eng

MDPI

Systematic Review

Resilience of Post-Quantum Cryptography in Lightweight IoT Protocols: A Systematic Review

Mohammed Almutairi [1,2,*] and Frederick T. Sheldon [1]

[1] Department of Computer Science, College of Engineering, University of Idaho, Moscow, ID 83844, USA; sheldon@uidaho.edu
[2] Applied College, University of Hafr Al Batin, Hafar Al Batin 39923, Saudi Arabia
* Correspondence: almu9701@vandals.uidaho.edu

Abstract

The rapid advancement of quantum computing poses significant threats to classical cryptographic methods, such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC), which currently secure Internet of Things (IoT) and cloud communications. Post-Quantum Cryptography (PQC), particularly lattice-based schemes, has emerged as a promising alternative. CRYSTALS-Kyber, standardized by the National Institute of Standards and Technology (NIST) as ML-KEM, has shown efficiency and practicality for constrained IoT devices. Most existing research has focused on PQC within the Transport Layer Security (TLS) protocol. Consequently, a critical gap exists in understanding PQC's performance in lightweight IoT protocols. These are Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), particularly under adverse network conditions. To address this gap, this paper provides a systematic review of the literature on the network resilience and performance of CRYSTALS-Kyber when integrated into these protocols operating over lossy and high-latency networks. Additional challenges include non-standardized integration, resource limitations, and side-channel vulnerabilities. This review provides a structured synthesis of current knowledge, highlights unresolved trade-offs between security and efficiency, and outlines future research directions, including protocol-level optimization, lightweight signature schemes, and resilience testing of PQC-secured IoT protocols under realistic conditions.

Keywords: Kyber; end to end security; cloud security; IoT and cloud security; MQTT; unreliable networks; PQC resilience

Academic Editor: Xinqing Xiao

Received: 8 September 2025
Revised: 24 October 2025
Accepted: 1 December 2025
Published: 2 December 2025

Citation: Almutairi, M.; Sheldon, F.T. Resilience of Post-Quantum Cryptography in Lightweight IoT Protocols: A Systematic Review. *Eng* **2025**, *6*, 346. https://doi.org/10.3390/eng6120346

1. Introduction

The rapid advancement of quantum computing poses significant risks to classical cryptographic systems such as RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography), widely used to secure communications between Internet of Things (IoT) devices and cloud platforms. Quantum algorithms, particularly Shor's algorithm, have demonstrated capabilities to compromise these cryptographic foundations by efficiently factoring large integers and solving discrete logarithm problems and tasks previously considered computationally infeasible for classical computers [1]. This phenomenon, often referred to as "harvest-now, decrypt-later," poses a serious risk to long-lived IoT data and justifies the urgent transition to quantum-resistant cryptography (Figure 1). Also, Grover's algorithm accelerates brute force attacks, significantly reducing the effective security of symmetric encryption schemes [2]. Consequently, there is an urgent need to transition

toward quantum-resistant cryptographic protocols, collectively known as Post-Quantum Cryptography (PQC).

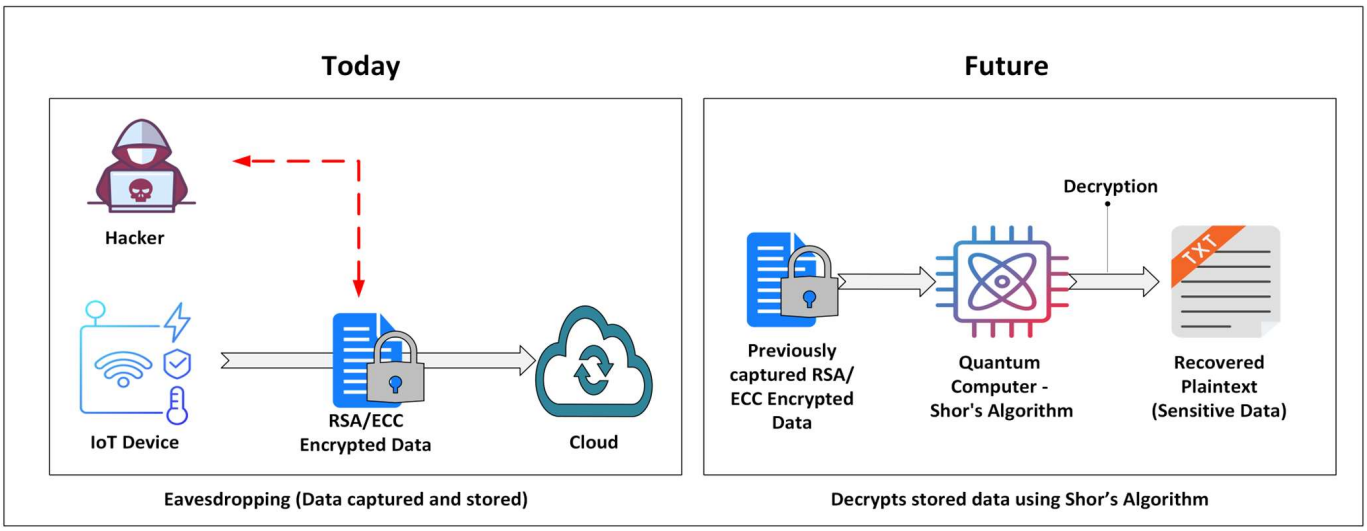

Figure 1. The "Harvest-Now, Decrypt-Later" threat model. Encrypted IoT data can be intercepted and stored today by adversaries, with the expectation that future quantum computers will decrypt them once powerful enough, compromising long-term confidentiality.

In response to these quantum threats, the National Institute of Standards and Technology (NIST) initiated a global standardization process to identify robust and efficient PQC algorithms. As of 2024, CRYSTALS-Kyber was selected and standardized by NIST for Key Encapsulation Mechanisms (KEMs), marking it as a critical candidate for securing sensitive data against quantum-enabled adversaries [3]. Kyber is notable in IoT because of its efficiency, small keys, and suitability for resource-limited devices with constrained processing, memory, and energy [4].

Several recent studies have benchmarked the performance of Kyber, demonstrating its practicality in various IoT contexts. For example, Fitzgibbon and Ottaviani (2024) evaluated Kyber on typical IoT hardware such as the Raspberry Pi 4, confirming its superior speed compared to other PQC finalists [4]. Sajimon et al. (2022) similarly highlighted Kyber's practical benefits by implementing and evaluating it on Linux-based IoT edge devices, recommending it due to its demonstrated efficiency and manageable computational overhead [5]. Moreover, practical studies such as Bürstinghaus et al. (2020) demonstrated Kyber's compatibility with embedded Transport Layer Security (TLS) libraries. Their findings revealed that Kyber outperformed traditional ECC-based methods in handshake speed [6].

