JOURNAL OF POST-QUANTUM CRYPTOGRAPHY AND SYSTEMS

RESEARCH ARTICLE

Volume 01, Issue 01, 2026

From Theory to Deployment: A Review of Quantum-Resistant Cryptographic Systems and Their Real-World Applications

Mohammed A. Abdewi

Mathematics and Computer Science Department, Faculty of Science, Al-Azhar University, Nasr City, Cairo, Egypt

Email: mohammed.alsatori82@gmail.com

ABSTRACT

The high rate of development of quantum computing is a major threat to classical cryptographic systems such as RSA, Diffie Hellman and elliptic curve cryptography, which are based on mathematical problems amenable to quantum algorithms. In reaction, post-quantum cryptography (PQC) has become a research priority area aimed at the creation of quantum-resistant cryptography. In this paper, the review of the quantum-resistant cryptographic systems has been made, bridging the gap between the theoretical background and the implementation. The paper introduces a systematic taxonomy of key PQC strategies, such as lattice-based, code-based, hash-based, and multivariate cryptographic schemes, their basic principles, strengths, and weaknesses. It also analyses the security measures like quantum and classical resistance, cryptanalysis as well as the vulnerabilities in implementation. The paper also examines the system design issues, performance assessment measure, and the actual deployment in areas like secure communication, cloud computing, IoT, and blockchain. The review also covers current activities in standardization, especially the NIST PQC program, and a migration approach such as hybrid cryptographic models and crypto-agility. Finally, the key problems related to efficiency, scalability and long-term security are described, as well as future research directions. The article will provide an in-depth overview of the PQC systems and help build robust and quantum-resistant digital infrastructures that are both secure and scalable.

Keywords: Post-Quantum Cryptography (PQC), Quantum-Resistant Algorithms, Cryptographic Security, Quantum Computing Threats, Secure System Design

1. Introduction

Contemporary digital security relies on cryptographic system, offering a secure communication framework, information protection, authentication, and privacy within numerous applications, such as e-commerce, cloud computing and systems of critical infrastructure (Singh et al., 2025). Conventional public-key cryptography systems, like the RSA, Diffie Hellman, and Elliptic Curve Cryptography (ECC) schemes have been based on the computational infeasibility of mathematical challenges such as integer factorization and discrete logarithm. Despite the decades of guaranteeing a high level of security, the efficiency of these techniques with time is becoming increasingly doubtful with the emergence of the paradigm of computerization, primarily, with the introduction of quantum computing (Barzen & Leymann, 2024).

Quantum computing represents a radically novel model of computation that exploits quantum mechanical properties like superposition and entanglement to efficiently compute some problems in comparison to classical systems. Remarkably, the algorithm of Shor illustrates the fact that problems of integer factorization and discrete logarithm, which form the basis of popular cryptographic protocols, can be resolved in a time that is proportional to the power of a quantum computer that is powerful enough. Likewise, the algorithm presented by Grover provides a quadratic speedup to brute-force search and thus undermines the effective security of symmetric cryptographic primitives (Bavdekar et al., 2022). Large-scale, fault-tolerant quantum computers are not yet fully realized but continuing advancements in technology indicate that they will become a viable threat soon, a major threat to the existing cryptographic infrastructures (Alvarado et al., 2023).

To address these issues, the discipline of post-quantum cryptography (PQC) has become an urgent field of study aimed at creating cryptographic algorithms that do not fall prey to classical and quantum attackers (Chhetri et al., 2025). PQC algorithms are often founded on problems that are assumed to be resistant to quantum attacks, such as lattice-based, code-based, hash-based and multivariate polycentricities. In contrast to quantum cryptography, based on quantum communication channels, PQC tries to offer quantum-resistant designs that can be executed on existing classical hardware and embedded within existing digital systems (Sharma et al., 2023).

Although there have been great strides in the theory of PQC algorithm design, there are still several challenges in the move of the schemes out of theory and on to practical implementation. Computational efficiency, key size overhead, implementation complexity, compatibility with legacy systems, and real-world security vulnerabilities are critical that should be considered (Canto et al., 2023). In addition, the necessity of multipurpose assessment systems and common migration policies has gained even greater significance, as governments and industry players start planning a quantum-on-demand future (Joseph et al., 2022).

This is a review paper, which will present a deep and systematic discussion of quantum-resistant cryptographic systems, the gap between theory and practical implementation. In particular, the paper discusses the design and security assumption of key PQC algorithms, their performance and implementation features, and how they can be used to create an environment in modern computing. It also summarizes existing standardization initiatives and addresses some of the real-world issues related to the implementation and transition to post-quantum security systems (Xie et al., 2024).

The rest of this paper is organized in the following manner. Section 2 introduces the basic notions and security models applicable in post-quantum cryptography. Section 3 gives an elaborate taxonomy of quantum resistant cryptographic

algorithms. Section 4 talks about security analysis and resiliency to different attack models. Section 5 will consider the considerations in the system design and integration plans to apply PQC to the real-life situations. Part 6 will focus on performance measurement and benchmarking of PQC implementations. Section 7 contains real world applications and cases. Section 8 deals with real-life issues and threat modeling. Section 9 examines existing standards, policies and migration strategies. Section 10 summarizes the open research problems and future directions and concludes with remarks in Section 11 (Chang & Khan, 2026).

2. Fundamentals of Post-Quantum Cryptography

Post-quantum cryptography (PQC) is a groundbreaking change in cryptographic system designs and analysis, motivated by the expected capabilities of quantum computing (Bernstein, 2025). In contrast to classical cryptographic methods, which are based on computational hardness assumptions, which can be defeated by quantum algorithms, PQC puts emphasis on the design of secure primitives (which are based on problems which are thought to be immune to both classical and quantum adversaries). This section has given a synopsis of the base concepts, such as security models and the quantum threat environment, which has changed over time.

2.1 Overview of Cryptographic Security Models

Historically, cryptographic security has been defined with regards to the ability of an adversary to compromise system. In classical contexts, opponents are supposed to run deterministic or probabilistic polynomial-time algorithms on classical computing systems. The computational infeasibility of solving a set of mathematical problems, e.g., integer factorization and discrete logarithms, under reasonable time constraints is thus the basis of security guarantees (Chen et al., 2016).

Adversarial models, however, need to be redefined with the advent of quantum computing. The quantum adversarial model assumes that the attackers have access to quantum computing resources, which allows them to take advantage of algorithms that are able to solve certain problems more effectively than the classical algorithms. This can lead to the weakness of cryptographic schemes that are secure in classical assumptions in a quantum environment (Mosca, 2018).

Here, post-quantum cryptographic designs are aimed at providing quantum-resistant security, that is, the hardness in their design cannot be broken by quantum adversaries. Other problems, like Learning With Errors (LWE), Shortest Vector Problem (SVP), decoding random linear codes, and locating pre-images or collisions in cryptographic hash functions are commonly assumed to be difficult in PQC. These issues are now in known efficient quantum algorithms that can solve them in a polynomial time (Bindel et al., 2019). Other classical ideas like indistinguishability under chosen-plaintext attack (IND-CPA) and indistinguishability under chosen-ciphertext attack (IND-CCA) are also applied to quantum models in PQC. Scenarios in which adversaries are allowed to make quantum queries to cryptographic oracles are considered by researchers to give stronger concepts like quantum IND-CPA (QIND-CPA) security. The sophisticated models are such that cryptographic schemes are secure even when playing with quantum-capable adversaries.

