ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Navigating the NIST PQC Standards: Trade-offs and Case Studies

Anna Wiktoria Dybel | Department of Computer Sciences and Mathematics, Cracow University of Technology, Poland | ORCID: 0009-0009-5896-5976

Joanna Kołodziej | NASK – National Research Institute, Poland | ORCID: 0000-0002-5181-8713

Abstract

The rapid advancement of quantum computing poses a significant threat to classical cryptographic systems, particularly to widely used public-key schemes that rely on integer factorisation and the discrete logarithm problem. To ensure long-term data security against potential quantum adversaries, post-quantum cryptography (PQC) is currently standardised by the National Institute of Standards and Technology (NIST). This paper goes beyond a theoretical overview by employing a systematic methodology to evaluate the empirical performance trade-offs of the newly standardised algorithms (ML-KEM, ML-DSA, and SLH-DSA) and key finalists (FN-DSA and HQC). Based on a comprehensive review of fragmented performance data, the work presents a comparative analysis focusing on data overhead, computational latency, and resource efficiency. As a primary contribution, this study proposes a deployment-oriented taxonomy that explicitly maps these PQC standards to optimal practical use cases, considering diverse constraints across Internet of Things, cloud environments, and blockchain networks. Furthermore, the paper addresses critical real-world deployment challenges, such as vulnerabilities to side-channel attacks and hardware-level implementation constraints. Ultimately, this work systematises current knowledge into

Received: 18.02.2026

Accepted: 29.04.2026

Published: 15.07.2026

Cite this article as:
A.W. Dybel, J. Kołodziej "Navigating the NIST PQC standards: Trade-offs and case studies," ACIG, vol. 5, no. 2, pp. 201–203, 2026, doi: 10.60097/ACIG/221494

Corresponding author:
Anna Wiktoria Dybel, Department of Computer Sciences and Mathematics, Cracow University of Technology, Poland;
E-mail: anna.dybel@doktorant.pk.edu.pl
0009-0009-5896-5976

a unified decision-making framework, guiding system architects in complex migration towards a quantum-resilient digital ecosystem.

Keywords
cybersecurity, PQC, cryptography, NIST, quantum-resistant

1. Introduction

Cryptography predates the digital era, as the need for secure information exchange over insecure channels existed independently of computing systems. It has evolved significantly from simple substitution ciphers to algorithms based on intractable mathematical problems that even the most powerful machines cannot solve. Historical trends demonstrate that methods perceived as secure at their inception may become vulnerable as knowledge and technology advance. It has emerged that classical public-key schemes, such as the Rivest–Shamir–Adleman (RSA) [1] and elliptic curve cryptography (ECC), which have stood as foundational elements of secure communication for more than 40 years, are vulnerable to quantum computing. Although quantum computers capable of compromising current public-key cryptography do not yet exist, the advancement of quantum computing makes the transition to quantum-resistant algorithms necessary. Therefore, research communities, standardisation organisations, and the technology sector are undertaking efforts to build a quantum-resilient digital ecosystem to protect sensitive data.

Quantum computing introduces a computational paradigm that offers capabilities that classical computing cannot achieve. Its potential lies not in performing classical algorithms faster but in leveraging quantum mechanics to develop new algorithms for specific problems. This technology holds immense promise for fields, such as drug discovery [2, 3] and materials science, enabling outcomes that remain beyond the scope of classical technologies. Despite the benefits, this computational power could pose a significant threat to cryptographic systems [4–6]. In particular, Shor's [7] and Grover's [8] algorithms could efficiently break widely used cryptographic schemes.

To mitigate the risk posed by quantum computing, two approaches have been devised: quantum key distribution (QKD) [9] and post-quantum cryptography (PQC). QKD is grounded in the fundamental principles of quantum mechanics, whereby any attempt to eavesdrop disturbs the system and reveals the adversary's

presence. PQC is based on new mathematical problems that are deemed intractable by quantum and classical computing. Currently, PQC is prioritised due to its feasibility to deploy on classical infrastructures.

This paper provides an overview of PQC identified during the National Institute of Standards and Technology (NIST) selection process. These standards are described in terms of their performance, with emphasis on key sizes and cryptographic operation speed. While the existing literature often presents isolated benchmarks focusing on single domains like Internet of Things (IoT) or blockchain, or offers general theoretical reviews, this paper contributes a unified and comprehensive taxonomy. Rather than examining metrics in vacuum, this work consolidates fragmented performance data from various independent studies to create a centralised guide for making decisions. This unified framework explicitly maps algorithms standardised by NIST to their optimal practical use cases across multiple technological domains, accounting for hardware and network constraints. The content is supplemented by case studies illustrating the implementation of selected standards in security scenarios. Overall, this provides a better understanding of the challenges associated with deploying new standards in classical cryptography.

The rest of the paper is organised as follows. Section 2 demonstrates the emerging risks posed to classical cryptography by quantum computing. Section 3 introduces the research methodology and decision framework used to develop the taxonomy. Section 4 introduces post-quantum primitives and categorises their mathematical foundations. Section 5 reviews the NIST standardisation process, followed by Section 6, which specifies the security strength levels. Section 7 presents a comparative study of NIST finalists, with a particular focus on performance benchmarks and analysing the suitability of their parameter sets for specific use cases. Finally, Section 8 summarises the analysis and concludes the paper.

2. Vulnerabilities in Classical Cryptography

Shor's algorithm was published by Peter Shor in 1994 [7], which poses a threat to RSA and ECC. This algorithm can solve integer factorisation and discrete logarithm problems exponentially faster than classical computers by leveraging a fundamental feature of quantum computing: quantum parallelism, which enables simultaneous operations on multiple inputs and the computation of periods via Quantum Fourier Transform [10]. Grover's algorithm

was introduced by Lov Grover in 1996 [8] to enhance the efficiency of searching unsorted databases. It leverages quantum parallelism to achieve a quadratic speedup. However, it could be useful in brute-force attacks on symmetric encryption keys, reducing their strength by about half [11].

The Harvest now, decrypt later (HNDL) strategy poses a particular threat to data with a long lifecycle, such as medical, governmental, or military records. This approach allows adversaries to intercept and archive encrypted data today with the intent of decrypting it when sufficiently powerful quantum computers could be capable of executing both Shor's and Grover's algorithms [12, 13].

The scale and complexity of this challenge are unprecedented since the deployment of public-key cryptography. Despite improved tools and awareness, previous experience suggests that this transition is a lengthy process. However, the HNDL threat demands immediate action to secure data against future compromise. Given that migration could span a decade or more, significant public and private sector resources are now focused on developing and deploying quantum-resistant solutions [14, 15]. The proposed mitigation steps against quantum threats are summarised in Table 1 [16].

3. Research Methodology and Decision Framework

To bridge the gap between theoretical PQC specifications and practical implementation, this survey employs a systematic

Table 1. HNDL mitigation strategy.

