.org/10.48084/etasr.10141

ABSTRACT

This paper presents lightweight Post-Quantum Cryptography (PQC), identifying its importance for a shift from traditional cryptographic schemes, vulnerable to quantum threats, to efficient PQC algorithms. Lattice-based cryptography stands out owing to its small key sizes and computational efficiency, with CRYSTALS-Kyber and NTRU algorithms being substantial representatives for Internet of Things (IoT) applications. However, PQC implementation in IoT environments has various obstacles to overcome. Minimizing energy consumption, scalability, and hardware limitations remain key challenges for PQC smooth integration into these resource-constrained networks. The present review analyzes the state-of-the-art PQC, makes security and performance comparisons among leading algorithms, and evaluates optimization techniques aimed at reducing resource overheads. Algorithmic refinement, hardware acceleration, and hybrid cryptography are also discussed as methods for mitigating these challenges. The results indicate that continuous research and development efforts should be made to improve the PQC technologies, and thus achieve their practical deployment in IoT systems. Quantum threats in IoT will be, hence, prevented with the employment of secure and scalable IoT ecosystems in a post-quantum world.

Keywords-post-quantum cryptography; IoT security; lightweight cryptography; quantum-resistant algorithms; lattice-based cryptography; resource-constrained devices

I. INTRODUCTION

The sudden growth in IoT marked a revolutionary end to traditional industries, including healthcare, manufacturing, smart cities, and industrial automation, enabling billions of devices to be interconnected. On the negative side, this unprecedented growth has resulted in a number of critical security vulnerabilities, since many of these IoT devices are inherently resource-constrained, and their operations rely on lightweight cryptographic protocols [1]. These limitations make IoT systems particularly vulnerable to cyberattacks, especially in the face of the looming threat of quantum computing. Traditional cryptographic methods, such as RSA and ECC, will become obsolete in the quantum era due to quantum algorithms, like Shor's, which can efficiently solve the mathematical problems those methods rely on [2].

To alleviate these challenges, Post-Quantum Cryptography (PQC) has come out as one of the most important research areas in which NIST takes part by standardizing quantum-resistant cryptographic algorithms [1, 3]. Among these algorithms, lattice-based cryptography, code-based cryptography, and multivariate polynomial-based cryptography have gathered great attention due to their resistance against quantum attacks [4, 5]. However, most PQC algorithms are computational-resource-intensive, and hence may not be properly adapted to the resource-constrained IoT devices, where energy efficiency, processing power, and memory usage have to be considered [1, 4]. This has motivated the creation of lightweight PQC algorithms specifically designed to secure IoT environments without compromising the cryptographic strength against quantum threats [6].

This review is intended to deliver an in-depth analysis with respect to lightweight PQC and its application in IoT environments. Its contribution will spare special attention to the security versus performance trade-off concerning resource consumption in several PQC implementations for constrained devices. It will also offer a proper comparison of the leading PQC families emerging from the standardization process of NIST, highlighting the strong and weak points concerning IoT security. In particular, this work will deeply explore the lattice-based cryptographic algorithms of CRYSTALS-Kyber and NTRU, which have demonstrated great promise in balancing security with efficiency [4, 7].

In the last few years, a great amount of research has been conducted on developing PQC algorithms, considering their applicability to constrained environments, like IoT. Authors in [2] investigated PQC solutions against the quantum-era vulnerabilities of IoT devices. They mainly focused on the layered architecture and security requirements of IoT while highlighting challenges related to its resource-constrained nature. Efficiency, scalability, and quantum resilience were emphasized when lattice-based cryptosystems were reviewed. A sensitive classification for the constrained IoT devices was proposed and cryptosystem efficiency was defined with respect to these devices' limitations. The role of lattice-based solutions in securing IoT against evolving quantum threats was stressed along with the need for future research.

Authors in [8] explored lattice-based cryptography as a PQC solution for IoT devices. They covered mathematical underpinning, including LWE and NTRU, within the context of its suitability for lightweight cryptographic applications, considering specific security challenges met in IoT. The paper discussed hardware and software strategies for implementation taking into account energy efficiency, scalability, and quantum attack resilience. It concluded by advocating LBC as a leading candidate to secure IoT in the quantum era due to its adaptability and worst-case security assurances. Authors in [9] examined the suitability of PQC in IoT. Since quantum computing is already threatening classical cryptographic systems that utilize algorithms such as Shor's, this study limited its investigation to two NIST-standard PQC contenders: CRYSTALS-KYBER and NTRU. An IoT prototype system was tested in terms of performance metrics: CPU, memory, and network usage. The results designated Kyber512 and LightSaber as the most viable options due to their very low computational requirements and memory efficiency. Energy-performance trade-offs were provided, demonstrating how PQC can be securely and efficiently deployed in IoT devices. Authors in [10] explored the implications of quantum computing to traditional cryptographic methods and introduced PQC. An overview of the PQC algorithms was provided, with a particular focus on CRYSTALS-KYBER, which is robust against quantum attacks due to grounding in lattice-based cryptography. The review covered the PQC development, from theoretical work to its practical application, concentrating on NIST's role in PQC standardization. Challenges regarding implementation efficacy and security validations were also analyzed. It was concluded that PQC can be applied by default in secure communications, especially in areas such as IoT and critical domains with data sensitivity, to enable resilience. Authors in [11] addressed the integration of PQC methods within IoT, with a particular focus on resource-constrained devices. The recent advances in PQC, particularly lattice-based cryptography, were evaluated as solutions to the vulnerabilities brought in by quantum computing. A performance evaluation of various PQC algorithms in IoT contexts was performed and possible strategies to optimize both software and hardware implementations were discussed. It was found that although some results are very promising, such as those concerning CRYSTALS-Kyber, there are still standardization and scalability issues that need to be overcome. The necessity to tune IoT security to the current NIST PQC standardization for future-proof robust security was underlined. Authors in [12] explained how cryptography keeps developing to withstand both quantum and classical computations. The cryptographic systems were classified as lattice-based, hash-based, and code-based cryptosystems. It was determined that NIST played the most crucial role in each class, providing post-quantum standards. The mathematical fundamentals of modular arithmetic and lattice structures were investigated and algorithms, such as NTRU, Ring-LWE, and McEliece, were reviewed. It was concluded that, even though lattice-based methods may be promising in constrained settings, further research is required to establish whether these schemes are superior for post-quantum security.