2.2 Quantum Threat Landscape

The main reason behind the post-quantum cryptography is the possibility of quantum algorithms affecting popular cryptographic systems. Of these, the algorithm by Shor is the most dangerous, as it allows to factor large integers efficiently and compute discrete logarithms in a time that is a polynomial in the input size. This means that even popular cryptosystems based on public-key encryption like RSA, Diffie Hellman key exchange and elliptic curve cryptography (ECC) are fundamentally insecure against sufficiently powerful quantum computers (Aggarwal et al., 2017).

Besides public-key cryptography, there are also symmetric cryptographic primitives that are impacted, albeit to a lesser degree. The algorithm of Grover offers a quadratic speedup of the brute-force search of keys, which in effect halves the security of symmetric algorithms. As an illustration, a 128-bit symmetric key would provide just about 64 bits of protection against a quantum adversary. This does not make symmetric cryptography irrelevant, but it requires bigger key sizes and stronger hash functions to ensure sufficient security margins (Ralegankar et al., 2021).

The urgency of dealing with these threats is further increased by the idea of the so-called harvest now, decrypt later attacks when adversaries gather encrypted information now, and with the introduction of quantum capabilities, the adversaries will decrypt the information in the future. This is especially alarming in the case of sensitive information that needs to be kept confidential over a long period like governmental, financial and healthcare information.

Though not yet, large-scale quantum computers that can solve existing cryptography systems are underway, it has been estimated that in the coming decades, the development of quantum computing hardware and error correcting algorithms will allow the creation of them. As a reaction, the international community, led by the NIST Post-Quantum Cryptography Standardization Process, is actively pursuing the development of secure and efficient quantum-resistant algorithms, along with their standardization.

As the process of replacing global cryptographic infrastructures is complex, the process of post-quantum migration is likely to be a long and resource-intensive process. Thus, active research, assessment, and implementation plans will be necessary to have a seamless and safe conversion to quantum-safe cryptography systems.

3. Taxonomy of Quantum-Resistant Cryptographic Algorithms

Post-quantum cryptography refers to a wide array of cryptographic constructions, which rely on mathematical problems, where resilience to both classical and quantum attacks has been presumed. These methods vary in terms of hardness assumptions, computational efficiency, key sizes and applicability. In this section, major PQC families are systematically classified, and their principles, benefits, and drawbacks are pointed out (Cherkaoui Dekkaki et al., 2024).

Table 1. Classification of major post-quantum cryptographic algorithm families

Category	Hard Problem	Advantages	Limitations
Lattice-based	LWE, SVP	Strong security, versatile	Large keys
Code-based	Syndrome decoding	Proven security	Very large keys

Hash-based	Hash functions	Simple, secure	Large signatures
Multivariate	Polynomial equations	Fast signatures	Security concerns
Isogeny-based	Elliptic curve isogenies	Small keys	Recently broken

3.1 Lattice-Based Cryptography

One of the most conspicuous approaches to PQC, which employs problems such as Learning With Errors (LWE) and Ring-LWE, is lattice-based cryptography. These include solving noisy linear equations and they are said to be resistant to both classical and quantum attacks (Zong, 2025). Their strong theoretical foundation including worst-case to average-case reductions which are powerful yield of security is their greatest strength. Also, lattice-based schemes can support more general features, such as homomorphic encryption (Chen, 2024). Such ones are Kyber (key encapsulation) and Dilithium (digital signatures), both chosen in the NIST PQC standardization process. These plans can however be described as having huge key sizes and this may affect the effectiveness of the storage and communication.

3.2 Code-Based Cryptography

Cryptography based on codes, such as the McEliece cryptosystem, is based on the hardness of decoding random linear error-correcting codes (Meyer, 2025). Its primary advantage is that it has a long history of security and no realistic attacks have been capable of compromising well-parameterized applications. The schemes also offer quick encryption and decryption processes. Although these have these benefits, one of their key constraints is that they have very large public key sizes, which can be difficult to implement in resource-constrained systems like IoT and embedded systems.

3.3 Hash-Based Cryptography

Hash cryptography is a cryptography that builds digital signatures by cryptographic hash functions. It is secure based on properties like collision resistance and pre-image resistance which are still relatively resistant to quantum attacks, excepting the algorithm of Grover. Stateless and stateful signatures can be facilitated by merkle tree-based schemes like XMSS and SPHINCS+. They are easy, intuitive, and need a minimum of complex mathematics (Alagic et al., 2022). Nevertheless, they can generate huge signature sizes and can also limit the number of secure signatures in stateful variants.

3.4 Multivariate Cryptography

Multivariate cryptography is a cryptography system based on the solution of multivariate equations in finite fields, NP-hard problems (Sahu & Mazumdar, 2024). The schemes are fast in generating signatures and have comparatively small signature sizes. Nevertheless, their security has not been so steady in the past and several schemes have been cracked because of development in algebraic cryptanalysis. The major challenges are the resistance to structural, algebraic, and rank-based attacks and secure design remains a research problem.

3.5 Other Emerging Approaches

New PQC designs are isogeny-based cryptography, based on the intractability of computing an isogeny between elliptic curves. These schemes provide smaller key sizes but have been exposed to recent major cryptanalytic challenges. The interest in hybrid cryptographic schemes is also increasing, which are based on the combination of classical and post-quantum algorithms to provide security in the transition period. These strategies offer backward compatibility and progressive integration of PQC mechanisms (Bagirovs et al., 2024).

4. Security Analysis and Cryptographic Resilience

The hardness of mathematical problems, and resistance to classical or quantum adversaries, lies at the core of the security of post-quantum cryptographic (PQC) systems. Since these systems will be used to substitute or supplement the existing cryptographic systems, security analysis and resilience testing is vital. In this section, the essential features of security proofs, quantum attack resistance, cryptanalysis, and implementation vulnerabilities of PQCs are discussed (Sahu and Mazumdar, 2024). Table 2 presents a comparative analysis of security properties of families of PQCs.

Table 3. Security characteristics of different PQC algorithm families

PQC Family	Quantum Resistance	Classical Resistance	Maturity Level
Lattice-based	High	High	High
Code-based	High	Very High	Very High
Hash-based	High	Very High	High
Multivariate	Medium	Medium	Moderate
Isogeny-based	Uncertain	Medium	Low

4.1 Security Proofs and Assumptions

Post-quantum cryptography schemes are based on a set of well-understood computational hardness assumptions that are thought to be resistant to quantum computing as well. The assumptions are used in formal security proofs, which strive to show that it is at least as difficult to break a cryptographic scheme as the underlying mathematical problem. As an example, lattice-based schemes rely on the hardness of Learning With Errors (LWE) and Shortest Vector Problem (SVP) problems, and the use of code-based cryptography is based on the hardness of decoding random linear codes (Albrecht et al., 2015).

Decryption of security proofs in PQC Security proofs are often reductionist in nature, with the security of a cryptographic construction being decreased to the perceived hardness of the underlying problem. Most of these proofs are stated in the context of common security concepts like indistinguishability under chosen-plaintext attack (IND-CPA) and indistinguishability under chosen-ciphertext attack (IND-CCA) and are constantly generalized to quantum-

conscious models. But compared to classical cryptographic assumptions, most PQC assumptions have not been examined over such long intervals, which creates an element of uncertainty as to whether they will remain robust over such long intervals.

4.2 Resistance to Quantum Attacks

One of the primary conditions of post-quantum cryptographic schemes is that they are resistant to known quantum algorithms. The algorithm by Shor is a devastating attack on the classical public-key cryptosystems since it allows solutions to integer factorization problems and discrete logarithm problems to be solved effectively and thus makes generally used systems like RSA and ECC insecure in a quantum environment. PQC algorithms, in turn, are explicitly tailored to not exploit these susceptible mathematical structures, but to use problems that no known efficient quantum algorithms exist (Jaques et al., 2020).