Phase	Strategic objective	Technical scope and implementation
I. Discovery	Cryptographic Agility Assessment	dentify all cryptographic primitives across the infrastructure stack, including TLS/SSL, IPsec VPNs, internal applications, and cloud-native integrations
II. Analysis	Information Shelf-life Stratification	Classify data based on sensitivity and required secrecy duration. Assets with a longevity ≥ 3-5 years are designated as high–priority targets for HNDL mitigation.
III. Isolation	Critical Vector Prioritization	Focus security hardening on long–lived, high–sensitivity traffic: VPN tunnels, database persistence layers, and software distribution systems.
IV. Migration	Hybrid Protocol Deployment	Transition to Hybrid Cryptographic Schemes combining classical algorithms with NIST–standardized PQC.
V. Governance	Vendor and Channel Assurance	Enforce PQC roadmaps across the supply chain. Prioritize securing the communication channel (e.g., MACsec, TLS) to protect data in transit from interception.

comparative analysis guided by a core research question: How do the empirical performance trade-offs of NIST-standardised algorithms dictate their optimal deployment across diverse technological environments characterised by strict hardware and bandwidth constraints? To answer this, the research design follows a strict three-phase methodology, such as literature selection, criteria formulation, and use-case mapping.

First, empirical performance data were collected from peer-reviewed literature and official NIST reports, intentionally focusing on practical metrics rather than purely mathematical foundations. The scientific validity of this approach relies on cross-referencing results from multiple independent benchmarks, providing a more comprehensive and statistically robust evaluation than a single experimental setup.

Second, to establish a rigorous basis for the proposed taxonomy, the algorithms were compared across three explicit criteria:

- Data overhead: Public key, signature, and ciphertext sizes, representing primary bandwidth constraints and network latency factors.
- Computational latency: Execution time required for critical cryptographic operations, such as key generation, encapsulation, signing, and verification.
- Resource efficiency: Energy consumption and computational footprint, dictating feasibility for resource-constrained IoT and edge devices.

Finally, the taxonomy was constructed by mapping the empirical performance profiles of each algorithm against the strict requirements of various technological environments. Algorithms demonstrating low energy consumption and efficient execution times were mapped to resource-constrained IoT devices. Schemes characterised by highly compact signatures but intensive computational requirements were assigned to bandwidth-limited environments, such as blockchain networks. Conversely, algorithms prioritising conservative security models with large data overheads were designated exclusively for high-integrity offline tasks, including firmware updates.

4. Post-Quantum Cryptography and Core Families

Post-quantum cryptography aims to develop algorithms based on new mathematical problems that remain resistant to both

conventional and quantum algorithms. PQC is divided into the following five categories [17]:

- *Lattice-based cryptography* is the most versatile family of PQCs that offers an optimal balance between robustness and efficiency. The foundation of this family lies in two hard mathematical problems, such as shortest vector problem (SVP) and learning with errors (LWE), which offer reductions from worst-case lattice problems, ensuring that breaking an average key is as difficult as solving the toughest possible instance [18].
- *Code-based cryptography* builds upon the computational difficulty of decoding random linear error-correcting codes and offers strong security guarantees due to 45 years of cryptanalysis. Despite this, code-based cryptography schemes require large public keys.
- *Hash-based cryptography* [19] provides the most mathematically conservative security foundation in PQC, relying exclusively on hash function security, rather than complex mathematical assumptions that might be vulnerable to future cryptanalytic advances or unexpected algorithmic breakthroughs. Hash-based cryptography can be divided into two main approaches, stateful and stateless. Stateful schemes offer relatively small signatures, but their practical use is challenging because each key pair can sign only a limited number of messages, necessitating strict state management. In contrast, stateless schemes eliminate the need for tracking keys but incur significantly larger signature sizes.
- *Isogeny-based cryptography*, which relies on the hardness of computing isogenies between supersingular elliptic curves to offer exceptionally small public-key sizes. Nevertheless, one of its algorithms, supersingular isogeny key encapsulation (SIKE), was compromised by classical computation.
- *Multivariate cryptography* [20] relies on the non-deterministic polynomial (NP)-hard problem of solving systems of non-linear multivariate quadratic equations over finite fields. It outperforms competitors in speed by using simple addition and multiplication over small finite fields, making it ideal for low-cost IoT devices, such as radio frequency identification (RFID) chips. Although it provides exceptionally short signatures compared to other post-quantum algorithms, it often lacks formal security proofs; notably, the Rainbow signature scheme was significantly compromised by a classical attack.

5. NIST PQC Standardisation

National Institute of Standards and Technology launched its multi-year standardisation initiative in 2016, which aims to establish

quantum-resistant cryptography methods (including key encapsulation mechanisms and digital signatures) capable of withstanding attacks from both classical and quantum computers [21–25]. Initially, 82 submissions were received and subsequently evaluated through rigorous cryptanalysis and performance benchmarking over several years. The evaluation was based on security, cost, and performance criteria as well as algorithm and implementation characteristics [21]. In 2022, NIST announced four selected algorithms to be standardised: CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, and SPHINCS+ [23].

Although NIST selected the winners, it decided to launch a fourth evaluation round that included Classic McEliece, Bike, hamming quasi-cyclic (HQC), and SIKE. This decision was motivated by the need to diversify key establishment methods and the desire to select an algorithm based on an alternative mathematical problem. It was widely expected that the selection would be a two-horse race between HQC and BIKE. SIKE had already been broken, and Classic McEliece was considered unsuitable for general use, given its large public keys [26]. Consequently, in this phase, which concluded in March 2025, NIST additionally selected HQC, which relies on quasi-cyclic codes [27]. Furthermore, HQC shares similarities with LWE-based cryptosystems, such as ML-KEM [28]. According to the official NIST report, Classic McEliece was a strong candidate, despite generating large keys. It was not selected due to the risk of conflict with concurrent efforts within standards of the International Organisation for Standardisation (ISO) and concerns regarding the creation of incompatible standards. It was determined that the benefits of deploying this algorithm in niche applications did not outweigh the costs associated with increased migration complexity, given that the primary priority was a general-purpose solution. Consequently, NIST decided to omit this algorithm for now, without ruling out the possibility of adopting the ISO standard in future [25].

In 2024, NIST published the first final Federal Information Processing Standards (FIPS) [29–31], formalising their new names:

- Module-Lattice Key Encapsulation Mechanism (ML-KEM), standardised as FIPS 203 [29], is derived from the CRYSTALS-Kyber algorithm [32]. It is a key encapsulation mechanism that relies on lattice cryptography and the learning with errors problem, offering a balance between strong security and the computational efficiency of cryptographic operations, and generating relatively compact key sizes. Therefore, ML-KEM is the primary KEM

standard defined by NIST. The transformation of CRYSTALS-Kyber into ML-KEM involved several significant modifications, including adjustments to the Fujisaki–Okamoto transformation and changes to secret-key management, encapsulation algorithms, and randomness generation.