II. COMPARATIVE ANALYSIS OF POST-QUANTUM CRYPTOGRAPHIC TECHNIQUES FOR IOT APPLICATION

This section presents the results of an extended comparative review on various post-quantum cryptographic algorithms. Their methodologies, results, and limitations are assessed for their relevance in safeguarding resource-constrained IoT devices against quantum computing threats. The insights drawn concern algorithm efficiency, implementation challenges, and compliance with the evolving cryptographic standards. Table I presents the analysis results of the reviewed papers. This review underlines the growing body of research that surrounds lightweight PQC in IoT environments, emphasizing how security is balanced with performance in resource-constrained settings. Several studies have illustrated how PQC, while offering strong security, needs further optimization so that it can be applied to real-world use.

III. POST-QUANTUM CRYPTOGRAPHY OVERVIEW

Since quantum computers are increasing their power, classical cryptographic systems could be endangered. RSA and Elliptic Curve Cryptography are usual classic encryption algorithms, based on the hardness of the integer factorization problem and discrete logarithm problems, intractable for a classic computer. For a quantum computer, such tasks are feasible thanks to Shor's algorithm, which indirectly renders conventional cryptography vulnerable to quantum attacks [12, 19]. This challenge leads to the development of PQC, which is resistant against both classical and quantum computing attacks. PQC represents several families of cryptographic algorithms based on problems which remain hard to solve even for quantum computers. NIST has spearheaded efforts to standardize the PQC algorithm through a multi-round process which evaluates security, performance, and scalability of different approaches. In the last few rounds, NIST identifies a number of promising algorithm families, including lattice-based, code-based, multivariate, and hash-based [1, 20]. Figure 1 illustrates four different cryptographic approaches.

TABLE I. REVEWED PAPER ANALYSIS

Ref / Year	Problem statement	Post quantum families used	Presented Scheme	Advantages	Limitations
[13] 2017	IoT security systems based on classical cryptography are vulnerable to quantum computing.	Hash-Based Code-Based Lattice-Based Multivariate Polynomial Isogeny-Based	Proposes integrating quantum-resistant cryptography into existing IoT architectures to mitigate future risks.	Demonstrates the feasibility of PQC in IoT using lattice-based cryptography.	Scalability of PQC solutions in large IoT networks remains a challenge.
[14] 2022	IoT communication channels are vulnerable to advanced attacks, like Mirai botnet, demanding innovative PQC methods.	Isogeny-Based Hash-Based Lattice-Based	Introduces the Diffie Supersingular Multiplication (DSM) model to secure IoT communication, validated using Mirai botnet attacks and Xilinx ISE14.5.	DSM enhances frequency by 30%, reduces area by 24%, and achieves a 10% error reduction compared to traditional methods.	DSM implementation lacks generalizability beyond the tested IoT environments and requires further exploration of scalability in diverse setups.
[4] 2022	IoT edge devices face challenges in implementing cryptographic schemes due to limited resources and energy constraints.	Lattice-Based	Implements NTRU In IoT nodes using Contiki-NG OS, optimizing key generation, encryption, and decryption on resource-constrained hardware.	NTRU is suitable for modern microcontrollers, but its memory and energy demands are excessive for older IoT platforms.	Focus on specific hardware (ARM Cortex-M4), lacks generalizability to all IoT environments, and excludes real-world network-level challenges.
[15] 2022	The advent of quantum computing threatens classical cryptographic algorithms, necessitating the exploration and standardization of quantum-resistant cryptosystems.	Lattice-Based Hash-Based Code-Based Multivariate Polynomial Isogeny-Based Non-Commutative	Reviews various cryptographic families, like lattice-based, hash-based, and multivariate cryptography, and discusses the NIST standardization efforts and challenges.	Highlights advancements in lattice cryptography, isogeny-based systems, and hash-based signatures. Analyzes NIST's final round candidates for post-quantum standards.	Focuses on theoretical and computational aspects, with limited insights into real-world scalability and diverse environmental conditions.
[16] 2023	IoT-enabled cloud systems face scalability and security challenges due to classical cryptography.	Lattice-Based	Proposes a hybrid PQC and blockchain-based secure cloud architecture for IoT systems.	Significant performance gains in scalability and security metrics compared to traditional models.	The hybrid approach may introduce computational overhead in larger cloud systems.
[6] 2024	Traditional signatures lack long-term security for MIoT and are vulnerable to quantum threats.	Hash-Based	Proposes INF-HORS, a lightweight PQ digital signature that does not require hyper-trees and minimizes cryptographic overhead.	Achieves 20× faster signature generation and smaller signature sizes compared to BLISS-I.	May not be suitable for all PQC applications due to specific optimizations for MIoT.
[3] 2024	Lattice-based PQC schemes are resource-intensive for IoT devices with constrained power and efficiency.	Lattice-Based	Introduces a customized SIMD architecture with fine-grained parallelism for efficient LBC operations.	Achieves 10× speedup over RISC-V and 5× over ARM Cortex-M4 implementations for CRYSTALS-Kyber and CRYSTALS-Dilithium schemes.	Limited to LBC schemes and might not be extendable to other PQC schemes without modification.
[1] 2024	Evaluating PQC algorithms' performance on low-power devices is necessary for secure IoT environments.	Lattice-Based Code-Based Hash-Based Isogeny-Based	Benchmarked NIST PQC candidates on Raspberry Pi 4 to simulate IoT conditions.	CRYSTALS-Kyber and CRYSTALS-Dilithium are the most efficient algorithms for key encapsulation and signatures.	Limited to Raspberry Pi, not representative of all constrained devices in IoT.
[5] 2024	The need for efficient hardware implementations of lattice-based PQC algorithms for embedded systems.	Lattice-Based	Presents a TTA-based ASIP design with hardware accelerators for CRYSTALS-Kyber, Saber, and NewHope algorithms.	Demonstrates greater efficiency and performance than existing RISC-V cores.	Only evaluates FPGA and ASIC platforms; limited testing on actual IoT devices.
[17] 2024	Quantum computing threatens existing IoT security models; need for PQC solutions.	Lattice-Based	Develops SSI-PQM, integrating NTRU-based PQC with a MACsec-secured IoT platform.	SSI-PQM improves performance over RSA by 161%, ensuring secure IoT communications.	Limited to NTRU-based PQC; additional PQC algorithms may need to be integrated for broader application.
[18] 2024	RSA and ECC are vulnerable to quantum attacks, necessitating post-quantum algorithms for secure signatures.	Lattice-Based Hash-Based	Post-quantum algorithms CRYSTALS-Dilithium, Falcon, and SPHINCS+ are evaluated for key generation, signing, and verification, using the liboqs library.	Post-quantum algorithms, like CRYSTALS-Dilithium, excel in key generation, Falcon offers compact signatures, SPHINCS+ ensures flexibility but slower speeds.	Limited hardware setups, few algorithm candidates evaluated, lacks real-world validation against quantum attacks.
[7] 2024	Developing resource-efficient, secure implementations of CRYSTALS-Kyber for constrained devices to counter quantum threats.	Lattice-Based	Optimizes CRYSTALS-Kyber using modular arithmetic, polynomial multiplication, and lightweight hash modules, tailored for ASICs and FPGAs.	Resource-efficient design using minimal LUTs, FFs, and BRAMs, achieving high performance (244 MHz) on constrained hardware.	Focus on FPGA prototypes, limited hardware applicability, and emphasis on resource efficiency over extensibility.