However, despite these promising initial results, significant research gaps remain. Existing literature lacks comprehensive end-to-end evaluations of PQC integration in IoT-to-cloud communication. Holistic benchmarking across key performance metrics (latency, memory usage, and ciphertext size) and practical deployment considerations remains largely unexplored. Additionally, the implications of fully integrating PQC into existing IoT and cloud infrastructures, particularly addressing interoperability, performance trade-offs, and side-channel vulnerabilities, require further exploration.

Existing reviews on PQC have surveyed its broad landscape or benchmarked algorithm performance on IoT hardware, especially within robust protocols like TLS. This focus has left a critical gap in the network resilience of PQC in lightweight IoT protocols (MQTT and CoAP) under adverse conditions. To our knowledge, this is the first systematic review to synthesize the literature on the end-to-end performance of PQC-secured IoT protocols

in high-latency and lossy network environments. This work addresses these practical deployment challenges, providing a targeted synthesis for researchers and practitioners securing next-generation IoT infrastructures.

Research Questions

1. What post-quantum cryptographic schemes have been evaluated for IoT-to-cloud security?
2. What performance trade-offs (latency, bandwidth, memory) are reported when integrating PQC into IoT protocols?
3. What open challenges and research gaps remain for deploying PQC in real-world IoT-cloud systems?
4. How do PQC-secured lightweight protocols perform under realistic network conditions?

However, a critical analysis of the review reveals that these promising results are primarily focused on PQC integration within robust, high-overhead protocols, such as TLS. While essential, this focus overlooks a significant portion of the IoT ecosystem that relies on lightweight, publish-subscribe protocols like Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) for efficiency. Recent research has called for the development of PQC-friendly versions of these specific protocols. Unlike ideal lab environments, many IoT deployments face high packet loss and variable latency. This gap in understanding the resilience of PQC in IoT protocols represents a significant blind spot for practical, large-scale deployment.

This paper synthesizes current research on integrating CRYSTALS-Kyber into IoT-to-cloud communication and compares the performance of PQC methods against classical methods. Also, it identifies a critical research gap, specifically, the lack of systematic evaluation of PQC in lightweight IoT protocols under real-world network conditions. Based on this analysis, the paper outlines key challenges and recommends future directions to guide researchers and practitioners working toward quantum-secure IoT infrastructures.

2. Background and Related Work

2.1. The Threat of Quantum Computing to Current Cryptography

Quantum computing poses a technically well-defined threat to classical public-key infrastructures. Shor's algorithm enables polynomial-time factoring and discrete logarithms, reducing the effective security of RSA and ECC from "infeasible" to "routine" once scalable fault-tolerant machines emerge [7]. Grover's algorithm also undermines symmetric cryptography by halving the effective key space, necessitating longer keys to maintain equivalent strength. These advances threaten a wide range of systems, such as IoT firmware updates, blockchain signatures, and satellite communications, that rely on RSA/ECC handshakes [7,8]. Table 1 summarizes the major milestones in the NIST PQC standardization process, including the selection of CRYSTALS-Kyber and other dates. NIST's transition guidance urges federal agencies and critical-infrastructure operators to inventory vulnerable cryptography now and plan upgrades. Thus, the long-lived data remain confidential beyond 2035 PQShield.

Table 1. NIST-PQC Standardization Timeline.

Year	Milestone
2016	NIST issues a call for PQC proposals.
December 2017–January 2019	Round 1 (69 candidates) → Round 2 (26).
July 2020	Round 3 finalists and alternates announced (7 KEM/sig algorithms).
5 July 2022	NIST selects CRYSTALS-Kyber as the sole KEM to be standardized, alongside Dilithium, Falcon and SPHINCS+ for signatures.
13 August 2024	Final FIPS 203—Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), derived from Kyber, is published; it becomes the primary federal standard for general-purpose encryption [9].
11 March 2025	NIST announces Hamming Quasi-Cyclic (HQC) as an additional KEM for specialized use cases and releases status report NIST IR 8545 on Round 4 [10].

2.2. Overview of CRYSTALS-Kyber (ML-KEM)

Kyber, standardized as ML-KEM, is a lattice-based KEM built on the difficulties of the Module Learning with Errors (M-LWE) problem. Lattice assumptions are believed to resist both classical and quantum attacks and admit efficient polynomial-time implementations [11]. A high-level view of how the Kyber algorithm works is shown in Figure 2. A KEM is used to send a symmetric key between two parties using asymmetric algorithms. Table 2 shows Kyber's three parameter forms, their related NIST security levels, and key/ciphertext sizes. These values are essential when comparing PQC schemes with traditional methods in constrained IoT environments.

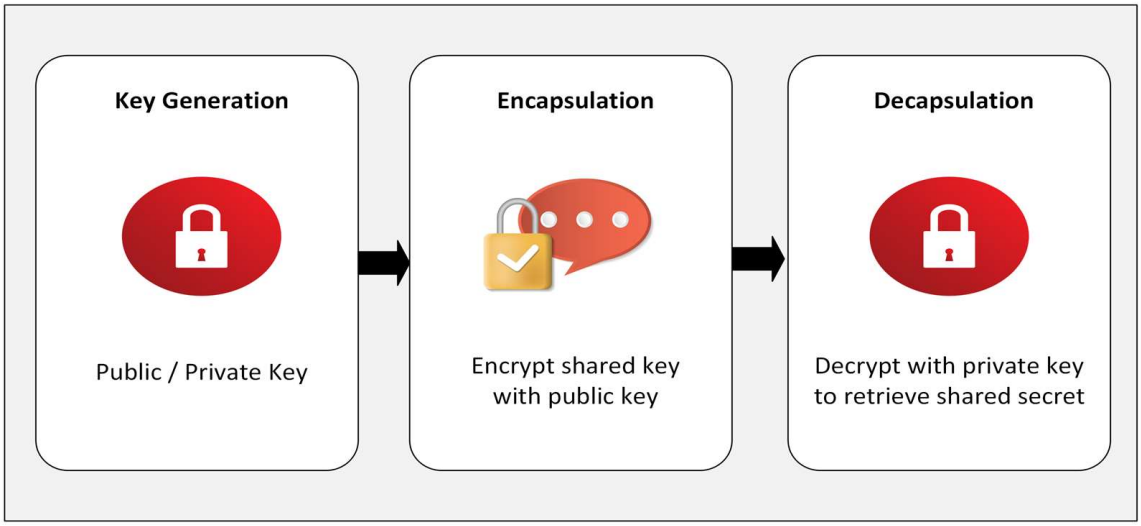

Figure 2. CRYSTALS-Kyber Algorithm Simplified.