- Module–Lattice Digital Signature Algorithm (ML-DSA), adopted as the FIPS 204 standard [30], is directly based on the CRYSTALS-Dilithium algorithm [33]. It is a lattice-based digital signature scheme that relies on the hardness of the module-learning with errors (M-LWE) problem, which gives strong security proofs and efficient cryptographic operations. Although it generates large signature sizes, its implementation does not require complex operations, such as floating-point operations.
- Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), standardised as FIPS 205 [31], is based on the SPHINCS+ algorithm, which is a stateless, hash-based signature scheme that offers a highly conservative security model relying on the robustness of cryptographic hash functions rather than algebraic assumptions. Although it provides a reliable long-term security hedge, it entails substantial performance trade-offs, including significantly larger signature sizes and higher signing latency [34].
- Falcon Digital Signature Algorithm (FN-DSA), identified in the summary listings as FIPS 206, is derived from the Falcon algorithm [35], which is a lattice-based signature scheme utilising NTRU lattices with Fast Fourier Sampling to achieve high computational efficiency and exceptionally compact signature sizes. Although it minimises network overhead and energy consumption, its reliance on complex floating-point arithmetic introduces significant implementation challenges and susceptibility to side-channel vulnerabilities.

To date, neither HQC nor Falcon has been standardised. However, the initial draft standard for Falcon (FIPS 206) is expected to be released imminently [36]. NIST continues its efforts to standardise additional digital signature schemes to ensure cryptographic diversity. The objective is to find solutions characterised by compact signatures and based on mathematical problems distinct from the lattice. In 2026, NIST is expected to select candidates from a group of 14 to the third round of additional digital signature schemes process [24].

6. NIST's Security Strength

A crucial aspect of analysing cryptographic algorithms is security assessment, which provides insight into their resilience

against attacks. Although quantum computing poses a major threat to the current cryptographic system, predicting its true capabilities, such as speed and memory size, is challenging. Therefore, NIST proposed and developed broad categories of security strength for PQC. Rather than relying on specific bit-security estimates for submitted algorithms, these categories are benchmarked against the computational resources required to compromise the existing standards, specifically the AES block cipher family and the SHA hash functions. This approach explicitly accounts for quantum algorithmic threats, such as Grover's algorithm. A detailed classification of these five security levels is provided in Table 2 [11, 26, 37]. Table 3

Table 2. NIST security levels.

Level	Algorithm
I	AES–128
II	SHA–256
III	AES–192
IV	AES–384
V	AES–256

Table 3. NIST post-quantum cryptography security levels for selected algorithms.

Type	Algorithm	Standard	Security
Lattice-based	CRYSTALS–KYBER–512	ML–KEM–512	Level 1
	CRYSTALS–KYBER–768	ML–KEM–768	Level 3
	CRYSTALS–KYBER–1024	ML–KEM–1024	Level 5
	CRYSTALS–Dilithium2	ML–DSA–44	Level 1
	CRYSTALS–Dilithium3	ML–DSA–65	Level 3
	CRYSTALS–Dilithium5	ML–DSA–87	Level 5
	Falcon–512 (FN–DSA–512)	FN–DSA–512	Level 1
	Falcon–1024 (FN–DSA–1024)	FN–DSA–1024	Level 5
Hash-based	SPHINCS+–128	SLH–DSA–128 (s/f)	Level 1
	SPHINCS+–192	SLH–DSA–192 (s/f)	Level 3
	SPHINCS+–256	SLH–DSA–256 (s/f)	Level 5
Code-based	HQC–128	—	Level 1
	HQC–192	—	Level 3
	HQC–256	—	Level 5

demonstrates the security levels that are available for each of the PQC algorithms.

7. Overview of NIST Finalists

In this section, we present a comparative analysis of PQC finalists. Notably, these algorithms belong to different families based on distinct mathematical problems, which lead to differences in key and signature sizes and performance. Therefore, this aspect is critical within the context of hardware constraints, as the existing infrastructure is frequently ill-equipped to meet the substantial memory and computational demands imposed by these emerging standards. Increased data sizes may lead to latency and performance bottlenecks, presenting a significant implementation challenge for resource-constrained systems. Consequently, analysis of performance and hardware compatibility is widely regarded as a fundamental complement to the verification of theoretical security of these algorithms [38]. Comparison of post-quantum schemes with classical ones is crucial for assessing their readiness for deployment.

7.1. Key Encapsulation Mechanism Schemes

Although PQC is widely considered slower than classical cryptography, most performance analyses indicate that PQC is comparable to classical algorithms and can be significantly better [39–41]. A prominent illustration of this is Sosnowski et al. [40], which presents testing across a range of hardware environments that indicates that ML-KEM-512 executes approximately three times faster than X25519 elliptic curve Diffie–Hellman across all security levels, whereas its communication overhead is only moderate [17].

However, this computational efficiency is often offset by network-layer challenges. A detailed examination of ML-KEM-768 presented in Wang and Shahril Ismail [42] demonstrates that, despite a 15-20% increase in transport layer security (TLS) handshake latency relative to RSA, the algorithm exceeds classical Elliptic Curve Diffie–Hellman Ephemeral (ECDHE) in computational efficiency by requiring significantly fewer CPU cycles. Although public-key sizes surpass those of current RSA or ECC standards, they remain considerably more compact and bandwidth-efficient than alternative post-quantum schemes, such as McEliece, which utilises keys several orders of magnitude larger. Furthermore, the combination of robust security and minimal power requirements positions ML-KEM as a viable solution for resource-constrained environments.

Abbasi et al. [43] presents a comprehensive benchmarking study conducted across three distinct hardware architectures, such as a cloud server, a user laptop, and an IoT device. The results demonstrate that ML-KEM consistently exhibits superior performance and energy efficiency compared to other evaluated key encapsulation mechanisms. Notably, ML-KEM consumes up to three times less energy than alternative KEM schemes, making it a strong candidate for resource-constrained edge devices. Through targeted library optimisations, the authors achieved performance improvements of 12.5%–16.7% over NIST reference benchmarks. Furthermore, in key generation tasks, ML-KEM was more than three orders of magnitude faster than RSA-3072. Additionally, its integration into the TLS protocol introduces minimal overhead and negligible packet fragmentation, while the algorithm demonstrates near-linear scalability in server environments.

Hamming quasi-cyclic has been selected recently for standardisation as a backup; consequently, its analysis is not yet as extensive as its counterpart ML-KEM. Nonetheless, comparative studies indicate that its performance is relatively slower and it also requires a larger bandwidth than ML-KEM. Its encapsulation keys require 2241 bytes, whereas ML-KEM keys require only 800 bytes for security level 1, which may be a disadvantage in bandwidth-constrained systems. A detailed comparison of these parameters, highlighting differences in key sizes and ciphertext lengths between the two algorithms, is presented in Table 4. Furthermore, Truong et al. [28] mentioned that the resources-constrained implementation of HQC is feasible, which was broad in Kim et al. [44].