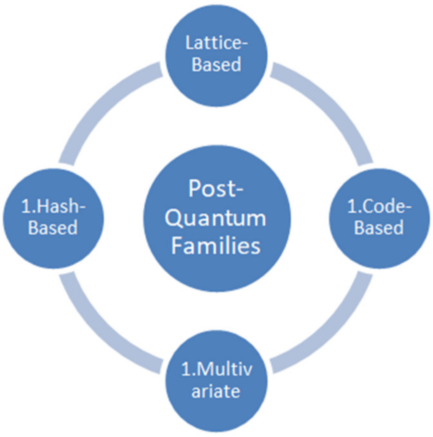

Fig. 1. PQC families.

A. *Lattice-Based Cryptography*

Lattice-based cryptography used to be in the spotlight as one of the most promising PQC approaches. It relies on mathematical problems, including SVP and LWE, which are believed to remain resistant against quantum computers [4, 12]. Among the most representative lattice-based schemes, in their current state, are the ones chosen for key encapsulation in CRYSTALS-Kyber and for digital signatures in CRYSTALS-Dilithium by NIST for the second round, due to their strong security properties, including efficiency in constrained environments [3]. In particular, lattice-based cryptography is rather suitable for IoT devices due to its flexibility within the security-performance-resource consumption trade-off. Owing to the nature of the problems, it allows for the elaboration of algorithms that require smaller key sizes and faster computation compared to several other post-quantum alternatives, which are particularly relevant in resource-constrained environments, such as IoT [4].

B. *Code-Based Cryptography*

Code-based cryptography is one of the oldest post-quantum approaches, relying on problems that involve decoding a random linear code, well beyond the powers of even quantum computers. The McEliece cryptosystem is among the most representative schemes in this class and to this date, having resisted all classical and quantum attempts of attack [5]. Most of the cryptographic schemes based on these codes suffer from big key-size problems, negatively affecting the memory and storage of all kinds of resource-restricted IoT devices [1].

C. *Multivariate Cryptography*

Multivariate cryptography is based on the difficulty of solving systems of multivariate polynomial equations over finite fields. These problems are very hard to solve and, hence, this cryptography type is one of the strongest candidates for post-quantum security. However, similar to code-based cryptography, multivariate schemes are often very inefficient with respect to key sizes and computational overhead, which makes them unsuitable for most constrained applications [15].

D. *Hash-Based Cryptography*

Hash-based cryptography provides a very secure and efficient way of generating digital signatures. Schemes, like the Merkle Signature Scheme (MSS) and Leighton-Micali Signature Scheme (LMS), provide quantum-resistant security based on the properties of cryptographic hash functions, which are not easily inverted by quantum algorithms [9, 13] Hash-based signatures are computationally efficient with relatively small key sizes, which makes them a potential option for utilization in IoT applications. However, most of these schemes normally suffer from state management issues, rendering them complex for large-scale deployment [8].

In summary, PQC can be achieved by different means in order to provide protection for the digital communications threatened by quantum computing. However, such techniques would largely differ in efficiency with respect to the use case and system limitations. Among these methods, in IoT applications, where most devices are always bounded in processing power, memory, and energy consumption, lattice-based cryptography is envisaged as the most promising one due to its efficient balance between security and performance [4, 12].

IV. EXPLORING POST-QUANTUM CRYPTOGRAPHY: TECHNIQUES, SECURITY, AND EFFICIENCY

In this section, different PQC techniques are examined in terms of mathematical grounds, security guarantees, and deployability in resource-constrained settings, like IoT. The comparison is carried out concerning computational efficiency, memory, key size, and security.

A. *Lattice-Based Cryptography*

Lattice-based cryptography is one exciting and well-thought-of area in PQC considering efficiency and security. It depends on the hardness of problems related with high-dimensional lattices, such as SVP, CVP, and LWE. These problems are considered infeasible even by a quantum computer, therefore making lattice-based cryptographic schemes strong candidates in post-quantum security [1, 20].