Table 2. Parameter sets and security levels. (All three share a 32-byte shared secret).

Variant	NIST Level	Public-Key (Bytes)	Cipher-Text (Bytes)	Symmetric Comparable
Kyber-512	1	800	768	AES-128
Kyber-768	3	1184	1088	AES-192
Kyber-1024	5	1568	1568	AES-256

Performance advantages for IoT-cloud links.

- Completes encapsulation on IoT class processors three to five times faster than classical schemes, reducing latency and energy consumption during the handshake process.
- Constant-time C implementations achieve 2–4 ms encapsulation on Cortex-M4 devices within the same power envelope (based on benchmark studies summarized in Section 2.4).
- Its simple message-independent design makes it more resistant to side-channel attacks than other lattice-based alternatives.

Standardization status under FIPS 203, Kyber is selected as the default federal choice for data encryption. Vendors must label compliant implementations with "ML-KEM" and follow the byte-exact encodings and test vectors defined therein [12].

2.3. Mathematical Foundations of Kyber and Lattice-Based Cryptography

The security of CRYSTALS-Kyber rests on the assumed computational difficulty of solving mathematical problems on lattices. Specifically, Kyber's security is derived from the M-LWE problem. Primarily, M-LWE is a mathematical challenge that is easy to formulate but is strongly believed to be hard to solve for both classical and quantum computers. This provides a robust foundation for a quantum-resistant cryptosystem [13].

The breakthrough in PQC was not only identifying these hard problems but designing efficient and practical cryptographic schemes based upon them. The assumed difficulties of lattice-based problems like M-LWE against quantum attacks are the primary reason the NIST selected CRYSTALS-Kyber as the standardized algorithm for general-purpose KEM. This choice reflects years of public analysis concluding that Kyber offers a strong balance of security, performance, and implementation readiness.

While a deep mathematical analysis is beyond the scope of this review, a foundational understanding of lattice-based cryptography is crucial for the security claims of PQC. Accordingly, our focus is on the practical implementation and network performance trade-offs of these algorithms.

2.4. Key Prior Studies on PQC (Kyber) in IoT and Cloud Settings

Recent studies have explored the integration of PQC, particularly CRYS-TALS-Kyber, into IoT and edge devices. These works collectively establish a strong basis for assessing its practicality in real-world constrained environments.

- Fitzgibbon et al. (2023) benchmarked NIST's PQC finalists on a Raspberry Pi 4, representing a typical IoT class device [4]. Among the candidates, CRYSTALS-Kyber appeared as the fastest KEM, with key generation, encapsulation, and decapsulation completing in the hundreds of microseconds [14]. Kyber consistently outperformed other candidates on low-power platforms, confirming its suitability for resource-constrained IoT devices. Additionally, Dilithium was identified as the most efficient signature algorithm on the same platform, which is relevant for future authentication needs [4].
- Sajimon et al. (2022) implemented several NIST PQC finalists (Level 3 security), including Kyber, on a Raspberry Pi 4 running Linux, simulating a typical IoT edge device [5]. Their evaluation recommended suitable PQC schemes based on performance in constrained environments. While specific metrics were not detailed, Kyber was among the top performers due to its known speed, reinforcing its practicality for real-world IoT deployments.
- Bürstinghaus et al. (2020) integrated Kyber for key exchange and SPHINCS+ for digital signatures into an embedded TLS library (mbedTLS) [6]. Their tests on lightweight devices revealed that Kyber's key agreement outperformed classical ECC (ECDH) by

approximately 10× in speed. However, the addition of SPHINCS+ introduced high latency and memory overhead during TLS handshakes. This emphasizes the need to carefully select lightweight signature algorithms, suggesting Dilithium may be a more practical alternative for IoT use. This underscores that full PQC stacks require a balanced selection of encryption and signature schemes.

- K. Mayes (2020) demonstrated that Kyber-768 on an ultra-constrained device was implemented on a Multi-application Operating System (MULTOS) security module with 13 KB of RAM [15]. Although successful, the encapsulation process took nearly 10 s, even with a cryptographic co-processor, demonstrating that Kyber can function in minimal memory environments but at the cost of speed. A related study implementing a Kyber-768 variant on a similar smart card platform with a cryptographic co-processor reported concrete performance figures: key generation in 79.6 ms, encapsulation in 102.4 ms, and decapsulation in 132.7 ms. These results demonstrate that Kyber can function in minimal memory environments with promising speed [16]. This sets a lower bound for Kyber's practicality and suggests real-world use should target hardware at or above Cortex-M4/M7 levels.
- Kumari et al. (2022) reviewed about 70 studies mapping PQC to microcontrollers and gateways [17]. They found lattice-based KEMs, particularly Kyber, offered the best trade-off among ciphertext size, speed, and code footprint (<10 KB flash, <4 KB RAM), while noting side-channel and key management challenges.
- Mahdi and Abdullah (2025) emphasize that while algorithms such as CRYSTALS-Kyber are computationally efficient, practical deployment still faces hurdles [18]. These include energy consumption, hardware limitations, and scalability across heterogeneous IoT devices. Also, they proposed optimization techniques currently under exploration, such as hardware acceleration, algorithmic improvement, and hybrid frameworks to enhance feasibility. Long-term success will demand systematic engineering efforts to balance security, efficiency, and scalability.
- Chung et al. (2022) evaluated Kyber-512/768 and other NIST finalists in a TLS 1.3 stack running on a Raspberry Pi 4 manufactured by Raspberry Pi Ltd., Cambridge, UK (Cortex-A72) and an STM32F411 manufactured by STMicroelectronics, Geneva, Switzerland (Cortex-M4) [19]. Full handshakes completed in 1.1 to 1.4 × the latency and fit within 32 KB RAM, showing post-quantum security is feasible on IoT hardware.
- Tasopoulos et al. (2022) demonstrated that implementing PQC in TLS 1.3 for resource-constrained devices increases execution time, memory usage, and bandwidth requirements [20]. Similarly, Abbasi et al. (2025) reported that trustful PQC implementation can raise handshake size by up to 7× compared to classical approaches, although they showed that optimization strategies can reduce bandwidth demands by 40–60% [21]. Beyond TLS, Blanco-Romero et al. (2024) integrated PQC into IoT protocols such as CoAP and MQTT-SN, addressing the limited understanding of PQC's impact on lightweight communication mechanisms [22]. Similarly, Paul et al. (2021) investigated PQC integration with Trusted Platform Modules (TPMs) in TLS, and they found it feasible but noted performance degradation when offloading hash computations [23]. Together, these works highlight both the challenges and opportunities of PQC adoption in IoT environments, emphasizing the need for optimized implementations to balance security, performance, and scalability.
- Achoe (2025) recommends as future work to develop custom-built lightweight PQC-friendly versions of MQTT, CoAP, and 6LoWPAN [16]. This highlights a recognized need for research focused specifically on these IoT protocols.
- Kumar et al. (2022) and Almutairi & Sheldon (2025) surveyed post-quantum cryptography in IoT and IoT-Cloud contexts, emphasizing the urgency of migrating IoT

systems to quantum-safe algorithms [24,25]. Their works outline candidate schemes, integration challenges, and highlight PQC as an emerging solution to strengthen IoT-Cloud security, though neither includes an implementation study, serving primarily as conceptual motivation. On the industry side, cloud providers such as AWS have begun testing hybrid TLS configurations with Kyber in production environments, signaling that cloud infrastructures are PQC-ready and shifting the research focus toward IoT integration [26]. Alongside the transition to PQC, for instance, Hazber et al. propose a framework that leverages blockchain and AI-driven threat detection to enhance data integrity and scalability. This highlights a different but complementary approach to supporting IoT security [27].