The computational superiority of ML-KEM over classical ECDHE stems directly from its mathematical foundations. Built upon the module-LWE problem, its core operations rely on efficient matrix multiplication and polynomial addition, enabling highly optimised, low-energy implementations. Conversely, the substantial communication overhead of HQC is an inherent architectural constraint derived from decoding random linear error-correcting codes, rather than a mere software limitation. This fundamental theoretical divergence between lattice- and code-based paradigms explicitly justifies prioritising ML-KEM for bandwidth sensitive protocols like TLS in the proposed taxonomy.

7.2. Digital Signatures Schemes

Digital signatures underpin secure communication and data integrity by verifying the identity of the message's author.

Table 4. Sizes of keys and ciphertexts (in bytes) of PQC KEM standards.

Parameters	ML-KEM			HQC		
	1	3	5	1	3	5
Encapsulation key	800	1184	1568	2241	4514	7237
Decapsulation key	1632	2400	3168	2321	4602	7333
Ciphertext	768	1088	1568	4433	8978	14421
Shared secret key	32	32	32	32	32	32

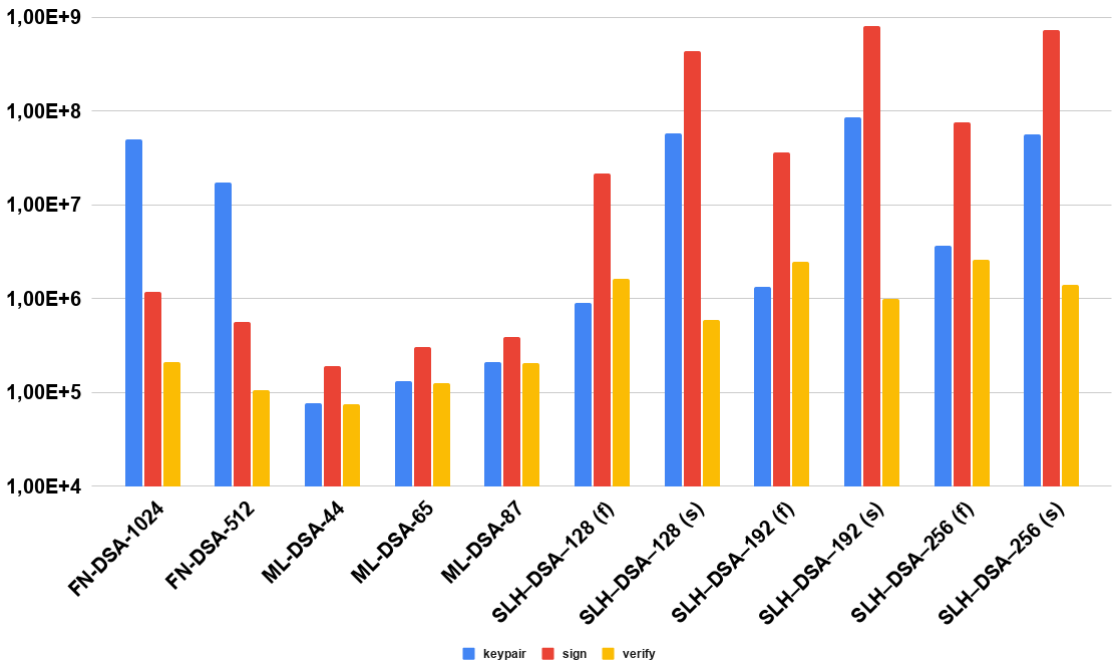

Figure 1. DSA benchmarks on an x86-64 processor with AVX2 extensions measured in clock cycles.

The analysis of digital signatures should focus on evaluating the time required for critical cryptographic operations, the key and cipher sizes, and the implementation vulnerabilities to determine their feasibility for deployment across different platforms. Figure 1 presents signature benchmarks on an x86-64 processor using data from the Open Quantum Safe open-source initiative [45]. The presented data clearly illustrate the differences between implemented standards, especially SLH-DSA.

According to Kim et al. [44], which employed a practical benchmark, ML-DSA offers efficient signing but requires substantially larger keys and signatures than classical RSA; therefore, its use is challenged in

Table 5. Sizes of key and signature (in bytes) of PQC digital signatures schemes.

Standard	Security level	Public key	Signature	Private key
ML-DSA-44	Level 2	1312	2420	2560
ML-DSA-65	Level 3	1952	3309	4032
ML-DSA-87	Level 5	2592	4627	4896
FN-DSA-512	Level 1	897	666	1281
FN-DSA-1024	Level 5	1793	1280	2305
SLH-DSA-128 (s/f)	Level 1	32	7856/17088	64
SLH-DSA-192 (s/f)	Level 3	48	16224/35664	96
SLH-DSA-256 (s/f)	Level 5	64	29792/49856	128

network-constrained systems. Comparison of ML-DSA with Falcon (FN-DSA) also yields larger keys and signatures and slower verification times. Similarly, comparable findings were reported in Abbasi et al. [43], in which a comprehensive benchmark was conducted concerning the cryptographic operations, keys, and signatures. Based on the findings, ML-DSA might lead to packet fragmentation. Nonetheless, the benchmark demonstrates that ML-DSA offers an efficient energy profile compared to FN-DSA, which ensures favourable parallelisation potential and offers faster verification.

In Raavi et al. [41], a comprehensive performance analysis was provided comparing the digital signature schemes. The main findings indicate that SLH-DSA is fastest for signing messages longer than 3.256 MB, compared to ML-DSA and FN-DSA, although it incurs the highest network overhead. Although ML-DSA performs well in both cases, FN-DSA may be a better choice for environments with network and memory constraints. Equally to this finding, Dziechciarz and Niemiec [39] demonstrated that PQC, especially ML-DSA, indeed provides the best performance for small file size, while SLH-DSA achieves the worst performance, even compared to RSA. Moreover, this study also observes that SLH-DSA with 's' suffix generates smaller signatures, but at the expense of speed. Meanwhile, 'f' suffix achieves better performance, but at the expense of a larger signature size.

Schemitt et al. [46] conducted the simulation of the performance of PQC digital signature schemes in order to assess the feasibility of their adoption as a new standard in Bitcoin and Ethereum. These findings indicate that PQC algorithms, particularly ML-DSA and Mayo, outperform current standards across all security levels.

Moreover, Mayo is among the candidates in the second additional NIST round and may be selected for standardisation. However, the round is still going. While these findings suggest the feasibility of PQC to deploy blockchain in terms of time of operation, this study highlights that it did not evaluate the size of keys and signatures, which are significantly larger than the current ones.

In contrast, Juaristi et al. [47] presented a comprehensive benchmark assessing key and signature sizes and found that FN-DSA generates the smallest signature among PQC schemes; however, it is 19 times larger than the current standard signatures. Additionally, SLH-DSA achieved the smallest key size among other PQC alternatives. Nevertheless, each PQC scheme produces extremely large signatures relative to current standards, particularly as the security level increases. Based on these findings, the study concluded that ML-DSA-44 is the most balanced option.