1) *Key Encapsulation Mechanism (KEM)*

The KEM forms the basis of secure communication between devices. Among the most viable variants of KEMs are the lattice-based ones, such as CRYSTALS-Kyber, which excel in efficiency due to their small key sizes and fast operations. For instance, CRYSTALS-Kyber utilizes the LWE problem and polynomial arithmetic over a finite field to generate keys. The NIST-selected version features an approximate public key size of 800-1,184 bytes, enabling very fast operations for encryption and decryption. Compared to most post-quantum schemes, superior performance is achievable due to its extreme speeds and resource efficiency [3]. The small key sizes are an important factor in IoT-related applications, since bandwidth and memory are limited. The key encapsulation mechanisms are depicted in tabular form in Table II. CRYSTALS-Kyber strikes a perfect balance between security and efficiency in computation. Therefore, it is ideal for constrained IoT devices, [4].

TABLE II. KEY ENCAPSULATION MECHANISMS

Algorithm	Public key size (bytes)	Ciphertext size (bytes)	Security level
CRYSTALS-Kyber	800-1,184	768-1,088	NIST Level 1
NTRU	930-1,230	750-1,020	NIST Level 1

2) Digital Signatures

Lattice-based schemes also enable the construction of post-quantum digital signatures. Among them, the digital signature algorithm CRYSTALS-Dilithium is based on the hardness of the Module Learning With Errors problem, a variant of the LWE problem that advances security. CRYSTALS-Dilithium enjoys the smallest signature sizes of 1,700-2,500 bytes and faster signing/verification times compared to its competitors, which makes it highly attractive for IoT applications, where large signatures could be prohibitive due to bandwidth and processing limitations [4, 5]. Other notable algorithms are Falcon and SPHINCS+. Similar to CRYSTALS-Dilithium, Falcon is lattice-based, thus allowing for very compact signature sizes. However, Falcon's performance in more resource-constrained environments, such as IoT, has not been fully assessed given its more complex structure. Table III shows a comparison of signature algorithms' signature and key sizes.

TABLE III. SIGNATURE ALGORITHMS

Signature algorithm	Signature size (bytes)	Key size (bytes)
CRYSTALS-Dilithium	1700-2500	2400-3800
Falcon	1200-1700	800-1200
SPHINCS+	32000	16-48

3) Security Strengths

The current power of the lattice-based cryptography is essentially based on the inherent difficulties of lattice-related problems. Given the lattice structure, even with quantum computers, solving problems, such as LWE or SVP, requires exponentially large computational resources compared to what is feasible nowadays, making lattice-based cryptography one of the best options to secure IoT communications, ranging from classical to quantum adversaries [20].

B. Code-Based Cryptography

Code-based cryptography is one of the oldest and best-studied PQC techniques. This method is based on the hardness of decoding random linear codes, a problem that is difficult for both classical and quantum computers to solve. The McEliece cryptosystem, invented back in the late 1970s, is still considered one of the most robust and resilient code-based schemes [5].

1) Key Sizes and Performance

The major disadvantage of code-based cryptography, and especially McEliece, is the key size. Public keys can have sizes up to a few megabytes, making them less appropriate for IoT devices, given the strict memory and bandwidth constraints [1]. Table IV illustrates the typical key sizes for McEliece. Despite these large key sizes, code-based cryptosystems are highly secure, offering excellent resistance against both classical and quantum attacks. However, their heavy resource consumption tends to be a limiting factor for allowing their implementations in resource-constrained settings, like IoT [1].

TABLE IV. MCELIECE KEY SIZES

Algorithm	Public key size (MB)	Private key size (KB)
McEliece (classic)	1-3	50-60

C. Multivariate Public Key Cryptography (MPKC)

MPKC is based on the hardness of solving systems of multivariate quadratic equations over finite fields. Multivariate schemes are considered efficient regarding the signature size and computational cost, which makes them suitable for lightweight applications, like IoT. On the other hand, their security has been questioned because several schemes have been broken over the last few years [9, 15].

1) Multivariate Signature Schemes

The most famous multivariate scheme, Rainbow, was a candidate in the NIST process for PQC standardization. It offers small signature sizes and relatively fast operations. However, recent cryptanalysis puts its long-term security into doubt [9]. Typical metrics for multivariate cryptosystems are listed in Table V.

TABLE V. SIGNATURE SIZE

Algorithm	Signature size (bytes)	Security level
Rainbow	66-130	NIST level 1-3
GeMSS	128-256	NIST level 1-3

D. Hash-Based Cryptography

Hash-based cryptography has gained predominance due to its simple and highly secure structure. Merkle Tree Signatures and LMS are just examples of hash-based digital signatures whose security depends on the cryptographic properties of hash functions [8].

1) Efficiency and Security

Besides efficient, hash-based signatures are highly secure in the case of low-size data transmissions and hence suitable for IoT applications where secure low bandwidth utilization is a big concern. On the other side, one of the major disadvantages of the hash-based cryptography is its stateful nature. In stateful schemes, successful management of the secret keys is required. This further complicates their deployment in large-scale IoT networks requiring secure managing of millions of devices [8]. Table VI demonstrates the signature and key size.

TABLE VI. SIGNATURE AND KEY SIZE

Signature algorithm	Signature size (bytes)	Key size (bytes)
LMS	64	32-64
XMSS	50	16-32

E. Key Size

Figure 2 represents the public key sizes of several PQC algorithms. Public key size is important when implementing cryptography with resource-constrained devices. The larger the key size is, the more memory is required, and the more bandwidth will be used. Thus, the key takes more time to transmit, which can negatively influence performance in some systems, usually by low-power or low-bandwidth means.

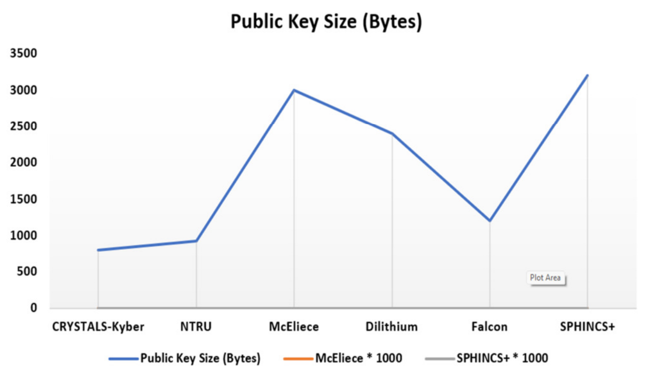

Fig. 2. Public key size comparison.