Collectively, these studies show that Kyber is the most promising KEM for constrained environments. However, PQC adoption still faces challenges in terms of efficiency and scalability, particularly in IoT-to-cloud communication. This review identifies this as a primary gap for future research.

Table 3 highlights a specific gap in current PQC research. While the device-level performance of CRYSTALS-Kyber is well established and its integration into TLS has been extensively benchmarked [20,21], lightweight IoT protocols remain largely overlooked. Several studies explicitly call for securing protocols such as MQTT and CoAP [16,22], yet the few available implementations are incomplete. For example, the only published study of a Kyber-secured MQTT variant [28] evaluated computational performance on sensor hardware but missed network-level factors such as latency, packet loss, and handshake reliability. To date, no work has systematically assessed the end-to-end performance and resilience of PQC-secured IoT protocols under the unreliable conditions common in real-world deployments.

Table 3. Synthesis of Prior Studies and Identification of the Research Gap.

Study	Focus Protocol	Device Benchmark	End-to-End Test	Network Condition Analysis	Key Contribution	Remaining Gap
Fitzgibbon et al. (2023) [4]	(Implicitly TLS)	✓	✗	✗	Kyber benchmarked on Raspberry Pi, the fastest KEM among candidates.	Limited to device-level tests and not IoT protocols
Sajimon et al. (2022) [5]	TLS/IoT devices	✓	✗	✗	Implemented PQC finalists on Linux-based edge devices; Kyber efficient	Did not include network or protocol-level performance
Bürstinghaus et al. (2020) [6]	TLS	✓	✓	✗	Integrated Kyber + SPHINCS+ into mbedTLS, and it has faster handshakes than ECC	Signature scheme overhead too high for IoT
Mayes (2020) [15]	N/A (standalone Kyber)	✓	✗	✗	Demonstrated Kyber-768 on ultra-constrained MULTOS (13 KB RAM), and its encapsulation is feasible but slow (~10 s without co-processor and ~100 ms with)	Shows Kyber's practicality floor and no IoT protocol integration
Kumari et al. (2022) [17]	Survey	✗	✗	✗	Comprehensive survey of PQC for IoT microcontrollers	No implementation results, and it is theoretical

Table 3. *Cont.*

Study	Focus Protocol	Device Benchmark	End-to-End Test	Network Condition Analysis	Key Contribution	Remaining Gap
Chung et al. (2022) [19]	TLS	✓	✓	✗	Benchmarked Kyber on Cortex-M4 and Pi4, and it is feasible for IoT.	No MQTT/CoAP evaluation
Mahdi & Abdullah (2025) [18]	General IoT	✗	✗	✗	Highlighted optimization, energy, scalability challenges	No protocol-level or experimental validation
Tasopoulos et al. (2022) [20]	TLS 1.3	✓	✓	✗	Showed PQC increases execution time, memory, bandwidth	Limited to TLS and no IoT protocols
Blanco-Romero et al. (2024) [22]	CoAP, MQTT-SN	✓	✓	✗	Integrated PQC into lightweight IoT protocols	No adverse network analysis
Paul et al. (2021) [23]	TLS with TPM	✓	✓	✗	Demonstrated PQC in TLS with TPM offloading	Performance hit with TPM hash offload
Achoe (2025) [16]	MQTT/CoAP	✗	✗	✗	Called explicitly for PQC-secured lightweight protocols	No implementation, and it is only a call for research
YoungBeom et al. (2025) [28]	MQTT	✓	✓(partial)	✗	First KEM-MQTT implementation on 8-bit AVR nodes.	Excluded network performance
Abbasi et al. (2025) [21]	TLS (multi-platform)	✓	✓	✓	Systematic TLS benchmarks across devices	TLS only and missing IoT protocols
Identified Gap	MQTT/CoAP	✓	✓	✓	-	No existing study systematically evaluates Kyber over MQTT under adverse network conditions.

✓ indicates the gap or area is covered or benchmarked. ✗ means that it is not covered. N/A indicates that the item is not applicable.

3. Methodology

This article is a structured narrative review. Nevertheless, it follows key elements of the PRISMA 2020 framework to ensure transparency and reproducibility of the literature selection process.

3.1. Research Focus

This review builds upon the research questions defined in the Research Questions Section. It specifically focuses on synthesizing empirical evidence on CRYSTALS-Kyber performance and implementation feasibility in IoT-to-cloud communication. The objective is to unify measurable results (latency, memory, bandwidth) and identify continuous deployment challenges in constrained environments.

3.2. Eligibility Criteria

Included studies had to: (i) be peer-reviewed articles or conference papers published between 2017 and 30 April 2025; (ii) report empirical measurements of Kyber on IoT, edge, or embedded platforms; (iii) present at least one comparator cryptosystem. Exclusion criteria were non-English language, theoretical analyses, and studies lacking device-level metrics.

3.3. Information Sources and Search Strategy

A comprehensive search for desired studies was conducted in August 2025 across multiple databases. It is important to note that overly broad search terms such as "IoT-Cloud Security", "Post-Quantum Cryptography", and "Communication" were intentionally avoided, as they yield thousands of results that are not relevant to the specific implementation challenges in IoT. Instead, our search strategy was designed to be highly targeted. We used a primary search string ("CRYSTALS-Kyber" OR Kyber) AND ("Internet of Things" OR IoT OR edge) to identify practical work on Kyber in IoT contexts. A secondary, even more specific search (Kyber OR "post-quantum") AND (MQTT OR CoAP) AND (performance OR resilience OR "packet loss" OR latency) was performed to precisely identify literature addressing the research gap involving lightweight protocols under negative network conditions. This focused approach ensures the relevance of the identified studies.