Although SLH-DSA is known for its strong security, grounded in the well-understood properties of cryptographic hash functions, it has numerous limitations due to its stateless design. Compared to its counterparts, it offers a less favourable trade-off between security and key size [48].

The performance trade-offs observed in digital signature schemes can be directly traced back to their fundamental mathematical designs. ML-DSA's energy-efficient signing reflects its straightforward algebraic structure, which avoids complex floating-point calculations. While FN-DSA achieves highly compact signatures using NTRU lattices and Fast Fourier Sampling, this specific mathematical design becomes a severe bottleneck in constrained environments lacking hardware-accelerated floating-point arithmetic. Furthermore, the massive network overhead of SLH-DSA is the direct mathematical cost of its stateless, hash-based architecture. By avoiding structured algebraic assumptions, SLH-DSA explicitly sacrifices efficiency for conservative security, justifying its taxonomy placement as a specialised tool for offline tasks, such as firmware updates.

7.3. Taxonomy of Post–Quantum Cryptographic Techniques

The landscape of NIST-standardised algorithms presents a complex multi-criteria optimisation problem for system architects. To bridge the gap between theoretical algorithm specifications and practical deployment, this paper proposes a structured taxonomy, presented in Figure 2. Concrete application examples corresponding to these categories are listed in Table 6.

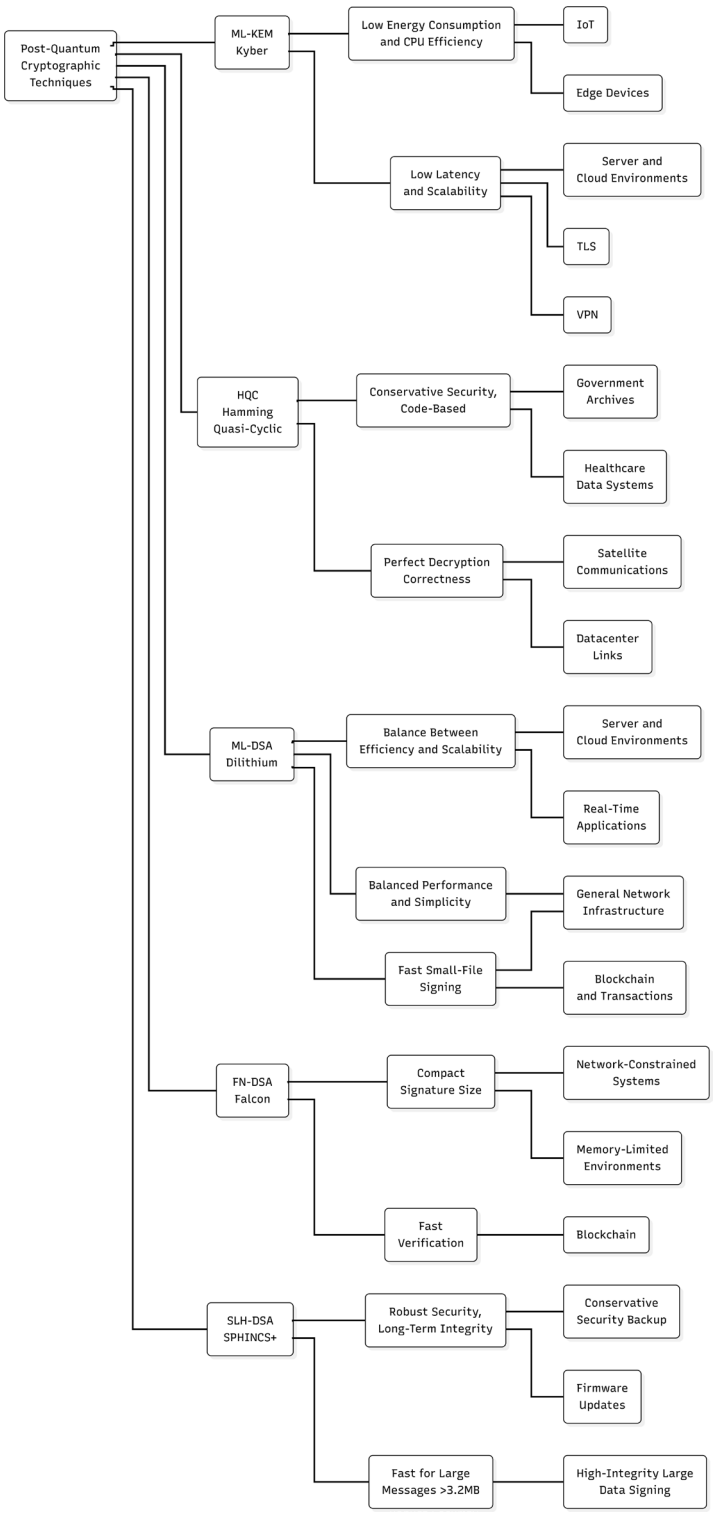

Figure 2. Taxonomy of post-quantum cryptographic techniques.

Table 6. PQC adoption depends on requirements.

Use cases	Recommended PQC	Requirements	References
Resource-constrained Devices and IoT	ML-KEM, ML-DSA	Low energy consumption and high efficiency on limited hardware	[52]
Wearable sensors and monitoring devices (Healthcare), real-time application	ML-KEM	High computational efficiency and low resource overhead	[53]
TLS Handshake, VPN, Key Exchange in 6G-AKA	ML-KEM	Low latency, and negligible packet fragmentation	[54–56]
SIM authentication in 6G-AKA	ML-DSA	Security and efficiency balance	[54]
Server and Cloud Environments	ML-KEM, ML-DSA	Scalability and minimal protocol overhead for high-volume connections	[57]
Blockchain	FN-DSA	Relatively compact signature size and efficient verification time	[39, 41]
Blockchain-based Federated Learning	ML-DSA	Fast signing and verification, manageable signature size, strong security guarantees	[58]
Firmware update	SLH-DSA	Long-term integrity, offline signing	[59]
CA	SLH-DSA	High security domains	[59]

This taxonomy is methodologically grounded in the empirical size constraints summarised in Tables 1, 4, and 5, as well as the benchmarks discussed in previous sections. By mapping specific system priorities, such as bandwidth conservation, acceptable network overhead, and conservative security assumptions, directly to corresponding algorithms, the taxonomy provides a deployment-oriented framework for PQC migration.

Within this framework, ML-KEM emerges as the most robust, general-purpose key encapsulation mechanism. As evidenced by the metrics in Table 4 and performance benchmarks, it serves as a highly efficient drop-in replacement for classical KEMs in standard protocols like TLS, achieving a favourable balance between low computational overhead and practical key sizes. To ensure crypto-agility and mitigate risks associated with lattice-based assumptions, HQC is included as a primary non-lattice fallback, offering deployable key sizes of approximately 2.2 kB that are well suited for network infrastructure.