1) *CRYSTALS-Kyber*

- Public Key Size: 800 bytes
- Significance: CRYSTALS-Kyber has one of the smallest key sizes amongst all the lattice-based PQC schemes. Thus, it should be an excellent candidate for IoT applications. A nice balance between small key size and security is one of the main reasons it was selected by NIST for post-quantum standardization.

2) *NTRU*

- Public Key Size: 930 bytes
- Significance: NTRU is a lattice-based algorithm that provides slightly larger key sizes compared to CRYSTALS-Kyber, but still efficient for use in constrained environments. NTRU has been very well studied and provides sufficient security against both classical and quantum attacks, making it a good fit for IoT deployment, where both memory efficiency and security are matters of concern.

3) *McEliece (Classic)*

- Public Key Size: 3 MB
- Significance: McEliece is a code-based cryptosystem which offers very strong security. In contrast, it has a huge key size of 3 MB, which is challenging to use in IoT devices. The key size for McEliece makes it impracticable for many resource-constrained systems despite its high security level.

4) *CRYSTALS-Dilithium*

- Public Key Size: 2,400 bytes
- Significance: Another lattice-based algorithm focused on digital signatures. Its public key size is larger than that of CRYSTALS-Kyber but still reasonable for most IoT devices. The strong performance of CRYSTALS-Dilithium, particularly concerning signature verification, fits very well with the secure communication of IoT.

5) *Falcon*

- Public Key Size: 1,200 bytes
- Significance: Compared to CRYSTALS-Dilithium, Falcon possesses even smaller public key sizes, rendering it highly suitable for resource-constrained environments. Compact signatures and smaller keys make Falcon a strong candidate for IoT, though, its more complex structure may render it inefficient in some implementations.

The current analysis indicates that lattice-based algorithms, like CRYSTAL-Kyber, NTRU, CRYSTALS-Dilithium, and Falcon are highly applicable in IoT environments due to their relatively small public key sizes in addition to their strong security guarantees. When choosing a PQC scheme for IoT, one needs to take into consideration both the size of the public keys and computational demands of each algorithm.

V. LIGHTWEIGHT POST-QUANTUM CRYPTOGRAPHY

Quantum computing, while rapidly developing, imposes an urgent need for hashing and cryptographic schemes that could resist quantum-attack complexity, especially within the IoT context, which inherently demands lightweight mechanisms. Lightweight PQC essentially means developing quantum-resistant cryptographic algorithms, optimized for resource-constrained environments in IoT devices. These devices are usually constrained by their processing power, memory, and battery life, hence making most of the traditional PQC schemes resource-intensive. Herein, lightweight PQC algorithms aim to realize a good level of quantum resistance at lower computational overheads, key sizes, and memory consumptions [21].

A. *Importance of Lightweight Post-Quantum Cryptography for Internet of Things*

IoT devices are usually severely limited in computation capability, memory, and energy use. In practice, these gadgets often run in places that are far away from being serviced or at locations that require ultra-low power consumption. Furthermore, they might have very small memory footprints that cannot fit large key sizes or complex cryptographic processes. Traditional PQC schemes, while keeping security intact, usually involve large keys and computationally intensive operations, which renders them inappropriate for these kinds of environments. Three major areas that the lightweight PQC scheme addresses are [21]:

- Key Size Reduction: Large key size results in greater storage. Such keys consume more time to be transmitted, which can be an issue in bandwidth-limited networks, like IoT environments.
- Computational Efficiency: PQC algorithms should be designed to operate efficiently on any low-power device without quickly draining the battery.
- Memory Usage: Lightweight PQC algorithms are designed to be highly memory-efficient. This enables their use even in the smallest IoT device, which may have only 128 KB of memory.

B. Challenges in Designing Lightweight Post-Quantum Cryptography

It is very tricky to make cryptographic algorithms quantum resistant and lightweight at the same time. In fact, post-quantum algorithms involve more complex mathematical operations compared to classical cryptography. Several challenges have to be dealt with while creating lightweight PQC for IoT devices:

1) Balancing Security and Performance

The most serious challenge in lightweight PQC is to provide a balance between security and performance. While it is true that the lattice-based cryptography, among other post-quantum algorithms, provides security against quantum attacks, these algorithms are more resource-intensive compared to classical cryptographic algorithms [22]. In most IoT devices, normally powered by a battery with very limited computational capability, this may be a big hurdle. Lightweight PQC has to make sure that the algorithms are adequately lightweight for running ın such a constrained device, yet they are able to stand up to the security level deemed necessary [2, 20]

2) Reducing Key and Signature Sizes

Large key and signature sizes are some of the major defects in most PQC schemes. Although, for example, algorithms like CRYSTALS-Kyber and NTRU have somewhat decent key sizes, other post-quantum schemes, such as McEliece in code-based cryptography, have really large keys. Their practical use in IoT is therefore not realistic. A great amount of lightweight PQC research tries to reduce key and signature size without compromising security [4, 5].

3) Efficient Energy Usage

IoT devices rely on limited battery power. Consequently, energy efficiency is a critical requirement for lightweight PQC algorithms. Most post-quantum algorithms involve complex mathematical operations compared to the classical cryptographic algorithms. For example, some of the lattice-based cryptographic algorithms require polynomial multiplications, which can be quite computationally intensive [6, 20]. Thus, lightweight PQC should reduce the number of operations.

4) Adaptability Across Platforms

The form of IoT devices ranges from simple sensors to more powerful devices, like smart home controllers. In these cases, lightweight PQC should be able to adapt to a wide variety of platforms, ranging from low-power microcontrollers to more capable processors. This often demonstrates the ability to scale cryptographic algorithms, depending on the available resources of the device, down to the most constrained devices while keeping the security intact [1, 4].

C. Lattice-Based Lightweight Post-Quantum Cryptography

Among the various families of PQC, lattice-based cryptography undoubtedly involves some of the most promising candidates for lightweight implementations, due to the fact that mathematical operations related to lattice problems, such as LWE and its variants, can be performed efficiently and scaled on constrained devices. All lattice-based schemes provide natural resistance to quantum attacks owing to the difficulty of solving lattice problems with quantum computers [22].