Constructions based on lattices, such as many others, are widely believed to be quantum resistant since quantum solutions to LWE and similar problems do not exist in polynomial time. Likewise, code-based and hash-based schemes have been found to be highly resistant to a quantum adversary with only a few weaknesses to quantum search algorithms including Grover algorithm.

4.3 Classical vs Quantum Cryptanalysis

The analysis of cryptography plays a crucial role in evaluating the security and stability of cryptographic systems. Classical and quantum cryptanalytic techniques need to be considered in the environment of post-quantum cryptography to have a holistic assessment of security. Classical cryptanalysis is the set of approaches which include algebraic attacks, lattice reduction techniques, code-based system decoding attacks and statistical techniques, such as differential and linear cryptanalysis of symmetric primitives.

Quantum cryptanalysis builds upon these techniques to add in quantum computational abilities. Although the existing quantum algorithms do not offer substantial benefits to the majority of PQC schemes, they still can benefit some of the attack vectors. Consequently, PQC schemes must be analysed in terms of hybrid threat models which consider the combined capacity of classical and quantum adversaries (Kundu et al., 2024).

4.4 Side-Channel and Fault Attacks

Besides theoretical security considerations, practical implementations of the post-quantum cryptographic systems are vulnerable to side-channel and fault attacks. Side-channel attacks are based on physical properties of computation, like execution time, power consumption or electromagnetic emissions, to leak sensitive information. The vulnerabilities apply especially in the hardware implementations and embedded systems (Azouaoui et al., 2022).

Fault attacks, in contrast, are a set of attacks that intentionally cause errors when performing cryptographic operations

in order to disclose secret information. PQC schemes particularly with complex arithmetic functions like lattice-based computation of polynomials can also present further implementation issues that predispose them to such attacks unless designed carefully.

In order to reduce these risks, it is necessary to use the strong implementation schemes, which are constant-time algorithms, masking, and the hardware-level protection. Such attacks lead to a need to ensure resilience to guarantee secure deployment.

4.5 Comparative Security Evaluation Across PQC Families

The maturity of security, resilience and practical robustness of different families of post-quantum cryptographic algorithms vary. The lattice-based cryptography has a solid theoretical basis and flexibility but needs a proper choice of parameters to withstand sophisticated attacks. Cryptography based on codes offers a high degree of confidence because it has long resisted cryptanalysis, and e.g. its large key sizes are a practical deployment issue.

Cryptography based on hash is advantageous to have a solid understanding of security assumptions whereas multivariate cryptography can perform efficiently but has long been plagued by stability problems. Newer hybrid cryptography solutions are also under consideration to deliver increased system resilience and offer layered security guarantees (Liu et al., 2025).

The current understanding of security analysis in post-quantum cryptography necessitates a multi-dimensional and holistic approach to combine the theoretical security proofs, classical and quantum attack resistance, and sound implementation practice. Even though major strides have been achieved in creating quantum-resistant cryptographic systems, continuous research, testing, and optimizations are necessary to face new threats and guarantee security in the long term.

5. From Theory to Practice: System Design and Integration

There are many technical and operational challenges to the move between theoretical post-quantum cryptographic (PQC) constructs and real-world implementation. Although quantum-resistant algorithms have been developed significantly, their successful implementation is determined by the effective system-level design, efficient implementation, and the ability to integrate smoothly with the existing infrastructures (Kong et al., 2022). In this section, the architectural issues, implementation issues and interoperability issues of deploying PQC into current computing environments are analysed.

5.1 Architectural Considerations

The application of post-quantum cryptographic algorithms to current communication and security systems is an essential step towards having quantum-resilient systems. Contemporary systems, including Transport Layer Security

(TLS), Virtual Private Networks (VPNs) and blockchain systems, depend on classical cryptographic primitives to exchange keys, authenticate and provide integrity of data. To replace or add these primitives with PQC algorithms, it is important to design the architecture to guarantee security without the need to severely impact system performance. To illustrate, the introduction of lattice-based key encapsulation schemes into TLS handshake protocols requires changes in the message formats, key exchange protocols and certificate processing mechanisms (Paquin et al., 2020).

The use of hybrid cryptographic models, which use classical and post-quantum algorithms in the same protocol, is one of the most popular methods used to enable this transition. Security in such models is ensured provided at least one of the underlying schemes is secure thus offering a protection in the transition period. Backward compatibility and gradual adoption can also be achieved by hybrid architectures, eliminating the dangers of migration shock. These methods, however, add complexity to the system design such as higher computational load, bigger payloads in communications, and more complex protocol logic. Figure 1 illustrates the integration process of the classical and post-quantum cryptographic elements.

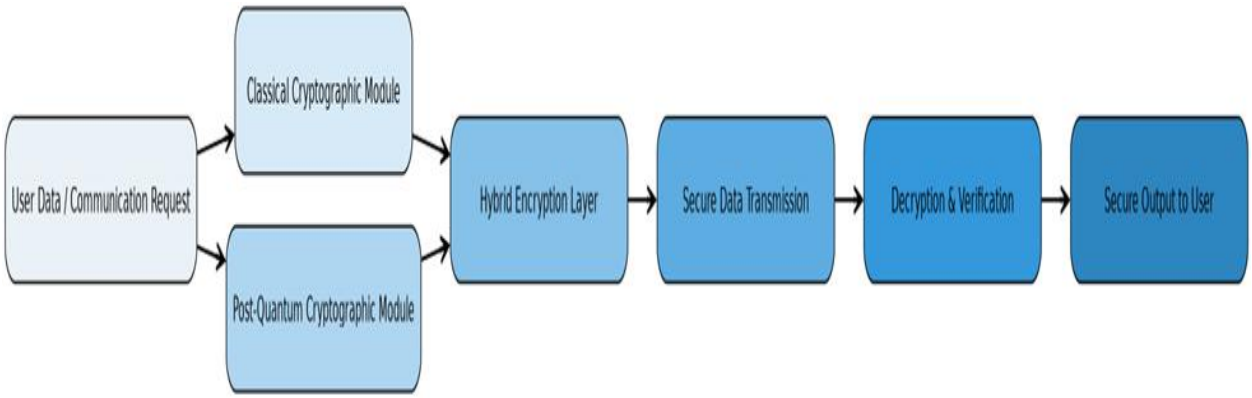

Figure 1. Workflow illustrating the integration of classical and post-quantum cryptographic modules in secure communication systems

Consequently, architectural decisions must carefully balance security, efficiency, and scalability requirements.

5.2 Hardware and Software Implementations

PQC schemes should be practically deployed, which requires the efficient implementation on the software and hardware platforms. Optimization of PQC algorithms level, in the software environment, involves the avoidance of challenges involving large key sizes, arithmetic and increased usages of memory. To reach acceptable performance levels, especially in high-throughput systems like cloud services and data centres, efficient implementation methods, such as optimized polynomial arithmetic, parallel processing, and algorithm-specific optimizations, are needed (Lei et al., 2023).

The limitations are even stiffer in hardware-constrained systems, like embedded systems and Internet of Things (IoT) systems. Lightweight implementations of PQC algorithms are needed due to the limited computational power,

memory limits and energy efficiency criteria. This has given rise to the introduction of dedicated hardware accelerators and cryptographic co-processors that are efficient in performing tasks like modular arithmetic and multiplication of polynomials (Lee et al., 2022). Secure processor and trusted hardware platform are also crucial in maintaining integrity and confidentiality of cryptographic operations, especially in the implementation of sensitive data applications.

Moreover, hardware implementations should be properly structured to withstand side-channel and fault attacks, which are simpler to attack in physical equipment. Constant-time execution, masking, and hardware-level isolation are critical techniques to provide safe and reliable PQC deployment (Ravi et al., 2024). In general, the realization of efficient and secure implementations within a wide range of platforms is one of the challenges in bringing PQC into practice.