In the context of digital signatures, ML-DSA emerges as the most balanced choice for standard network infrastructure, proving particularly effective and efficient when signing small files. However,

as evidenced in Table 5, its signature sizes can induce latency in bandwidth-constrained environments. Under such strict network or memory constraints, FN-DSA presents a better alternative, offering significantly smaller signature and public-key sizes. Nevertheless, FN-DSA requires a more complex architecture, primarily due to the use of floating-point arithmetic, which complicates secure constant-time signing [49]. Without fast floating point processing hardware, its signing operations are significantly bottlenecked, operating up to 20 times slower [50]. NIST prioritised design simplicity during its evaluation, noting that the technical complexity of FN-DSA could introduce vulnerabilities during implementation. Consequently, ML-DSA is more favourable due to its relatively straightforward and transparent structure [23].

Finally, SLH-DSA serves primarily as a conservative back-up standard, rather than a primary solution for general applications. Although its practical utility is limited by slower speeds and significant data overhead, exceeding 7.8 kB, as shown in Table 5, its selection is justified by robust security guarantees rooted in well-understood cryptographic hash functions, offering resilience distinct from structured lattice-based schemes [11].

7.4. Practical Deployment Challenges and Limitations

To fully address the deployment gap, it is crucial to recognise that the immediate integration of these standards will not occur as a strict drop-in replacement for classical algorithms. During the multi-year migration phase, industry best practices dictate the use of hybrid cryptographic schemes, which combine a classical primitive with a post-quantum standard to maintain traditional compliance while adding quantum resistance. However, this hybrid approach exacerbates the performance trade-offs outlined in this taxonomy by effectively doubling the communication overhead and computational latency during handshakes. Consequently, the proposed taxonomy becomes even more critical for system architects. Selecting an algorithm with a minimal footprint, such as ML-KEM or FN-DSA, is not merely an optimisation but a strict requirement to prevent packet fragmentation and connection timeouts when operating within a hybrid deployment framework.

Furthermore, real-world deployment must account for physical security vulnerabilities. Despite the robust theoretical security offered by algorithms like ML-KEM, their practical implementations may remain susceptible to side-channel attacks (SCAs), including timing analysis and differential power analysis. Because PQC

algorithms often require complex mathematical operations, they present new attack surfaces for adversaries observing power consumption or electromagnetic emissions. This vulnerability served as a primary motivation for the novel approach proposed by Zafar and Iqbal [51]. Rather than relying on the standard ML-KEM implementation, the authors introduced a more constrained variant supported by a fallback mechanism. Consequently, the resulting system achieves up to a 30% reduction in latency and significantly lower resource consumption, compared to conventional solutions, while maintaining high performance across both server and IoT platforms. Ultimately, securing PQC against SCAs requires constant-time implementations and hardware-level masking, adding further complexity to their widespread adoption.

8. Conclusions

This paper addresses the practical deployment challenges of PQC by synthesising empirical performance benchmarks with their underlying mathematical characteristics. The analysis demonstrates that while classical algorithms like RSA offer broad versatility across diverse applications, NIST–standardised PQC schemes entail specific operational trade-offs. These distinctions underscore the value of the proposed deployment taxonomy as a structured guide for system architects.

Beyond these contributions, the empirical data highlights that current schemes face several limitations and environment-specific constraints. Notably, SLH-DSA demonstrates that, despite offering conservative security, the massive data overhead renders it impractical for widespread deployment, particularly in bandwidth-sensitive certificate chains. Similarly, while ML-DSA provides a balanced, energy-efficient profile for general infrastructure, its relatively large signature sizes remain a networking challenge. FN-DSA mitigates the size issue but introduces critical computational bottlenecks on devices lacking hardware-accelerated floating-point arithmetic. Regarding KEMs, our performance analysis supports that ML-KEM is a proven, highly efficient solution, a finding practically validated by their adoption by major industry leaders, such as Cloudflare [56]. However, the development of optimised backup mechanisms remains a significant challenge, particularly when managing the increased network load during hybrid transition phases. These strict trade-offs underscore the need to intensify research into algorithms with more universal characteristics, as relying solely on niche solutions is insufficient for the global security ecosystem. Moreover, rapid progress in quantum computing and cryptanalysis requires

continuous assessment, as these developments could compromise cryptographic primitives much more quickly than in the past. This necessitates adopting a crypto-agility paradigm, preparing for more frequent standard rotation and continuous evaluation.

Future work will focus on extending this taxonomy by evaluating additional digital signature candidates from the ongoing NIST standardisation process. Specifically, exploring alternative mathematical approaches, such as MPC-in-the-Head or isogeny-based schemes, will proactively identify their optimal deployment environments, ensuring robust cryptographic diversity should they be standardised. Furthermore, it is essential to assess the performance of hardware-accelerated implementations. Benchmarking these primitives using FPGAs or dedicated ASIC coprocessors is crucial to mitigate their high computational and memory demands, particularly for resource-constrained IoT devices. Finally, further research must explore the practical integration of hybrid cryptographic schemes. This includes rigorously evaluating the latency and bandwidth overhead of combining classical and post-quantum algorithms within real-world protocols to ensure a secure, performant, and stable transition during the migration period.

References

[1] R.L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978, doi: 10.1145/359340.359342.

[2] S.K. Kandula, N. Katam, P.R. Kangari, A. Hijmal, R. Gurrala, M. Mahmoud, "Quantum computing potentials for drug discovery," in *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, New York, NY: IEEE, 2023, pp. 1467–1473, doi: 10.1109/CSCI62032.2023.00240.

[3] P.-H. Wang, J.-H. Chen, Y.-Y. Yang, C. Lee, Y.J. Tseng, "Recent advances in quantum computing for drug discovery and development," *IEEE Nanotechnology Magazine*, vol. 17, no. 2, pp. 26–30, 2023, doi: 10.1109/MNANO.2023.3249499.

[4] F. Barrett-danes, F. Ahmad, "Quantum computing and cybersecurity: A rigorous systematic review of emerging threats, post-quantum solutions, and research directions (2019–2024)," *Discover Applied Sciences*, vol. 7, no. 10, Art. no. 1083, 2025, doi: 10.1007/s42452-025-07322-5.

[5] C. Wang, J. Yu, Z. Pei, Q. Wang, C. Hong, "A first successful factorization of RSA-2048 integer by D-wave quantum computer," *Tsinghua Science and Technology*, vol. 30, no. 3, pp. 1270–1282, 2025, doi: 10.26599/TST.2024.9010028.

[6] A.C.H. Chen, "Implementation of Shor's algorithm: Factoring a 4096-bit integer under specific constraints," in *2025 8th International Conference on Circuit, Power & Computing Technologies (ICCPCT)*, Kollam, India, New York, NY: IEEE, 2025, pp. 440–446, doi: 10.1109/ICCPCT65132.2025.11176593.

[7] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings of 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, Los Alamitos, CA: IEEE Computer Society Press, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[8] L.K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*, 1996, arXiv:quant-ph/9605043, doi: 10.48550/ARXIV.QUANT-PH/9605043.