1) CRYSTALS-Kyber

Among the most promising lattice-based KEMs in the NIST PQC standardization process, CRYSTALS-Kyber has been designed considering both efficiency and strong quantum resistance. Depending on the environment, CRYSTALS-Kyber can be tuned to optimally balance performance and security, from 800 to 1,184 bytes. This makes it the most suitable candidate for lightweight PQC applications, while it can be efficiently run on low-power devices [4].

An additional important feature of Crystals-Kyber is that it is based on module learning with errors, which is a variation of the LWE problem and allows the use of even smaller key sizes, along with faster computations. This renders it highly applicable for IoT devices that have very restricted resources in terms of memory and computational power.

2) NTRU

NTRU is another lattice-based cryptographic scheme that has been optimized for usage in constrained environments. Its key sizes are similarly small, about 930 bytes, thus having very fast encryption and decryption. This scheme's security comes from the hardness of the N-th degree truncated polynomial ring problem and remains infeasible even to quantum computers [4]. Another important advantage of NTRU is its rather low memory and computational requirements. This renders it a strong candidate for lightweight PQC, especially in IoT applications. NTRU has shown good performance on low-power devices. As a result, it becomes practical when it comes to securing IoT networks.

D. Optimization Techniques for Lightweight Post-Quantum Cryptography

Various optimization techniques have also been proposed to further reduce the computational and memory overheads of PQC algorithms. The former, therefore, make PQC more viable within constrained environments, such as IoT:

1) Polynomial Approximation and Compression

The operations performed within lattice-based cryptography, like polynomial multiplication, are typically costly. Approximating polynomial operations through simpler arithmetic is one method to reduce this type of complexity, saving cycles, and so time and energy [5]. In addition, this allows numerous other techniques, like polynomial compression-only a subset of coefficients is employed in the polynomial for encryption and decryption-to save memory.

2) Algorithmic Simplification

Computational complexity can also be reduced by simplifying some of the underlying cryptographic algorithms. An indicative example is found in some variants of lattice-based cryptography, where fewer matrix multiplications are required during key exchange, hence reducing the energy and time needed to perform cryptographic operations [1].

3) Hardware Acceleration

Most IoT devices are designed with special hardware that allows acceleration for specific cryptographic operations. For example, polynomial multiplication or matrix operation support within hardware drastically cut down on the computational overhead of lattice-based cryptography. This form of hardware acceleration will enable lightweight PQC schemes to perform more powerfully on constrained devices without always draining their battery life or requiring more memory [4, 6].

E. Applications of Lightweight Post-Quantum Cryptography in Internet of Things

Certain major applications of lightweight PQC in IoT include healthcare, industrial automation, and smart city infrastructure. In such contexts, lightweight PQC makes sure that the data transmitted among various devices remain confidential, integrity is ensured, and authenticity is maintained. As a simple use case, one could secure the communication of medical devices to cloud servers with lightweight PQC to keep sensitive patient data safe from quantum-enabled adversaries [6]. Lightweight PQC can be employed to secure sensors to controller communications in industrial IoT. In this case, even when quantum computing threats become real, the command-and-control systems are guaranteed to remain safe. Lightweight PQC, due to its low overhead, is suitable for applications where high throughput and/or low latency are critical performance metrics [5]. Lightweight PQC is an effective augmentation of cryptography. The challenge beneath it is unique, providing security for IoT devices in the quantum world. By mainly aiming at the key size reduction, computational efficiency, and optimization of memory, the lightweight PQC ensures that resource-constrained environments have quantum-resistant security. Indicative examples are the CRYSTALS-Kyber and NTRU, which are the leading candidates of lattice-based schemes of lightweight PQC, balancing security with performance. It is expected that there will be a focus on different optimizations and hardware-based accelerations that are competitive enough for the deployment of lightweight PQC in diverse IoT devices.

VI. CHALLENGES AND FUTURE DIRECTIONS

The adoption of lightweight PQC in IoT environments faces many challenges due to the resource-constrained nature characterizing IoT devices and the inherently complex nature of post-quantum cryptographic algorithms.

A. Challenges in Lightweight Post-Quantum Cryptography Implementation

1) Resource Constraints in Internet of Things Devices

One of the major challenges to deploying PQC in IoT environments is the resource-constrained nature of the devices. In fact, most IoT devices are designed for minimal computations, with little memory and energy use. This is reasonable from an efficiency point of view, but traditional PQC algorithms, while secure against quantum attacks, remain rather computationally expensive and large in key size, which easily overwhelms processing power in low-power devices or battery-operated ones [23]. For instance, although lattice-based schemes, such as CRYSTALS-Kyber and NTRU, are considered to be fairly efficient, the resource consumption is still much higher compared to some classical schemes, like RSA and ECC. Their large key size, along with the complex arithmetic, makes the latency of encryption, decryption, and key exchange so huge that it may compromise real-time performance of IoT systems [4, 5].

2) Energy Efficiency

Energy consumption is a very critical problem in IoT devices, especially for those powered by batteries or renewable sources like solar panels. Most IoT devices operate for a very long time without any intervention of maintenance; consequently, energy efficiency for them is premium. Complex mathematical operations, such as polynomial multiplication in some PQC algorithms-for example, lattice-based cryptography-can consume a quite considerable amount of energy. As it is essential to carry out these operations several times for encryption and decryption, this may result in significant drain of battery life, leading to an IoT device with an operational period that will be much shorter than required [11]. Efforts to optimize PQC algorithms for energy efficiency have been made, but the intrinsic complexity of post-quantum algorithms makes optimization particularly challenging. Thus, from this point of view, the right balance between security and energy efficiency is still an open issue [4, 20].