3.4. Selection Process and Data Extraction

The selection process strictly followed the PRISMA 2020 framework to ensure transparency and reproducibility. Our eligibility criteria were designed to filter for studies that presented empirical, device-level measurements of Kyber on IoT platforms. Studies that were purely theoretical or lacked performance data were excluded. This strict filtering is the stamp of a systematic review and explains why the initial 102 records were narrowed to 13 core studies for synthesis. The strength of this review lies not in the quantity of papers surveyed but in the quality and synthesized evidence, which directly addresses the defined research questions. Figure 3 presents the PRISMA 2020 flow diagram reflecting these search results.

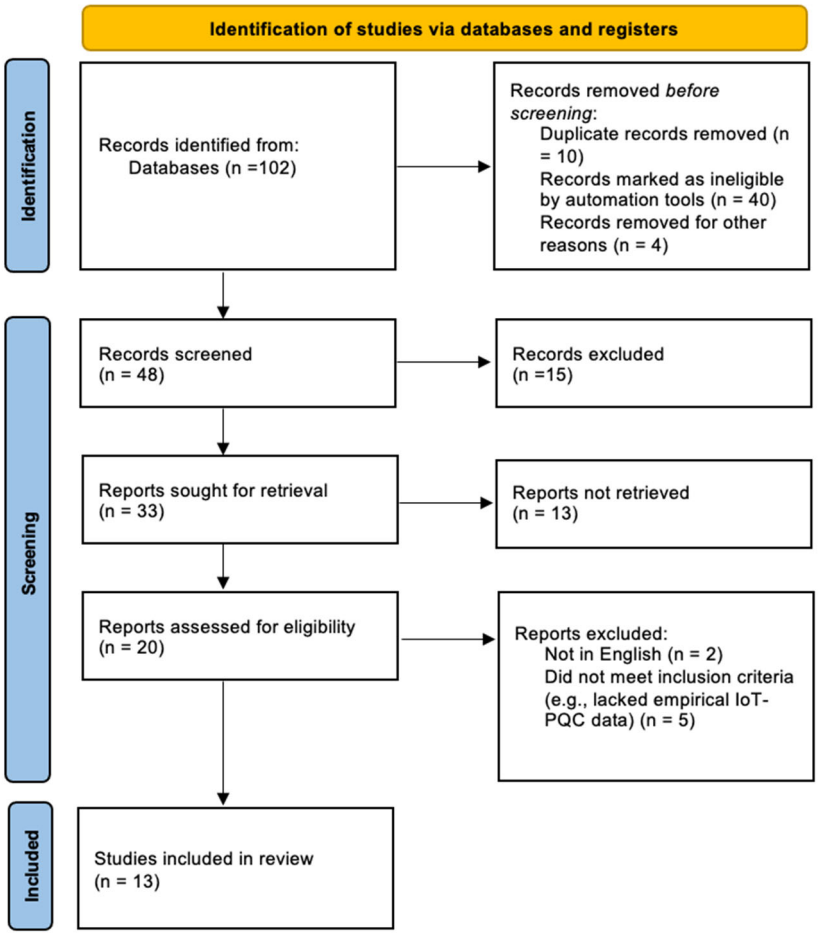

Figure 3. PRISMA Flow Overview.

3.5. Synthesis Approach

Because benchmarking platforms and metric definitions varied, a formal meta-analysis was not feasible. Quantitative data were normalized to common units (milliseconds per key-pair and bytes per ciphertext). Qualitative findings on implementation challenges were grouped by category.

4. Performance Comparison: PQC vs. Traditional Crypto (RSA/ECC)

This section synthesizes comparative findings from existing literature on Kyber and classical schemes (RSA, ECC) across key dimensions. These are execution speed, communication overhead, symmetric encryption compatibility, and practical feasibility in IoT environments.

4.1. Execution Speed

Multiple benchmarks show that Kyber can meet or even exceed the performance of RSA/ECC at comparable security levels. Demir et al. (2025) conducted comprehensive tests of Kyber vs. RSA-2048 and ECDH (P-256 ECC) [1]. Their results indicate that Kyber-512 (offering 128-bit security) completes key exchange roughly three times faster than RSA-2048 or ECDH-P256. Even Kyber-1024, the highest-security variant, outpaced RSA-3072 by a similar margin. The reason is that Kyber's math (lattice polynomials with number-theoretic transforms) can be computed much faster than RSA/ECC's large-integer exponentiations on general-purpose CPUs. For IoT devices, this translates into lower CPU usage, reduced energy consumption, and faster key exchange completion. All of which are vital for battery-powered and limited-resource environments. These findings are consistent with prior research, such as embedded TLS experiments where Kyber outperformed ECDH by an order of magnitude in handshake speed [6,29]. This counters the common misconception that PQC is naturally heavier or slower [1].

4.2. Communication Overhead (Key/Ciphertext Sizes)

The trade-off comes in data sizes. PQC generally has larger key and ciphertext sizes than traditional schemes, which can impact network bandwidth and memory usage. For instance, Kyber-512's public key is 800 bytes, and its ciphertext is ~768 bytes [1]. In contrast, a 2048-bit RSA public key is only 256 bytes, and an ECC P-256 public key is ~64 bytes. Thus, a Kyber handshake transmits more data, often in the kilobyte range, compared to a few hundred bytes for RSA or ECC. While this is manageable in high-bandwidth networks, it could pose challenges in IoT settings such as Low-power WAN (LPWANs) or devices with strict data quotas.

Also, memory usage is a consideration. Kyber requires around 1–2 KB of memory for key storage and math on a polynomial. However, most modern IoT devices (e.g., Raspberry Pi or Cortex-M4/M7 class microcontrollers) have sufficient resources to accommodate these needs. For example, a Raspberry Pi 4 can execute Kyber operations in microseconds, while even a constrained device with just 13 KB of RAM managed to run Kyber-768, with an encapsulation latency of just over 100 ms when using a co-processor [1,5,30]. Although Kyber's key sizes are larger, they remain practical as network protocols and hardware continue to evolve. Still, it is crucial to measure and report message sizes and memory usage to verify the actual overhead. For example, recording the exact bytes exchanged during key exchanges (Kyber vs. RSA/ECC) and tracking each algorithm's memory footprint on the simulated device. Prior studies mainly focus on speed, with limited analysis of memory or bandwidth impact [14]. This highlights an important gap that future research should address through a comprehensive evaluation of PQC schemes under constrained IoT conditions [31].