[9] W. Seok, K. Yu, W. Lee, "Analysis of research trends in distance extension for QKD network," in *2025 25th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Kaohsiung, Taiwan, New York City, NY: IEEE, 2025, pp. 1–3, doi: 10.23919/APNOMS67058.2025.11181424.

[10] C. Gidney, M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, 2021, doi: 10.22331/q-2021-04-15-433.

[11] R. Shajahan, K. Jain, P. Krishnan, "A survey on NIST 3rd round post quantum digital signature algorithms," in *2024 5th International Conference on Mobile Computing and Sustainable informatics (ICMCSI)*, Lalitpur, Nepal, New York City, NY: IEEE, 2024, pp. 132–140, doi: 10.1109/ICMCSI61536.2024.00027.

[12] N. Ahmed, L. Zhang, A. Gangopadhyay, "A survey of post-quantum cryptography support in cryptographic libraries," in *IEEE International Conference on Quantum Computing and Engineering (QCE)* 2025. arXiv:2508.16078, 2025, doi: 10.48550/ARXIV.2508.16078.

[13] H. Khaled, M.A. Metawei, S.M. Saif, M. Taher, S. M. Nassar, "Unveiling the threat: Quantum factorization techniques and their impact on RSA cryptosystems," in *2025 International Telecommunications Conference (ITC-Egypt)*, Cairo, New York City, NY: IEEE, 2025, pp. 48–55, doi: 10.1109/ITC-Egypt66095.2025.11186634.

[14] A. Regenscheid, "Transition to post-quantum cryptography standards," NIST paper IR 8547 ipd. Gaithersburg, MD: National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.IR.8547.ipd.

[15] J. Cho, C. Lee, E. Kim, J. Lee, B. Cho, "Software-defined cryptography: A design feature of cryptographic agility," arXiv:2404.01808v2, 2024, doi: 10.48550/ARXIV.2404.01808.

[16] J. Chawla, J. Chawla (Apr. 28, 2025). *Defending against HNDL attacks today*. [Online]. Available: https://blogs.cisco.com/innovation/defending-against-hndl-attacks-today. [Accessed: Jan. 31, 2026].

[17] G. Chhetri, S. Somvanshi, P. Hebli, S. Brotee, S. Das, "Post-quantum cryptography and quantum-safe security: A comprehensive survey," arXiv:2510.10436, 2025, doi: 10.48550/ARXIV.2510.10436.

[18] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," arXiv:2401.03703v1, 2024, doi: 10.48550/ARXIV.2401.03703.

[19] L. Li, X. Lu, K. Wang, "Hash-based signature revisited," *Cybersecurity*, vol. 5, no. 1, Art. no. 13, 2022, doi: 10.1186/s42400-022-00117-w.

[20] J. Ding, A. Petzoldt, "Current state of multivariate cryptography," *IEEE Security & Privacy*, vol. 15, no. 4, pp. 28–36, 2017, doi: 10.1109/MSP.2017.3151328.

[21] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, et al., "Status report on the first round of the NIST post-quantum cryptography standardization

process," NIST report IR 8240, Jan. 2019. Gaithersburg, MD: National Institute of Standards and Technology, 2019, doi: 10.6028/NIST.IR.8240.

[22] D. Moody, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, et al., "Status report on the second round of the NIST post-quantum cryptography standardization process," NIST report NIST IR 8309, Jul. 2020. Gaithersburg, MD: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.IR.8309.

[23] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, et al., "Status report on the third round of the NIST post-quantum cryptography standardization process," NIST report IR 8413-upd1, Sep. 29. Gaithersburg, MD: National Institute of Standards and Technology, 2022, doi: 10.6028/NIST.IR.8413-upd1.

[24] G. Alagic, M. Bros, P. Ciadoux, D. Cooper, Q. Dang, et al., "Status report on the first round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process," NIST report IR 8528, Oct. 24. Gaithersburg, MD: National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.IR.8528.

[25] G. Alagic, M. Bros, P. Ciadoux, D. Cooper, Q. Dang, et al., "Status report on the fourth round of the NIST post-quantum cryptography standardization process," NIST report IR 8545, Mar. 11. Gaithersburg, MD: National Institute of Standards and Technology, 2025, doi: 10.6028/NIST.IR.8545.

[26] S.M.R. Hosseini, "A comprehensive review of post-quantum cryptography: Challenges and advances." Cryptology ePrint Paper 2024/1940. [Online]. Available: https://eprint.iacr.org/2024/1940. [Accessed: Feb. 14, 2026].

[27] C. Aguilar-Melchor, O. Blazy, J.-C. Deneuville, P. Gaborit, G. Zemor, "Efficient encryption from random quasi-cyclic codes," *IEEE Transactions on Information Theory*, vol. 64, no. 5, pp. 3927–3943, 2018, doi: 10.1109/TIT.2018.2804444.

[28] Q.D. Truong, H. Nguyen, T.T. Nguyen, H. Lee, "NIST post-quantum cryptography standards: A comprehensive review of theoretical foundations and implementations," *IEEE Access*, vol. 14, pp. 14069–14097, 2026, doi: 10.1109/ACCESS.2026.3654142.

[29] National Institute of Standards and Technology (NIST), "Module-lattice-based key-encapsulation mechanism standard," *NIST report FIPS 203*, 2024. Washington, DC: NIST, 2024, doi: 10.6028/NIST.FIPS.203.

[30] National Institute of Standards and Technology (NIST), "Module-lattice-based digital signature standard," *NIST report FIPS 204*, 2024. Washington, DC: NIST, 2024, doi: 10.6028/NIST.FIPS.204.

[31] National Institute of Standards and Technology (NIST), "Stateless hash-based digital signature standard," *NIST report FIPS 205*, 2024. Washington, DC: NIST, 2024, doi: 10.6028/NIST.FIPS.205.

[32] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, et al., "CRYSTALS-kyber: A CCA-secure module-lattice-based KEM," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. London: IEEE, 2018, pp. 353–367, doi: 10.1109/EuroSP.2018.00032.

[33] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, et al., "CRYSTALS-dilithium: A lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 1, pp. 238–268, 2018, doi: 10.46586/tches.v2018.i1.238-268.

[34] D.J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, et al., "SPHINCS: Practical stateless hash-based signatures," in *Advances in cryptology – EUROCRYPT 2015*, vol. 9056, E. Oswald, M. Fischlin, Eds., Berlin: Springer, 2015, pp. 368–397, doi: 10.1007/978-3-662-46800-5_15.

[35] P.-A. Fouque, J. Hoffstein, K. Kirchner, V. Lyubashevsky, T. Pornin, et al., "Falcon: Fast-fourier lattice-based compact signatures over NTRU," in submission to the NIST's Post-Quantum Cryptography Standardization Process, pp. 1–75, 2018.