3) Key Size and Bandwidth Limitations

In most cases, the key sizes required by PQC algorithms are larger than in classical cryptography. The highly secure McEliece cryptosystem has public key sizes of several megabytes. Even though the key sizes are smaller for lattice-based algorithms, such as CRYSTALS-Kyber and NTRU, they remain far larger than the keys of RSA or ECC. These stronger key sizes introduce both storage and transmission issues for the specific keys in a memory-constrained IoT environment with expensive bandwidth [11]. This can cause network latency and bandwidth consumption, as larger keys take more bits to represent them, which can be critical in IoT networks where often real-time communications are required. Also, larger keys require more memory, which prohibits their use in many IoT devices due to the memory footprints being constrained [4].

4) Scalability

Other important challenges involve the scalability of lightweight PQC, since while connecting more and more IoT devices, each one should ensure secure and efficient communication over a huge network. A large-scale IoT system, such as smart cities or industrial automation networks, may require authentication of thousands or millions of devices that have to communicate securely with one another. PQC algorithms, especially those relying on resource-intensive operations, may have scaling issues without causing delays or affecting the overall system performance [1, 6]. Thus, solutions need to be provided for the correct handling of the key exchange, signature verification, and data transmission over large diversities in device classes running very different computational capabilities. This is further complicated by the need for backward compatibility with legacy systems that may not be as capable of supporting the additional computational burden imposed by PQC [4].

5) Hardware Limitations and Accelerations

Most IoT devices do not have hardware support for cryptographic operations, but instead rely on general-purpose microcontrollers that lack optimization for the complex operation requirements of PQC, possibly implying a slowdown in encryption and decryption, with greater energy use and latency. Although some works have been performed in implementing hardware accelerators for lattice-based cryptography using FPGAs or ASICs, these solutions are very pricey and definitely not suitable for large-scale deployment in low-cost IoT devices [1, 4]. The hardware limitation can be reduced if cryptographic accelerators for the PQC operations are added in future IoT devices. This could ensure that lightweight PQC can be efficiently deployed in a wide range of environments.

B. Future Directions for Lightweight Post-Quantum Cryptography

1) Algorithmic Optimization and Customization for Internet of Things

The most promising direction of lightweight PQC involves further optimization of the PQC algorithms according to IoT device requirements in respect to key-size reduction, simplification of mathematical operations, and energy-efficient optimization of encryption/decryption processes. Currently, lattice-based schemes, like CRYSTALS-Kyber and NTRU, have been optimized to a certain extent. Nevertheless, a greater improvement should be achieved to further reduce the former's resource consumption. Another related direction is the research of modular algorithms that can be tuned depending on the actual resources of a device. Quite naturally, stronger cryptographic variants can be utilized in IoT devices with more computational power, while lighter versions of the same algorithm can be executed by lower-power nodes. This will enable tailoring PQC for each device, offering a perfect balance between enhanced security and constrained resource consumption [4, 20].

2) Integration with Hardware Accelerators

The demand for lightweight PQC is increasing, and the need for dedicated hardware accelerators to handle the complex operations required by post-quantum algorithms is becoming more and more relevant. These accelerators can be implemented in IoT devices to offload cryptographic tasks from the main processor, reducing energy consumption, and thus improving performance.

Several works have already been carried out for the development of PQC solutions at the hardware level. Lattice-based cryptography, which requires polynomial multiplication, and different hardware accelerators have been proposed to accelerate this operation. As a matter of fact, these hardware accelerators can be integrated with the next-generation IoT devices, practically enabling the latter to perform quantum-resistant encryption and decryption operations without any loss in performance or energy efficiency [4, 5].

3) Security Standardization and Interoperability

While NIST is working on standardizing PQC, there is still more to be done to achieve its compatibility with IoT device-specific requirements. It also includes developing lightweight cryptographic libraries optimized for resource-constrained environments and ensuring that such libraries are compatible with the existing IoT platforms [4]. In addition, various IoT ecosystems demand that devices of distinct manufacturers securely communicate with one another by running different cryptographic protocols, making the task of developing standardized lightweight PQC algorithms that can be easily integrated into a variety of IoT systems quite essential to achieve seamless and secure communication across IoT networks [6].

4) Hybrid Cryptographic Systems

Another fast-emerging direction of lightweight PQC in IoT is developing hybrid cryptographic systems that can combine both classical cryptography and PQC. In the case of a hybrid system, classical cryptographic algorithms, such as RSA or ECC, are applied together with PQC algorithms, enriching the provided security layer. The approach allows IoT devices to smoothly proceed toward PQC but not without certain support by the classical systems. Hybrid cryptographic systems have particularly interesting applications when there is a need for interaction between legacy devices relying on classical cryptography and newer, quantum-resistant devices. The former ensure that communications remain secure during the transition to a fully quantum-safe world by utilizing both the classical and post-quantum algorithms [4, 6].

5) Efficient Key Management Systems

As a matter of fact, with PQC algorithms having larger signature sizes and more complex key exchange schemes, their efficient key management will be critical for scalability and security concerns in IoT networks. Further research should, therefore, focus on the development of PQC-optimized key management systems that guarantee secure generation, distribution, and key updating without overstretching the IoT device resources [1].

VII. CONCLUSION

Lightweight Post-Quantum Cryptography (PQC) is a direction for securing IoT systems with bounded resources in anticipation of future quantum attacks. Unlike conventional algorithms, which will become insecure owing to quantum computer advances, lightweight PQC seeks a sensitive equilibrium between security and efficiency, making it a viable alternative for IoT applications. Efficient algorithms, like CRYSTALS-Kyber, NTRU, and analogous lattice constructions, have been observed to provide post-quantum security along with efficient performance in bounded environments.

Several obstacles, including high consumption, key management complexity, and unscalability, have to be tackled through hardware acceleration, algorithm optimizations, and mixed techniques in order to enable ease of integration in IoT devices. The comparative analysis performed in the present work, indicates that even with high security assurance, in some cases, lattice-based cryptography can cause computational overhead, and thus, additional optimizations have to be conducted.

The present review reflects the current affairs in lightweight PQC, shedding new lights, accommodations, and yet unsolved obstacles in recent times. By studying alternative methodologies and their compatibility with IoT environments, a basis for post-quantum security technology evaluation and integration for academia and professionals in industries is determined. With continued studies, lightweight PQC will become a dominant player in securing IoT environments, and will enable the latter to become ubiquitous in a post-quantum era, enjoying long-term security in future cyber-attacks.