5.3 Interoperability Challenges

One significant issue regarding the implementation of post-quantum cryptographic systems is interoperability, especially with the high prevalence of old cryptographic systems. There is a strong interconnection between existing systems, protocols and applications and classical cryptographic algorithms, which may mean that introducing PQC solutions would require considerable changes. To be able to make a smooth transition and prevent any interruptions to current services, it is thus necessary to ensure compatibility with the legacy systems.

The main problem is handling the differences in the key sizes, computation needs, and protocol formats between classical and post-quantum schemes. To provide an example, the bigger key and signature sizes of most PQC algorithms may result in higher bandwidth usage and storage needs, which may affect the performance of the system. In addition, cryptographic libraries, certificate authorities and security protocols must be revised to facilitate the transition to PQC and this task can only be achieved with the collective efforts of multiple parties, such as software vendors, standardization organizations, and industry organizations.

The proposed transition strategies to resemble such challenges include the gradual migration, hybrid deployments, and crypto-agility frameworks. Crypto-agility describes the capability of systems to switch between various cryptographic algorithms in a short time and without fundamentally rearchitecting the system so that it can maintain with the changing security needs of organizations. Phage migration plans are plans where PQC algorithms are implemented in stages with the classical schemes being permissible to be tested, passed and performance analysed before full implementation. The risks of compatibility can be mitigated with the help of such strategies and offer a more controlled and safe process of transition to quantum-resistant infrastructures (Kumar et al., 2022).

The major support towards the successful introduction of post-quantum cryptography to the real world will be the holistic approach, which will address the concerns of architectural design, efficient implementation and compatibility. Even though hybrid models and crypto-agile frameworks provide feasible channels to deployment, there is still quite some way to go to optimize performance, ensure compatibility and security in a very diverse range of computing

environments. This will necessitate the co-operation of researchers, engineers and the industry stakeholders going forward since the conversion to quantum-safe systems is an on-going process, which is necessary to close the gap between theory and practice (Ullah et al., 2025).

6. Performance Evaluation and Benchmarking

The performance of post-quantum cryptography (PQC) algorithms in practice is significantly dependent on their operational properties in practice. Most PQC schemes provide high-security assurances against quantum adversaries, but they tend to add some extra computational and communication cost to classical cryptographic systems. Thus, systematic performance measurement and benchmarking are needed to determine their practicability, scalability, and applicability in various application areas (Ojetunde et al., 2025).

6.1 Key Performance Metrics

PQC algorithms are commonly evaluated by a variety of important performance metrics, such as, but not limited to, computational overhead, key size and bandwidth requirements, and latency and throughput. Table 3 compares the key performance characteristics of PQC algorithms.

Table 3. Performance comparison of major PQC algorithms based on key metrics

Algorithm Type	Key Size	Computation Cost	Latency	Suitability
Lattice-based	Medium	Medium	Moderate	General use
Code-based	Very Large	Low	Low	High security
Hash-based	Small–Medium	High	High	Signatures
Multivariate	Small	Low	Low	Signatures
Hybrid	Large	High	Moderate	Transition phase

The processing cost of cryptographic operations (including key generation, encryption, decryption and signature production and verification) is called the computational overhead. Most PQC protocols, especially lattice-based protocols and multivariate protocols, use complex mathematical operations, which may take a lot longer to compute than conventional algorithms.

The size of keys and bandwidth requirements are also significant factors to take into account because several PQC algorithms have significantly larger public keys, private keys and ciphertexts. An example is that code-based cryptographic schemes have very large public keys whereas hash-based signatures tend to generate large signature sizes. They directly affect the performance of communication, storage, and network performance, particularly in bandwidth-limited settings like IoT systems and mobile networks. Latency and throughput are also factors that dictate real time applicability of PQC algorithms. Figure 2 shows a comparison of the performance of PQC algorithms.

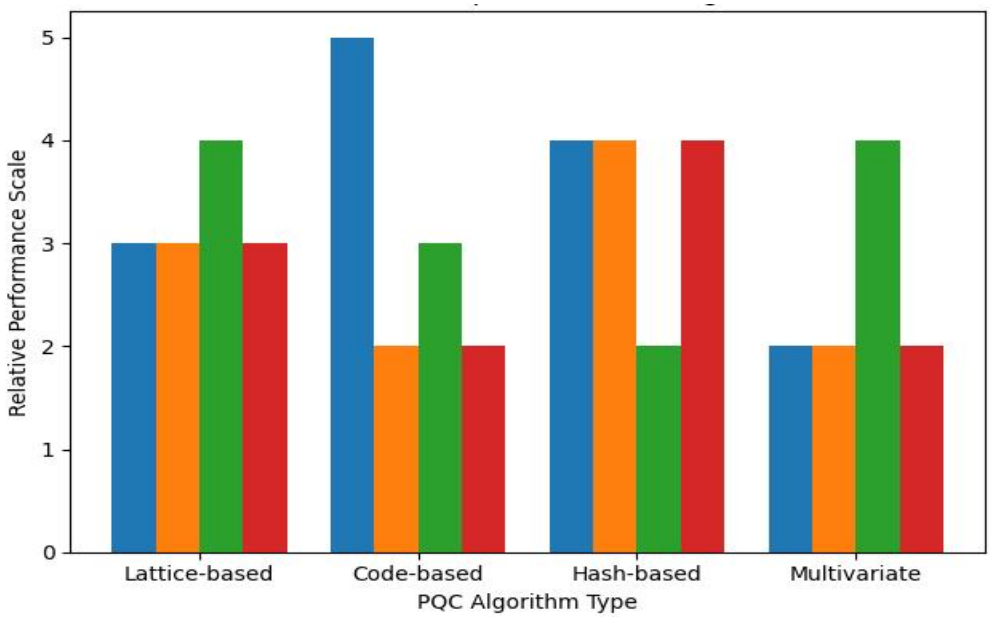

Figure 2. Comparative performance analysis of major PQC algorithms based on key evaluation metrics.

Latency is used to identify the lag caused by cryptographic operations, which is especially important in time-sensitive applications, like secure communications and financial transactions. On the other hand, throughput denotes a quantity of cryptographic operations that are capable of any point in time. They should determine the optimal default of these measures that will work towards achieving the ability of the PQC systems to achieve the performance demands of the modern digital infrastructures (Montenegro et al., 2025).

6.2 Benchmark Comparisons of Major PQC Algorithms

In case of normal circumstances, benchmarking studies would be handy in terms of comparative performance of various PQC algorithms. Kyber and lattice-based constructions have already shown good performance regarding computational complexity and scaling and, therefore, a viable candidate to be implemented in practice due to its efficient design and providing efficient polynomial arithmetic (Bos et al., 2018).

On the same note, using other types of digital signature like Dilithium, have been demonstrated to work well due to their signing and verification speed and are able to be applied to a large variety of applications which need secure authentication (Ducas et al., 2018). The algorithms may be applied in software, hardware and are better implemented.

However, as contrasted to the unconstrained platform, the efforts to benchmark constrained platforms have shown that performance may range dramatically with hardware architecture and optimization methods. Indicatively, embedded systems assessment indicates that proper implementation strategies are crucial in attaining satisfactory levels of performance (Kannwischer et al., 2019). The comparative benchmarking shows that no individual PQC algorithm is superior to all the rest in all performance dimensions, and context-based selection based on application requirements is necessary.