[36] R. Perlner, "FIPS 206 status update," presented at the 6th PQC Standardization Conference, Gaithersburg, MD, USA, Sep. 2025. [Online]. Available: https://csrc.nist.gov/presentations/2025/fips-206-fn-dsa-falcon. [Accessed: Jan. 29, 2026].

[37] V. Chouhan, M. Aldarwbi, S. Sadeghi, A. Ghorbani, A. Chow, et al., "Assessing the quantum readiness of cryptographic standards: Recommendations toward quantum-era compliance," *Computer Standards & Interfaces*, vol. 97, pp. 104–114, 2026, doi: 10.1016/j.csi.2025.104114.

[38] I. Laktionov, G. Diachenko, D. Moroz, I. Getman, "A comprehensive review of cybersecurity threats to wireless infocommunications in the quantum-age cryptography," *IoT*, vol. 6, no. 4, Art. no. 61, 2025, doi: 10.3390/iot6040061.

[39] D. Dziechciarz, M. Niemiec, "Efficiency analysis of NIST-standardized postquantum cryptographic algorithms for digital signatures in various environments," *Electronics*, vol. 14, no. 1, Art. no. 70, 2024, doi: 10.3390/electronics14010070.

[40] M. Sosnowski, F. Wiedner, E. Hauser, L. Steger, D. Schoinianakis, et al., "The performance of post-quantum TLS 1.3," in *Companion of the 19th international conference on emerging networking eXperiments and technologies*, Paris, New York, NY: ACM, Dec. 5, 2023, pp. 19–27, doi: 10.1145/3624354.3630585.

[41] M. Raavi, Q. Khan, S. Wuthier, P. Chandramouli, Y. Balytskyi, et al., "Security and performance analyses of post-quantum digital signature algorithms and their TLS and PKI integrations," *Cryptography*, vol. 9, no. 2, Art. no. 38, 2025, doi: 10.3390/cryptography9020038.

[42] Y. Wang, E. Shahril Ismail, "A review on the advances, applications, and future prospects of post-quantum cryptography in blockchain and IoT," *IEEE Access*, vol. 13, pp. 112 962–112 977, 2025, doi: 10.1109/ACCESS.2025.3584473.

[43] M. Abbasi, F. Cardoso, P. Váz, J. Silva, P. Martins, "A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments," *Cryptography*, vol. 9, no. 2, Art. no. 32, 2025, doi: 10.3390/cryptography9020032.

[44] D. Kim, J. Choi, S. Yoon, S.C. Seo, "Optimized implementation of HQC on Cortex-M4," *ICT Express*, vol. 11, no. 5, pp. 939–944, 2025, doi: 10.1016/j.icte.2025.07.001.

[45] Open Quantum Safe (OQS). (2026). *Continuous benchmarking*, OQS Algorithm Performance Visualizations. [Online]. Available: https://openquantumsafe.org/benchmarking/. [Accessed: Jan. 20, 2026].

[46] A.G. Schemitt, H.F. da Silva, R.C. Lunardi, D. Kreutz, R.B. Mansilha, et al., "Assessing the impact of post-quantum digital signature algorithms on blockchains," in 2025 *IEEE 24th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 2373–2380, 2025, doi: 10.48550/ARXIV.2510.09271.

[47] P. Juaristi, I. Agudo, R. Rios, L. Ricci, "Benchmarking post-quantum cryptography in ethereum-based blockchains," in *Computer Security. ESORICS 2024 International Workshops*, J. Garcia-Alfaro et al., Eds., vol. 15263. Cham: Springer Nature, 2025, pp. 340–353, doi: 10.1007/978-3-031-82349-7_23.

[48] M.E. Bizri, A.M. El-Hajj, L. Sliman, A.M. Haidar, "Institutional approaches to post-quantum cryptography: A comparative analysis of migration frameworks," *IEEE Access*, vol. 14, pp. 3259–3283, 2026, doi: 10.1109/ACCESS.2025.3650465.

[49] M. Andrysco, A. Nötzli, F. Brown, R. Jhala, D. Stefan, "Towards verified, constant-time floating point operations," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Toronto. New York, NY: ACM, 2018, pp. 1369–1382, doi: 10.1145/3243734.3243766.

[50] B. Westerbaan. (Mar. 05, 2024). *The state of the post-quantum internet*. [Online]. Available: https://blog.cloudflare.com/pq-2024/ [Accessed Feb. 5, 2026].

[51] A. Zafar, S.S. Iqbal, "Integrating code-based post-quantum cryptography into SSL TLS protocols through an interoperable hybrid framework," *Discover Computing*, vol. 28, no. 202, 2025, doi: 10.1007/s10791-025-09735-7.

[52] M.D. Hakim Azammullah, S.F. Syed Adnan, R. Mohamad, N.N. Mohamed, "Runtime and energy analysis of KYBER, a post quantum cryptography (PQC) on an IoT platform," in *2025 IEEE Symposium on Wireless Technology & Applications (ISWTA)*, Penang, New York, NY: IEEE, 2025, pp. 1–7, doi: 10.1109/ISWTA68114.2025.11329628.

[53] T.B. Maqsood, K. Hameed, M. Junaid, N. Tahir, "Enhancing IoT healthcare security with post-quantum cryptography: A performance and case study analysis," in *2025 6th International Conference on Advancements in Computational Sciences (ICACS)*, Lahore, Pakistan, 2025. New York, NY: IEEE, 2025, pp. 1–8, doi: 10.1109/ICACS64902.2025.10937815.

[54] T.N. Turnip, B. Andersen, C. Vargas-Rosales, "Toward 6G authentication and key agreement protocol: A survey on hybrid post quantum cryptography," *IEEE Communications Surveys & Tutorials*, vol. 28, pp. 3311–3345, 2026, doi: 10.1109/COMST.2025.3567439.

[55] AWS (2026). *Using Hybrid Post-Quantum TLS with AWS KMS AWS Key Management Service*. [Online]. Available: https://docs.aws.amazon.com/kms/latest/developerguide/pqtls.html. [Accessed Feb. 1, 2026].

[56] B. Westerbaan. (Oct. 28, 2025). "State of the post-quantum internet in 2025." [Online]. Available: https://blog.cloudflare.com/pq-2025/. [Accessed Feb. 8, 2026].

[57] S. Shen, H. Yang, W. Li, Y. Zhao, "cuML-DSA: Optimized signing procedure and server-oriented GPU design for ML-DSA," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 3, pp. 2295–2307, 2025, doi: 10.1109/TDSC.2024.3494835.

[58] D. Commey, G.V. Crosby, "PQS-BFL: A post-quantum secure blockchain-based federated learning framework," arXiv:2505.01866, 2025, doi: 10.48550/ARXIV.2505.01866.

[59] G. D'Onghia, A. Lioy, "Towards quantum-resistant trusted computing: Architectures for post-quantum integrity verification techniques," arXiv:2601.11095, 2026, doi: 10.48550/ARXIV.2601.11095.