4.3. Symmetric Encryption Throughput

After key exchange, both PQC and traditional cryptographic protocols rely on symmetric encryption (e.g., AES-GCM) for actual data transmission. Notably, symmetric encryption performance remains unaffected by the choice of public-key algorithm [4]. One difference is that with PQC KEMs like Kyber, the key exchange produces a shared secret of (e.g., 256 bits), which can be directly used as an AES-256 key. With RSA/ECC, often a 128- or 256-bit secret is agreed and used similarly. There is no inherent performance difference in using the key for AES. As highlighted in prior studies, the performance difference between classical and PQC is largely limited to the handshake phase (i.e., key exchange), not the symmetric encryption itself. Therefore, future practical evaluations of post-quantum performance should focus on handshake latency, CPU utilization, memory load, and time-to-first byte rather than AES throughput [29].

4.4. Overall Feasibility

Current research presents a promising outlook: Kyber and other PQC schemes can outperform RSA/ECC in key exchange speed, even under constrained conditions [1]. Although they introduce larger key sizes and ciphertexts, these are well within the capabilities of many IoT-class devices. Moreover, PQC offers forward secrecy and quantum resistance, making it a more future-proof solution. For instance, an IoT sensor that currently takes 50 ms to complete an ECC-based handshake might complete a Kyber-based handshake in 20 ms. These performance gains, as documented in existing benchmarks, suggest strong potential for PQC in resource-constrained deployments. However, further research is needed to comprehensively measure and compare encryption times, message sizes, and memory usage across Kyber, RSA, and ECC, particularly in the context of IoT-to-cloud secure communication.

In addition to speed, PQC types differ in data size. For example, Kyber-512 uses an 800-byte public key and produces a 768-byte ciphertext, compared to just 256 bytes for an RSA-2048 public key or ~64 bytes for ECC P-256. While these size differences are manageable for most modern networks, they could affect bandwidth and packet loss in constrained IoT systems [1,14]. Table 4 provides a detailed summary of these performance metrics.

Table 4. Key differences between classical cryptosystems and the CRYSTALS-Kyber.

Algorithm	NIST Security Level	Public Key Size (Bytes)	Ciphertext Size (Bytes)	Relative Speed (Key Exchange)
ECC (P-256)	1	~64	N/A	Baseline (1×)
RSA-2048	1	256	N/A	Slower (~0.7×)
Kyber-512	1	800	768	Much Faster (~3–5×)
Kyber-768	3	1184	1088	Much Faster (~3–5×)
Kyber-1024	5	1568	1568	Much Faster (~3–5×)

N/A indicates that the item is not applicable.

5. Discussion: Identified Research Gaps and Challenges

This review addressed the four research questions (RQs), synthesizing findings from 13 studies on PQC in IoT-to-cloud communication. The results highlight both progress and continued gaps.

5.1. The Primary Research Gap: Network Resilience in Lightweight Protocols Under Unreliable Network Conditions (RQ4)

The most critical gap identified is the absence of systematic evaluations of PQC-secured lightweight IoT protocols (MQTT, CoAP) under the realistic, often 'messy' network

conditions. Current benchmarks overwhelmingly focus on TLS, which differs basically from MQTT/CoAP in terms of handshake mechanisms and packet overhead [20,21].

- Existing efforts: Ref. [22] integrated PQC into CoAP and MQTT-SN, ref. [28] tested KEM-MQTT on AVR sensor nodes, and ref. [16] called for lightweight PQC protocols.
- Limitation: These studies focused only on computational feasibility and explicitly excluded network-level factors such as packet loss and high latency.
- Research needs: PQC's larger key sizes and ciphertexts are most impactful in lossy IoT environments. No existing study has quantified how handshake success rates, retransmissions, and latency evolve under degraded conditions. This review asserts that the central unanswered question for the field is: What happens when these IoT protocols are tested in more realistic network environments? Therefore, future work should utilize simulation-based and real-world testbeds to evaluate the performance of PQC-resilient MQTT/CoAP under constrained networks.

5.2. Related Challenges and Future Work

While the focus is on network resilience, several related challenges remain important for the broader adoption of PQC in IoT.

5.2.1. Practical Integration Challenges (RQ1 and RQ3)

While Kyber has emerged as the dominant PQC KEM, protocol integration remains immature. TLS 1.3 extensions exist, but no standardized approaches are available for MQTT/CoAP. Temporary hybrid schemes (classical + PQC keys) are widely used to ensure backward compatibility [6,21]. Authentication is another bottleneck, so replacing RSA/ECC-based certificates with PQ signatures like Dilithium significantly increases handshake size (2–5 KB) and processing cost. This highlights the need for lightweight PQ signature schemes and standardization of PQC at the IoT protocol layer. Ultimately, these integration issues force developers to navigate a critical trade-off: implementing the strongest post-quantum security versus maintaining minimal overhead. This challenge is especially found in resource-constrained IoT systems.

5.2.2. Resource Constraints and Optimizations (RQ2 and RQ3)

PQC is feasible on mid-range IoT hardware (Cortex-M4/M7), but ultra-constrained devices face trade-offs. By synthesizing the findings from the literature, a clear picture of these trade-offs emerges. In practical comparisons, Kyber consistently offers lower latency than RSA/ECC, but at the cost of a larger memory footprint and increased bandwidth for its keys and ciphertexts. Mayes showed Kyber-768 running on a 13 KB RAM smart card, but encapsulation required ~10 s without a co-processor [15]. More promising results with vectorized optimizations (ARM Neon) show potential for reducing CPU cycles and energy costs [18,32,33]. However, no extensive research has yet focused on optimizing CRYSTALS-Kyber specifically for ultra-constrained microcontrollers in practical IoT deployments. This represents a clear technical gap, as it is unknown if default PQC libraries are sufficient for such environments. Future studies must benchmark energy and memory usage across representative IoT devices to determine if targeted optimizations are required to meet performance and energy constraints [30].

5.2.3. Security Analysis in IoT Context (RQ3)

Performance is only part of the challenge; security in deployment is equally critical. Although Kyber is cryptographically secure under lattice assumptions, real-world IoT implementations are vulnerable to side-channel attacks. The KyberSlash timing attack

demonstrated key leakage in lab settings [34,35]. Current IoT PQC research rarely addresses resilience against timing, power, or cache-based side channels.

Moreover, IoT devices are exposed to man-in-the-middle attacks, protocol downgrades, and other threat vectors. PQC's main strength is resisting quantum decryption of intercepted data and addressing only part of the threat landscape (e.g., it prevents an attacker with a quantum computer from decoding intercepted data in the future, unlike RSA/ECC [1]). Also, a complete security model must account for randomness quality, key reuse policies, and endpoint trust models. Comprehensive IoT-specific threat models and side-channel PQC libraries are urgently needed.