6.3 Trade-offs Between Security and Efficiency

A key trade-off in post-quantum cryptography is the trade-off between the level of security and computational and resource efficiency. The increased level of security usually demands more parameters and consequently more complexity of computation, consumption of memory and overheads in communication. To take one example, adding key sizes to obtain greater resistance to quantum attacks can result in a higher bandwidth usage and reduced processing speed.

On the other hand, when optimizing to maximize efficiency, that is, minimizing the size of parameters, security guarantees can be undermined and more vulnerable to advanced cryptanalytic methods. Particularly in resource-constrained systems such as embedded systems and IoT devices, where computing resources, memory, and power consumption are limited, this is an especially crucial trade-off. As a result, designers should be extremely careful when selecting parameter sets that can provide an adequate level of security without affecting the acceptable performance (Alkim et al., 2016).

The hybrid cryptographic solutions provide a feasible way to address this issue by integrating classical and post-quantum algorithms, thus, spreading the security and performance demands among a set of schemes. The way to make the best use of PQC algorithms through improved mathematical techniques and efficient implementation strategies is also under investigation.

6.4 Case Studies of Experimental Implementations

Practical applications of PQC algorithms can shed light on their practical performance and implementation. In a number of papers, the application of lattice-based key encapsulation schemes in protocols such as TLS have been tested and found to increase the size of the handshake and the computation time but acceptable in performance in a number of applications.

In a similar manner, the application of PQC schemes to cloud computing systems has also demonstrated that the overhead of the computation process and use of hardware acceleration can be drastically reduced and make it possible to implement the large-scale applications successfully. These pragmatic studies attract attention towards the viability of adoption of PQC due to the role of performance conscious design.

The operational frameworks of experimental systems are also helpful in understanding the practical implications of implementing PQC, providing structured approaches to assessing the effectiveness of algorithms, their scalability, and obstacles to implementing them into the real-life systems (Montenegro et al., 2025).

Benchmarking and performance analysis are fundamental aspects in the process of transforming theoretical post-quantum cryptography to practice. Although PQC algorithms are still provided with mind-blowing overheads in terms of computation, key size and communication overheads, recent research and optimization endeavours are being done to render them efficient and scalable. Security vs. performance, an empirical benchmarking and a real test will be required to provide a fine balance that can enable the addition of PQC to the current digital system to be a success.

7. Real-World Applications and Deployment Case Studies

Moving post-quantum cryptography (PQC) concepts into reality is an important milestone towards quantum-resilient digital infrastructures. Table 4 summarizes the key areas of use of PQC.

Table 4. Application areas of post-quantum cryptography in real-world systems

Domain	Application	PQC Role
Secure Communication	TLS/SSL	Key exchange, encryption
Cloud Computing	Data storage	Data protection
IoT	Embedded devices	Lightweight security
Blockchain	Digital signatures	Transaction security
Government/Defense	Confidential data	Long-term protection

With the emergence of quantum threats as an increasingly realistic possibility, businesses in various sectors are actively researching the implementation of PQC in the real world. This part reviews important areas of applications, industry implementation initiatives, and new deployment examples that reveal the viability and difficulty of applying quantum-resistant cryptography solutions in practice (Imran et al., 2024).

7.1 PQC in Secure Communication Systems (TLS/SSL)

Internet security is based on secure communication protocols like Transport Layer Security (TLS) and Secure Socket Layer (SSL) which allow clients and servers to communicate with each other encrypted. Recent research and experimentation have largely been on the integration of PQC into these protocols. The modified TLS handshake has been designed to use lattice-based key encapsulation to either replace or supplement classical key exchange mechanisms such as RSA and Diffie Hellman (Banerjee and Chandrakasan, 2020).

PQC integration has been shown to grow handshake sizes and computational overhead but its effect on the overall system performance is generally manageable in most applications. Hybrid TLS models are implemented in a testing environment in lots of cases to provide backward compatibility and transitional security by combining classical and post-quantum algorithms. These advances show that PQC is capable of seamlessly being incorporated into the current communication infrastructures with considerate optimization and protocol modifications.

7.2 PQC in Cloud Security

Cryptographic mechanisms are critical in cloud computing environments to guarantee confidentiality, integrity and safe access control of data. PQC must be employed in cloud security to secure sensitive data against the long-term quantum threats especially in any case where there is a need to store and transmit data over a long time. CSPs are also experimenting with the concept of applying PQC algorithms to encryption services and key management systems and secure communication channels (Li et al., 2023). Practically speaking, deploying PQC in the cloud can take advantage

of the scalability of computational resources, which can be used to alleviate the performance penalty of complex cryptographic operations. To enhance the efficiency of the PQC implementations in large-scale cloud systems, parallel processing and hardware acceleration methods have been used.

7.3 PQC in Internet of Things (IoT)

The Internet of Things (IoT) offers some special challenges to the implementation of post-quantum cryptography since many devices have resource-constrained nature. PQC algorithms that require a lot of computation are hard to run due to limited processing power, memory, and energy availability. Despite these constraints, the need for quantum-resistant security in IoT systems is critical, particularly in applications involving healthcare, smart cities, and industrial control systems (Mahdi & Abdullah, 2025).

To overcome these issues, scholars have come up with lightweight PQC schemes implementations that are optimized to operate in restricted settings. Cryptographic algorithms based on a lattice and hash algorithms have been optimized to be computationally simple and have memory requirements reduced by using low-power devices. Nevertheless, the trade-offs between security, performance, and resource consumption are an important factor.

7.4 PQC in Blockchain and Distributed Systems

Distributed ledger technologies and blockchain are based on cryptographic primitives such as transaction validation and digital signatures, as well as consensus mechanisms. The fact that classical cryptographic functions might be susceptible to quantum attacks is a major threat to the future security of blockchain systems. Consequently, there is an increasing desire to implement PQC algorithms in blockchain solutions to guarantee quantum-secure security (Fernandez-Carames & Fraga-Lomas, 2020).

Post-quantum digital signature schemes are under consideration as an alternative to classical signature algorithms like ECDSA. Nevertheless, the issue of larger signature sizes and verification cost may affect the efficiency of transactions and storage.

7.5 Industry Adoption and Standardization Efforts

The use of post-quantum cryptography in industry is directly related to current standardization initiatives, most notably the NIST Post-Quantum Cryptography Standardization Process. This initiative has played a vital role in evaluating, selecting and standardization of quantum resistant cryptographic algorithms to be adopted across the board.

In addition to NIST, other international bodies, industry consortia and technology firms are also scurrying to come up and adopt PQC standards. The big technology sellers have already initiated pilot projects to incorporate PQC into their product and services, including secure communications systems, cloud environments, and hardware security chips.

7.6 Pilot Deployments and Real-World Experiments

Pilot deployments and experimentation yield fascinating information on the practical issues and performance consequences of implementing PQC in real systems. Some organizations have conducted enormous experiments to experiment with the implementation of PQC algorithms into the current infrastructures.

Consistent with this, the use of PQC to protect email systems, VPNs, and cloud-based services has been explored, and the benefits and limitations of current solutions have been presented. These experiments demonstrate that even though PQC algorithms come with extra overhead, with proper optimization and system design, it is possible to reduce the performance effects.

As seen in application and deployment case studies, post-quantum cryptography is no longer an area of theoretical research but rather is being applied in a broad variety of fields. Although there are still difficulties associated with performance, scalability, and interoperability, the continued presence of quantum-resistant cryptographic systems as adopted by various industries, standardization initiatives, and experimental implementations are good reasons to believe that quantum-resistant cryptographic systems are possible. Further studies and partnerships will be necessary to perfect these solutions and make them effective in the integration of the future digital infrastructures.