REFERENCES

[1] G. Fitzgibbon and C. Ottaviani, "Constrained Device Performance Benchmarking with the Implementation of Post-Quantum Cryptography," *Cryptography*, vol. 8, no. 2, Jun. 2024, Art. no. 21, https://doi.org/10.3390/cryptography8020021.

[2] K. Seyhan, T. N. Nguyen, S. Akleylek, and K. Cengiz, "Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey," *Cluster Computing*, vol. 25, no. 3, pp. 1729–1748, Jun. 2022, https://doi.org/10.1007/s10586-021-03380-7.

[3] Z. Ye, R. Song, H. Zhang, D. Chen, R. C.-C. Cheung, and K. Huang, "A Highly-efficient Lattice-based Post-Quantum Cryptography Processor for IoT Applications," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2024, no. 2, pp. 130–153, 2024, https://doi.org/10.46586/tches.v2024.i2.130-153.

[4] J. Senor, J. Portilla, and G. Mujica, "Analysis of the NTRU Post-Quantum Cryptographic Scheme in Constrained IoT Edge Devices," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18778–18790, Jul. 2022, https://doi.org/10.1109/JIOT.2022.3162254.

[5] L. Akcay and B. O. Yalcin, "Lightweight ASIP Design for Lattice-Based Post-quantum Cryptography Algorithms," *Arabian Journal for Science and Engineering*, vol. 50, no. 2, pp. 835–849, Jan. 2025, https://doi.org/10.1007/s13369-024-08976-w.

[6] A. A. Yavuz, S. Darzi, and S. E. Nouma, "Lightweight and Scalable Post-Quantum Authentication for Medical Internet of Things." arXiv, May 09, 2024, https://doi.org/10.48550/arXiv.2311.18674.

[7] S. He, H. Li, F. Li, and R. Ma, "A lightweight hardware implementation of CRYSTALS-Kyber," *Journal of Information and Intelligence*, vol. 2, no. 2, pp. 167–176, Mar. 2024, https://doi.org/10.1016/j.jiixd.2024.02.004.

[8] R. Asif, "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms," *IoT*, vol. 2, no. 1, pp. 71–91, Mar. 2021, https://doi.org/10.3390/iot2010005.

[9] J.-A. Septien-Hernandez, M. Arellano-Vazquez, M. A. Contreras-Cruz, and J.-P. Ramirez-Paredes, "A Comparative Study of Post-Quantum Cryptosystems for Internet-of-Things Applications," *Sensors*, vol. 22, no. 2, Jan. 2022, Art. no. 489, https://doi.org/10.3390/s22020489.

[10] S. Li *et al.*, "Post-Quantum Security: Opportunities and Challenges," *Sensors*, vol. 23, no. 21, Jan. 2023, Art. no. 8744, https://doi.org/10.3390/s23218744.

[11] T. Liu, G. Ramachandran, and R. Jurdak, "Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization." arXiv, Jan. 31, 2024, https://doi.org/10.48550/arXiv.2401.17538.

[12] J. J. Rubia, R. B. Lincy, E. E. Nithila, C. S. Shibi, and A. Rosi, "A Survey about Post Quantum Cryptography Methods," *EAI Endorsed Transactions on Internet of Things*, vol. 10, pp. 1–9, 2024, https://doi.org/10.4108/eetiot.5099.

[13] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a Quantum World," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 116–120, Feb. 2017, https://doi.org/10.1109/MCOM.2017.1600522CM.

[14] S. Kumari, M. Singh, R. Singh, and H. Tewari, "To Secure the Communication in Powerful Internet of Things Using Innovative Post-Quantum Cryptographic Method," *Arabian Journal for Science and Engineering*, vol. 47, no. 2, pp. 2419–2434, Feb. 2022, https://doi.org/10.1007/s13369-021-06166-6.

[15] R. Bavdekar, E. J. Chopde, A. Bhatia, K. Tiwari, S. J. Daniel, and Atul, "Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research." arXiv, Feb. 06, 2022, https://doi.org/10.48550/arXiv.2202.02826.

[16] R. R. Irshad *et al.*, "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing," *IEEE Access*, vol. 11, pp. 105479–105498, Jan. 2023, https://doi.org/10.1109/ACCESS.2023.3318755.

[17] J. Choi and J. Lee, "Secure and Scalable Internet of Things Model Using Post-Quantum MACsec," *Applied Sciences*, vol. 14, no. 10, Jan. 2024, Art. no. 4215, https://doi.org/10.3390/app14104215.

[18] F. Opilka, M. Niemiec, M. Gagliardi, and M. A. Kourtis, "Performance Analysis of Post-Quantum Cryptography Algorithms for Digital Signature," *Applied Sciences*, vol. 14, no. 12, Jan. 2024, Art. no. 4994, https://doi.org/10.3390/app14124994.

[19] A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks," *Internet of Things*, vol. 9, Mar. 2020, Art. no. 100174, https://doi.org/10.1016/j.iot.2020.100174.

[20] M. Alvarado, L. Gayler, A. Seals, T. Wang, and T. Hou, "A Survey on Post-Quantum Cryptography: State-of-the-Art and Challenges." arXiv, Dec. 16, 2023, https://doi.org/10.48550/arXiv.2312.10430.

[21] T. M. Fernandez-Carames, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, Jul. 2020, https://doi.org/10.1109/JIOT.2019.2958788.

[22] A. Ali, M. a. H. Farquad, C. Atheeq, and C. Altaf, "A Quantum Encryption Algorithm based on the Rail Fence Mechanism to Provide Data Integrity," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18818–18823, Dec. 2024, https://doi.org/10.48084/etasr.8993.

[23] A. Ashraaf and H. Sarwar, "Analysis of Post Quantum Cryptography Algorithms concerning their applicability to IoT devices." Engineering Archive, Jan. 12, 2024, https://doi.org/10.31224/3471.