Furthermore, securing real-world deployments requires addressing specific implementation vulnerabilities beyond pure algorithmic strength. While Kyber's security is mathematically strong, its performance on different architectures, such as 64-bit ARM processors, must be optimized to prevent timing variations that could be exploited [36]. Therefore, a comprehensive security model must defend against a wide range of implementation attacks, including the side-channels discussed previously, which remain a significant threat to all PQC deployments [37]. While hardware acceleration on platforms like FPGAs can improve performance, this also introduces new potential vulnerabilities that must be carefully considered [38].

Table 5 summarizes the main research gaps identified through this review and offers recommendations for addressing each area.

Table 5. Summary of Identified Research Gaps and Future Directions.

Gap Area	Description	Supporting Studies	Insights and Recommendations
PQC Resilience in Lightweight IoT Protocols	Most evaluations focus on TLS, but MQTT/CoAP is largely unexplored. One KEM-MQTT study excluded network resilience.	[16,22,28]	This review highlights the lack of studies on PQC resilience in MQTT and CoAP protocols, particularly under high-latency and lossy conditions, and recommends focused practical evaluation.
Integration Challenges	PQC is feasible in TLS, but signatures (SPHINCS+) cause high latency. Hybrid schemes are temporarily used.	[6,21]	Explore Dilithium or hybrid TLS and standardization for IoT protocols.
Resource Constraints and Optimization	Ultra-constrained devices can run Kyber, but slowly without co-processors. Energy is still an issue.	[15,18]	It identifies the need to measure how PQC algorithms affect speed, memory, and energy use on ultra-low-power microcontrollers. Also, it recommends future work on creating optimized versions for embedded systems.
Security Evaluation in IoT Context	Some side-channel risks were identified in Kyber (e.g., Kybe-Slash) and a few IoT-specific threat models.	[34,35]	It points out the gap in side-channel analysis of Kyber in IoT and recommends that future work address timing attacks and power analysis risks in constrained environments.

6. Conclusions

This review synthesized current research on the deployment of post-quantum cryptography in IoT-cloud communication, with a particular focus on CRYSTALS-Kyber. Evidence shows that Kyber offers faster key exchange and lower computational cost than RSA and

ECC, which makes it promising for constrained IoT devices. However, significant challenges remain. This review confirms the existence of a critical and underexplored gap in the transition to quantum-safe security, which is the lack of resilience testing for PQC in lightweight IoT protocols. Our synthesis of the available evidence demonstrates that until the performance of Kyber-secured MQTT and CoAP is systematically evaluated in lossy and high-latency networks, a significant barrier to secure IoT deployment will remain. Beyond this central gap, additional barriers include the lack of standardized integration pathways, the performance hurdle of PQ signatures in authentication, resource constraints on ultra-low-power devices, and emerging side-channel vulnerabilities in PQC implementations. Addressing these issues requires simulation-based and real-world evaluations of Kyber-secured MQTT/CoAP under lossy and high-latency networks, optimization strategies for energy-constrained hardware, and the development of PQC libraries tailored for IoT. By systematically identifying these gaps, this review not only clarifies the current state of PQC research but also charts a roadmap for future investigations that are essential for a secure transition to post-quantum IoT infrastructures.

Author Contributions: Conceptualization, M.A.; methodology, M.A.; validation, M.A. and F.T.S.; formal analysis, M.A.; investigation, M.A.; resources, M.A.; data curation, F.T.S.; writing—original draft preparation, M.A.; writing—review and editing, F.T.S.; visualization, M.A.; supervision, F.T.S.; project administration, F.T.S.; funding acquisition, M.A. and F.T.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things	NIST	National Institute of Standards and Technology
PQC	Post-Quantum Cryptography	RSA	Rivest–Shamir–Adleman
ECC	Elliptic Curve Cryptography	CPU	Central Processing Unit
TLS	Transport Layer Security	MQTT	Message Queuing Telemetry Transport
CoAP	Constrained Application Protocol	KEM	Key Encapsulation Mechanisms
mbedTLS	embedded TLS library	RAM	Random Access Memory
LPWANs	Low-power WAN	HQC	Hamming Quasi-Cyclic
MULTOS	Multi-application Operating System	Cortex	A brand name for a family of processor cores developed by Arm.
WAN	Wide Area Network	RQ	research questions
M-LWE	Module Learning with Errors	SPHINCS+	stateless hash-based digital signature scheme

References

1. Demir, E.D.; Bilgin, B.; Onbasli, M.C. Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms. *arXiv* **2025**, arXiv:2503.12952. [CrossRef]
2. Bernstein, D.; Lange, T. Post-quantum cryptography. *Nature* **2017**, *549*, 188–194. [CrossRef] [PubMed]
3. Information Technology Laboratory. Post-Quantum Cryptography Standardization. 2024. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms (accessed on 17 March 2024).
4. Fitzgibbon, G.; Ottaviani, C. Constrained Device Performance Benchmarking with the Implementation of Post-Quantum Cryptography. *Cryptography* **2024**, *8*, 21. [CrossRef]