8. Threat Modeling and Practical Challenges

The implementation of post-quantum cryptography (PQC) systems brings with them a new layer of security concerns that go beyond the hypothetical power of algorithms. Though, PQC algorithms are developed due to their resistance to quantum attacks, their application to real-life conditions exposes them to numerous operational risks and vulnerabilities. Threat modeling is thus necessary to determine potential attack vectors, system resilience, and secure deployment (Pulipati, 2026). The following section discusses some of the most important practical issues, such as the vulnerability to the implementation, the risk of the side-channel, the issues of scalability, and the problems of migration.

8.1 Implementation Vulnerabilities

Post-quantum cryptographic schemes, even with good theoretical underpinnings, are prone to weaknesses due to poor implementation or inefficiency. The vulnerabilities in the implementation can be in the form of coding errors, poor choice of parameters, unsecure random number generation or poor validation of the inputs and the outputs. Such vulnerabilities may result in information leakage or even total failure of cryptographic systems.

In PQC, it is common to have high complexity of implementation compared to classical cryptography because of large parameter sizes, and complex mathematical calculations, especially in lattice-based and multivariate systems. This added complexity enhances the chances of making mistakes in the development and integration. Moreover, a lack of tests and standardized implementation guidelines may contribute to these risks (Facon et al., 2018). Rigorous

code auditing, formal verification techniques and observance of secure coding practices are necessary to reduce such vulnerabilities. Moreover, the standardization of libraries and reference implementation is also important to minimize risks associated with implementation.

8.2 Side-Channel Risks in Real Environments

More of a risk to the practical security of PQC systems are side-channel attacks, which take advantage of physical properties of computation, rather than vulnerability of the underlying algorithms. Attackers in the real world can use timing data, power usage characteristics, electromagnetic radiation or cache behavior to deduce secret keys or sensitive intermediate values.

Unless properly implemented, post-quantum cryptographic algorithms, especially those relying on complex arithmetic operations like multiplication of polynomials in lattice-based algorithms, can have data-dependent execution patterns. This increases their susceptibility to side-channel leakage. In addition, the increased computation time and key size of PQC can make observable side-channel signals stronger, which increases the possible attacks (Olaluwe et al., 2025).

Some of the mitigation measures are constant time implementations to remove timing differences, masking information to hide sensitive data, and hardware-based mitigation measures like secure enclave and electromagnetic shielding. The high-resistance to side-channel attacks is important to deploy PQC systems securely, and this is particularly true in those settings where the attackers can access physical or proximity devices.

8.3 Scalability and Usability Issues

One of the major problems with the use of post-quantum cryptographic systems is scalability and usability. Most PQC algorithms have a large key size, high computing power, and bandwidth requirements than classical cryptographic tools. These can affect the performance of the system especially when it is deployed on a large scale like a cloud system, enterprise network, and distributed system.

The usability problems are in addition to the technical scalability. Application of PQC into practice might require modification of software architecture, user interface and workflow. To illustrate, higher latency of cryptographic functions can impact user experience of real-time applications and larger certificate size can make certificate management and storage more challenging. Further, the lack of PQC technologies among developers and system administrators may be a barrier to adoption and increase the chances of misconfigurations (Radanliev et al., 2018).

To overcome these issues, optimized algorithms, efficient implementation techniques and simple tools that facilitate the integration and management should be created. Standardization and educating more individuals on the knowledge of PQC technologies should also be developed to make more individuals embrace the application of the technologies.

8.4 Migration Risks and Transitional Vulnerabilities

The transition to post-quantum solutions and classical cryptography systems is a multi-step, and complex process, which has its own risks and vulnerabilities. During this transition period, the systems are likely to be in the hybrid mode, with both classical and post-quantum algorithms in that they are backward compatible to be safe. Though hybrid solutions provide a promising method of migration, it can also introduce additional attack surfaces and complexity in systems (Giron et al., 2023). The possible threats of migration are compatibility problems with the legacy systems, possibility of misconfigurations during the integration and difficulties in upgrading cryptographic protocols and infrastructure aspects. Moreover, the presence of several cryptographic schemes can open up a possibility of downgrade attack where an attacker can induce the system to use a weaker or older algorithm. Incompleteness or inconsistency in implementing PQC on various components of the system can also bring about transitional vulnerabilities.

The way out of these risks is to ensure that the organizations have clear migration plans which involve comprehensive testing, gradual implementation, and monitoring. Of particular interest is the idea of crypto-agility, which allows systems to swiftly adapt to new cryptographic algorithms, which are useful in long-term security management. Moreover, the compliance with the uniform migration models and best practices can contribute to a safe and effective migration to quantum-resistant cryptographic infrastructures.

Threat modelling and practical issues are essential in the effective implementation of post-quantum cryptographic systems. Although PQC algorithms have high theoretical resistance against quantum attacks, their practical implementation presents a spectrum of weaknesses and complexity in their operation. Implementation flaws, addressing side-channel risks, scalability, and usability, and managing the challenges related to migration are all crucial steps to constructing secure and resilient quantum-safe systems. A proactive and holistic approach to the problems will play an important role in a successful and safe transition to post-quantum cryptography.

9. Standards, Policies, and Migration Strategies

The effective implementation of post-quantum cryptography (PQC) is not only conditional on the creation of safe algorithms, but it is also necessary to create standardized models, regulatory laws, and clear migration plans. Since global digital infrastructures are often based on interoperable cryptographic standards, the concerted actions of governments, standardization agencies and industry participants are crucial to guarantee a seamless and secure move to quantum-resistant systems (Campagna et al., 2015). This part will give an overview of the key standardization efforts, look at the global policy views and describe best practices and practical migration frameworks to organizations.

9.1 Overview of NIST PQC Standardization

One key participant in the development of post-quantum cryptography has been the National Institute of Standards and Technology (NIST), which has led the development of its multi-phase PQC standardization process, starting in 2016. The project has a goal of finding, analysing, and standardizing cryptographic algorithms that are secure against quantum adversaries, but are also efficient enough to implement in practice. It has been an international project, with scientists and organizations providing candidate algorithms, which are then analysed, benchmarked, and cryptanalytically tested.

Following several evaluation cycles, NIST has decided on a list of algorithms to be standardized, including lattice-based algorithms like Kyber to encapsulate keys and Dilithium to sign digests, and hash-based and other complementary algorithms. These selections represent a trade-off between good security assurances, performance, and ability to implement. The NIST standardization project offers a very much-needed critical base of industry adoption by delivering validated and widely embraced cryptographic solutions, which minimizes uncertainty and encourages interoperability among systems (Sjöberg, 2017).

9.2 Global Initiatives and Regulatory Perspectives

Along with NIST, there are several international bodies and regulators that are working on the creation and implementation of post-quantum cryptographic standards. The organizations such as European Telecommunications Standards Institute (ETSI), International Organization of Standardization (ISO) and regional cybersecurity organizations have also initiated programs aimed at testing PQC algorithms, setting security standards and supporting international standardization processes.

Governments and policymakers are starting to see the need to prepare against quantum threats, which is increasingly important, particularly in a regulatory context. In their national cybersecurity strategies, the different countries have emphasized the need to have quantum-safe cryptographic infrastructures, particularly over critical infrastructure such as financial networks, military communications, and medical data. Regulations also start to include demands on quantum-resistant security controls, urging organizations to determine their cryptography reliance and come up with transition plans (Alnahawi et al., 2021).

Through these international efforts, the value of international cooperation to maintain uniformity, interoperability, and broad implementation of PQC standards is reflected. In the meantime, regional focus and regulatory variations may come with several challenges that ought to be well coordinated and reconciled about policies.

9.3 Migration Frameworks

The transition of classical cryptographical systems to post-quantum solutions is a complicated process, which will need orderly structures to manage risks and continuity of activities. In this respect, one of the main terms is crypto-

agility, which is a capability of the systems to change cryptographic algorithms rapidly and effectively without the need to redesign systems extensively. Crypto-agile systems allow organisations to respond to changing security needs, add new standards and respond to new threats with minimal disruption.

The other popular strategy is the hybrid deployment in which both classical and post-quantum cryptography algorithms are deployed together. In these constructions, the security would be maintained so long as at least one of the underlying algorithms is secure, which will offer protection during the transition phase. The hybrid models are especially handy to continue to support backward compatibility with an old system and to slowly implement PQC mechanisms (Näther et al., 2024).

Migration models also focus on phased deployment plans, whereby, PQC algorithms are gradually integrated into the current systems. The roadmap to quantum-safe cryptographic systems is shown in Figure 3.

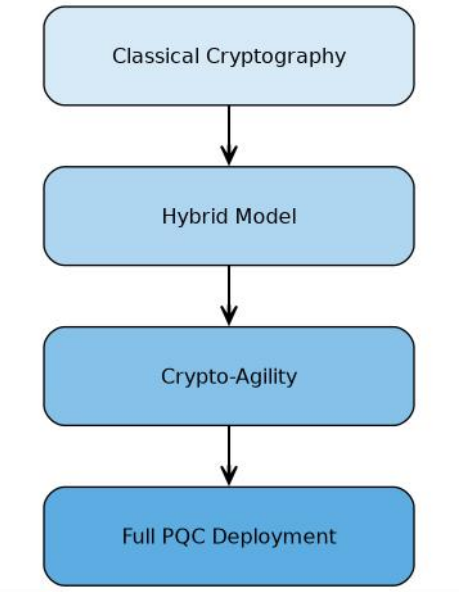

Figure 3. Migration framework depicting the transition from classical cryptography to full post-quantum deployment

By doing this, organizations can test performance, identify possible problems, and improve implementation strategies prior to full-scale implementation. Risk assessment, continuous monitoring, and improvement throughout are fundamental elements of effective migration frameworks.

9.4 Best Practices for Organizations

Organizations will need to be proactive and strategic in order to successfully switch to post-quantum cryptographic systems. Conducting a thorough inventory of current cryptographic resources, such as algorithms, protocols, and key management systems, to determine the dependencies and vulnerabilities, is one of the initial steps. This evaluation

helps organizations to focus on systems that are in urgent need such as those that deal with sensitive information with a long-term confidentiality policy.

Another important best practice is the implementation of crypto-agility in system architectures, which guarantees the flexibility of its use in implementing new cryptographic standards and correctly responding to evolving circumstances. The organizations are also encouraged to invest in replacing cryptographic libraries, infrastructure elements, and security protocols to enable the implementation of PQC algorithms, but also to make sure that it can be compatible with current systems using hybrid mechanisms.

Along with NIST, there are several international bodies and regulators that are working on the creation and implementation of post-quantum cryptographic standards. The organizations such as European Telecommunications Standards Institute (ETSI), International Organization of Standardization (ISO) and regional cybersecurity organizations have also initiated programs aimed at testing PQC algorithms, setting security standards and supporting international standardization processes.

Governments and policymakers are starting to see the need to prepare against quantum threats, which is increasingly important, particularly in a regulatory context. In their national cybersecurity strategies, the different countries have emphasized the need to have quantum-safe cryptographic infrastructures, particularly over critical infrastructure such as financial networks, military communications, and medical data. Regulations also start to include demands on quantum-resistant security controls, urging organizations to determine their cryptography reliance and come up with transition plans (Alnahawi et al., 2021).

Through these international efforts, the value of international cooperation to maintain uniformity, interoperability, and broad implementation of PQC standards is reflected. In the meantime, regional focus and regulatory variations may come with several challenges that ought to be well coordinated and reconciled about policies.

10. Open Challenges and Future Research Directions

Although post-quantum cryptography (PQC) has made considerable strides, there are still several outstanding challenges that need to be tackled to guarantee the secure, efficient and pervasive implementation of quantum-resistant cryptographic systems. With the field constantly developing, current research is needed to enhance the current methods, mitigate weaknesses, and venture towards other avenues that can make digital infrastructures more resilient in the quantum era. In this section, some of the key challenges are identified and potential research directions in the future are given.

10.1 Efficiency Improvements

The main issue in post-quantum cryptography is to enhance the efficiency of cryptographic algorithms without affecting the security. Most PQC schemes, especially lattice-based and code-based schemes, feature large key sizes,

high computational complexity, and higher memory needs than classical cryptographic schemes. These can be detrimental to their application in performance sensitive, resource constrained systems like IoT devices, mobile systems, and real-time applications.

Future studies ought to be aimed at maximizing the structure of the algorithms, minimizing the size of keys and cipher texts and maximizing the speed of computation by employing better mathematical methods and implementation. The prospects of improving performance include hardware acceleration, parallel processing and having specialized cryptographic co-processors. Also, lightweight PQC schemes that are optimized to fit a restricted environment are still a topic of interest.

10.2 Standardization Gaps

Although a lot has been done to bridge the gaps in standardization through various initiatives like the NIST PQC standardization process, there are still some gaps in the standardization. Not every cryptographic application is

covered by existing standards and further efforts are needed to standardise a wider set of cryptographic primitives, such as key exchange protocols, digital signatures, and secure multi-party computation models.

Moreover, it is also a continuing challenge to interoperate between the various PQC algorithms and interoperability with the established cryptographic standards. Differences in the implementation guidelines, parameter options and protocol modifications may cause system inconsistencies and compatibility problems. Further work must be done to extend the standardization structures, come up with an all-inclusive guideline to follow and make sure that the various standardization agencies worldwide are on the same page so that the adoption process can be carried out smoothly.

10.3 Long-Term Security Assumptions

The security of post-quantum cryptography systems in the long-term is contingent on the soundness of the mathematical assumptions underlying it, many of which have not received the same study as classical cryptographic problems. The fact that present PQC schemes are founded on problems that are thought to be resistant to quantum attacks does not negate the potential of future algorithmic breakthroughs, be it classical or quantum, and creates uncertainty as to their sustainability.

Further investigation is required to bolster the belief in these assumptions with rigorous cryptanalysis, formal security proofs, and empirical tests. Also, it is possible to mitigate the dependence on a single type of problem by investigating new assumptions of hardness and diversifying cryptographic strategies. The future security evaluations must also consider the development of quantum computing systems, error correction, and hybrid attack models, which are a combination of classical and quantum forces.

10.4 Integration with Emerging Technologies (AI, 6G, Quantum Networks)

Post-quantum cryptography and its integration with the new technologies are both challenging and promising. With the ongoing development of artificial intelligence (AI), sixth generation (6G) communication networks, and quantum communication systems, new demands are placed on the security, scalability, and performance.

Secure data processing and model protection in AI-driven systems needs to be performed with strong cryptographic algorithms, which can work effectively under distributed and data-intensive conditions. Likewise, 6G networks, which are characterized by an extremely low latency and high data rate, require cryptography solutions, which can be used to achieve high performance criteria, yet ensure high security levels. Quantum networks, however, can open new paradigms of secure communication, which necessitates the simultaneous use of classical, post-quantum, and quantum cryptographic practices. Future studies should examine the ways of successfully incorporating PQC into these new ecosystems, dealing with the issues of optimization of performance, protocol architecture, and interoperability. It will be necessary to have collaborative work between cryptographers, network engineers and system designers to make sure that security solutions keep up with changes in technology.

10.5 Need for Interdisciplinary Research

Post-quantum cryptography is too complex to be answered by a single solution, and it has to be multidisciplinary, a combination of the work of mathematics, computer science, engineering, and cybersecurity. The design, analysis and implementation of PQC systems require not just theoretical underpinnings, but practical knowledge of systems architecture, hardware design implementation and real-life implementation requirements.