5. Sajimon, P.C.; Jain, K.; Krishnan, P. Analysis of Post-Quantum Cryptography for Internet of Things. In Proceedings of the 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 25–27 May 2022.
6. Bürstinghaus-Steinbach, K.; Krauß, C.; Niederhagen, R.; Schneider, M. Post-Quantum TLS on Embedded Systems: Integrating and Evaluating Kyber and SPHINCS+ with mbed TLS. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, Taipei, Taiwan, 5–9 October 2020.
7. Abuarqoub, A. Security Challenges Posed by Quantum Computing on Emerging Technologies. In Proceedings of the 4th International Conference on Future Networks and Distributed Systems (ICFNDS), St. Petersburg, Russia, 26–27 November 2020.
8. Kirsch, Z.; Chow, M. Quantum Computing: The Risk to Existing Encryption Methods. 2015. Available online: https://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf (accessed on 20 July 2025).
9. Alagic, G.; Barker, E.; Chen, L.; Moody, D.; Robinson, A.; Silberg, H.; Waller, N. Recommendations for Key-Encapsulation Mechanisms. NIST Special Publication (SP) 800-227. 2025. Available online: https://csrc.nist.gov/pubs/sp/800/227/ipd (accessed on 20 July 2025).
10. Alagic, G.; Bros, M.; Ciadoux, P.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Liu, Y.-K.; Miller, C.; et al. *Status Report on the Fourth Round of the Nist Post-Quantum Cryptography Standardization Process*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2025.
11. Cryptographic Suite for Algebraic Lattices. Available online: https://pq-crystals.org/kyber/index.shtml (accessed on 6 August 2025).
12. FIPS; NIST. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024.
13. Zong, C. The Mathematical Foundation of Post-Quantum Cryptography. *Research* **2024**, *8*, 0801. [CrossRef] [PubMed]
14. Liu, T.; Ramachandran, G.; Jurdak, R. Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization. *arXiv* **2024**, arXiv:2401.17538. [CrossRef]
15. Mayes, K. Performance Evaluation and Optimisation for Kyber on the MULTOS IoT Trust-Anchor. In Proceedings of the 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 14–16 August 2020.
16. Achoe, D. Post-Quantum Cryptography for Securing Future-Proof Smart Energy Infrastructure. 2025. Available online: https://www.researchgate.net/publication/392734298_POST-QUANTUM_CRYPTOGRAPHY_FOR_SECURING_FUTURE-PROOF_SMART_ENERGY_INFRASTRUCTURE (accessed on 20 July 2025).
17. Kumari, S.; Singh, M.; Singh, R.; Tewari, H. Post-quantum cryptography techniques for secure communication in resource-constrained Internet of Things devices: A comprehensive survey. *Softw. Pract. Exp.* **2022**, *52*, 2047–2076. [CrossRef]
18. Mahdi, L.H.; Abdullah, A.A. Fortifying Future IoT Security: A Comprehensive Review on Lightweight Post-Quantum Cryptography. *Eng. Technol. Appl. Sci. Res.* **2025**, *15*, 21812–21821. [CrossRef]
19. Chung, C.C.; Pai, C.C.; Ching, F.S.; Wang, C.; Chen, L.J. When post-quantum cryptography meets the internet of things. In Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services, Portland, Oregon, 27 June–1 July 2022.
20. Tasopoulos, G.; Li, J.; Fournaris, A.P.; Zhao, R.K.; Sakzad, A.; Steinfeld, R. Performance Evaluation of Post-Quantum TLS 1.3 on Resource-Constrained Embedded Systems. In *Information Security Practice and Experience*; Springer: Cham, Germany, 2022.
21. Abbasi, M.; Cardoso, F.; Váz, P.; Silva, J.; Martins, P. A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments. *Cryptography* **2025**, *9*, 32. [CrossRef]
22. Blanco-Romero, J.; Lorenzo, V.; Almenares, F.; Sánchez, D.D.; Campo, C.; Rubio, C.G. Integrating Post-Quantum Cryptography into CoAP and MQTT-SN Protocols. In Proceedings of the 2024 IEEE Symposium on Computers and Communications (ISCC), Paris, France, 26–29 June 2024.
23. Paul, S.; Schick, F.; Seedorf, J. TPM-Based Post-Quantum Cryptography: A Case Study on Quantum-Resistant and Mutually Authenticated TLS for IoT Environments. In Proceedings of the ARES'21: The 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021.
24. Kumar, R.; Goyal, R. Top Threats to Cloud: A Three-Dimensional Model of Cloud Security Assurance. In *Computer Networks and Inventive Communication Technologies*; Springer: Singapore, 2021; pp. 683–705.
25. Almutairi, M.; Sheldon, F.T. IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. *Electronics* **2025**, *14*, 1394. [CrossRef]
26. Blog, A.S. How to Tune TLS for Hybrid Post-Quantum Cryptography with Kyber. AWS. 2022. Available online: https://aws.amazon.com/blogs/security/how-to-tune-tls-for-hybrid-post-quantum-cryptography-with-kyber/#: :text=How%20to%20tune%20TLS%20for,Maven%20project%20to%20use (accessed on 20 July 2025).
27. Hazber, M.A.G.; Albarrak, A.; Altamimi, M.; Muniasamy, A.; Islam, A.; Ahmed, M.A.; Alalayah, K.M.; Hussain, S.; Irshad, R.R. A blockchain-enabled edge computing framework leveraging artificial neural network and aquila optimization to enhance security and scalability of cloud-based IoT platforms. *Clust. Comput.* **2025**, *28*, 816. [CrossRef]

28. Kim, Y.B.; Seo, S.C. An Optimized Instantiation of Post-Quantum MQTT protocol on 8-bit AVR Sensor Nodes. In Proceedings of the ASIA CCS'25: The 20th ACM Asia Conference on Computer and Communications Security, Hanoi, Vietnam, 25–29 August 2025.
29. Commey, D.; Appiah, B.; Klogo, G.S.; Bagyl-Bac, W.; Gadze, J.D.; Alsenani, Y.; Crosby, G.V. Performance Analysis and Deployment Considerations of Post-Quantum Cryptography for Consumer Electronics. *arXiv* **2025**, arXiv:2505.02239. [CrossRef]
30. Hanna, Y.; Bozhko, J.; Tonyali, S.; Harrilal-Parchment, R.; Cebe, M.; Akkaya, K. A comprehensive and realistic performance evaluation of post-quantum security for consumer IoT devices. *Internet Things* **2025**, *33*, 101650. [CrossRef]
31. Ehsan, M.A.; Alayed, W.; Rehman, A.U.; Hassan, W.; Zeeshan, A. Post-Quantum KEMs for IoT: A Study of Kyber and NTRU. *Symmetry* **2025**, *17*, 881. [CrossRef]
32. Önder, E. Measuring the Performance of Post-Quantum Cryptography on Embedded Systems. Ph.D. Thesis, Worcester Polytechnic Institute, Worcester, MA, USA, 2021.
33. Hanafi, B.; Ali, M. Analyzing the research impact in post quantum cryptography through scientometric evaluation. *Discov. Comput.* **2025**, *28*, 32. [CrossRef]
34. Bernstein, D.J.; Bhargavan, K.; Bhasin, S.; Chattopadhyay, A.; Chia, T.K.; Kannwischer, M.J.; Paiva, T.; Ravi, P.; Tamvada, G. KyberSlash: Exploiting secret-dependent division timings in Kyber implementations. *Cryptology ePrint Archive*. 2024. Available online: https://eprint.iacr.org/2024/1049 (accessed on 20 July 2025).
35. Iavich, M.; Kuchukhidze, T. Investigating CRYSTALS-Kyber Vulnerabilities: Attack Analysis and Mitigation. *Cryptography* **2024**, *8*, 15. [CrossRef]
36. Sanal, P.; Karagoz, E.; Seo, H.; Azarderakhsh, R.; Mozaffari-Kermani, M. *Kyber on ARM64: Compact Implementations of Kyber on 64-Bit ARM Cortex—A Processors*; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Cham, Germany, 2021.
37. Canto, A.C.; Kaur, J.; Kermani, M.M.; Azarderakhsh, R. Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security. *arXiv* **2023**, arXiv:2305.13544. [CrossRef]
38. Taghavi, B.; Azarderakhsh, R.; Kermani, M.M. ParallelNTT: Maximizing Performance of Forward and Inverse NTT on FPGA for ML-DSA and ML-KEM. In Proceedings of the Great Lakes Symposium on VLSI 2025, New Orleans, LA, USA, 30 June–2 July 2025.