Of particular interest is the interdisciplinary research in terms of overcoming the issues of secure implementation, performance optimization and scaling up implementation. Academia, industry, and government organization can be collaborative to speed up innovation, exchange knowledge, and encourage the creation of standardized solutions. As well, it requires educational programs and training to create a highly qualified workforce that will be able to meet the changing needs of post-quantum security.

The field of post-quantum cryptography is a highly essential field of study with extensive implications on the future of digital security. Although significant progress has been achieved, the issues of efficiency, standardization, long-term security and their integration with the new technologies are not completely addressed. To resolve these problems, long-term research, interdisciplinary cooperation, and active adjustment to technological changes will be needed. With these future orientations, the research community will be able to have a robust, scalable and secure cryptographic system that can withstand the quantum era.

11. Conclusion

Post-quantum cryptography (PQC) is a desperate addition to securing the digital systems in the wake of the new

threats of quantum computing. This paper has provided a detailed description of quantum-resistant cryptographic systems, their conceptual framework, the kinds of algorithms, their security properties, the challenges in their implementation and how they can be used in practice. This analysis demonstrates that despite the resistance of PQC algorithms to quantum attacks, their implementation presents a challenge in terms of computational overheads, large key sizes, interoperability and implementation vulnerabilities. The performance measures of PQC and deployment case studies demonstrate that, even with these limitations, PQC can be effectively integrated in the existing infrastructures with optimized deployments and hybrid cryptography. Standardization work, in particular, the one that is led by NIST, has played an important role in offering directions to the world in terms of system adoption and interoperability. Simultaneously, quantum-safe system migration needs systematic plans, such as crypto-agility, gradual implementation, and ongoing risk evaluation. Such practical matters as side-channel resistance, scalability and usability should be discussed to attain efficient and secure implementation. The transition to quantum-resistant cryptography will become successful in the future, and it will be based on the further investigation, cooperation of the fields, and involvement of the industry. By overcoming the existing constraints and coordinating the technological, regulatory, and operational activities, PQC could offer a strong and scalable base to establish future digital infrastructures during the quantum era.

References

1. Barzen, J., & Leymann, F. (2024). Post-quantum security: Origin, fundamentals, and adoption. *arXiv preprint arXiv:2405.11885*.
2. Bavdekar, R., Chopde, E. J., Bhatia, A., Tiwari, K., & Daniel, S. J. (2022). Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. *arXiv preprint arXiv:2202.02826*.
3. Singh, M., Sood, S. K., & Bhatia, M. (2025). Post-quantum cryptography: a review on cryptographic solutions for the era of quantum computing. *Archives of Computational Methods in Engineering*, 1-42.
4. Alvarado, M., Gayler, L., Seals, A., Wang, T., & Hou, T. (2023). A survey on post-quantum cryptography: State-of-the-art and challenges. *arXiv preprint arXiv:2312.10430*.
5. Chhetri, G., Somvanshi, S., Hebli, P., Brotee, S., & Das, S. (2025). Post-quantum cryptography and quantum-safe security: A comprehensive survey. *arXiv preprint arXiv:2510.10436*.
6. Canto, A. C., Kaur, J., Kermani, M. M., & Azarderakhsh, R. (2023). Algorithmic security is insufficient: A comprehensive survey on implementation attacks haunting post-quantum security. *arXiv preprint arXiv:2305.13544*.
7. Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, *605*(7909), 237-243.
8. Sharma, S., Ramkumar, K. R., Kaur, A., Hasija, T., Mittal, S., & Singh, B. (2023). Post-quantum cryptography: A solution to the challenges of classical encryption algorithms. *Modern electronics devices and communication systems: select proceedings of MEDCOM 2021*, 23-38.

9. Xie, J., Zhao, W., Lee, H., Roy, D. B., & Zhang, X. (2024). Hardware circuits and systems design for post-quantum cryptography—A tutorial brief. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *71*(3), 1670-1676.
10. Chang, S. Y., & Khan, Q. (2026). Post-Quantum Cryptography in Networking Protocols: Challenges, Solutions, and Future Directions. *Cryptography*, *10*(1), 12.
11. Bernstein, D. J. (2025). Post-quantum cryptography. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1846-1847). Cham: Springer Nature Switzerland.
12. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, *16*(5), 38-41.
13. Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., & Stebila, D. (2019). Hybrid key encapsulation mechanisms and authenticated key exchange. In *International Conference on Post-Quantum Cryptography* (pp. 206-226). Cham: Springer International Publishing.
14. Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on Bitcoin, and how to protect against them. *arXiv preprint arXiv:1710.10377*.
15. Ralegankar, V. K., Bagul, J., Thakkar, B., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Quantum cryptography-as-a-service for secure UAV communication: applications, challenges, and case study. *Ieee access*, *10*, 1475-1492.
16. Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
17. Cherkaoui Dekkaki, K., Tasic, I., & Cano, M. D. (2024). Exploring post-quantum cryptography: Review and directions for the transition process. *Technologies*, *12*(12), 241.
18. Bagirovs, E., Provodin, G., Sipola, T., & Hautamäki, J. (2024). Applications of post-quantum cryptography. *arXiv preprint arXiv:2406.13258*.
19. Chen, A. C. (2024). Homomorphic encryption based on lattice post-quantum cryptography. *arXiv preprint arXiv:2501.03249*.
20. Zong, C. (2025). The mathematical foundation of post-quantum cryptography. *Research*, *8*, 0801.
21. Meyer, A. (2025). Post-Quantum Cryptography: An Analysis of Code-Based and Lattice-Based Cryptosystems. *arXiv preprint arXiv:2505.08791*.
22. Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., ... & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process.
23. Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: applications and future prospects. *Frontiers in physics*, *12*, 1456491.
24. Albrecht, M. R., Player, R., & Scott, S. (2015). On the concrete hardness of learning with errors. *Cryptology ePrint Archive*.

25. Azouaoui, M., Kuzovkova, Y., Schneider, T., & van Vredendaal, C. (2022). Post-quantum authenticated encryption against chosen-ciphertext side-channel attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 372-396.
26. Jaques, S., Naehrig, M., Roetteler, M., & Virdia, F. (2020). Implementing Grover oracles for quantum key search on AES and LowMC. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 280-310). Cham: Springer International Publishing.
27. Kundu, S., Norga, Q., Karmakar, A., Gangopadhyay, S., Bermudo Mera, J. M., & Verbauwhede, I. (2024). Scabbard: An exploratory study on hardware aware design choices of learning with rounding-based key encapsulation mechanisms. *ACM Transactions on Embedded Computing Systems*, *24*(1), 1-40.
28. Liu, Y., Zhou, B., & Jiang, H. (2025, November). CuKEM: A Concise and Unified Hybrid Key Encapsulation Mechanism. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security* (pp. 4707-4721).
29. Paquin, C., Stebila, D., & Tamvada, G. (2020, April). Benchmarking post-quantum cryptography in TLS. In *International Conference on Post-Quantum Cryptography* (pp. 72-91). Cham: Springer International Publishing.
30. Lei, D., He, D., Peng, C., Luo, M., Liu, Z., & Huang, X. (2023). Faster implementation of ideal lattice-based cryptography using avx512. *ACM Transactions on Embedded Computing Systems*, *22*(5), 1-18.
31. Ravi, P., Paiva, T., Jap, D., D'anvers, J. P., & Bhasin, S. (2024). Defeating low-cost countermeasures against side-channel attacks in lattice-based encryption. *IACR Transactions on Cryptographic Hardware and Embedded Systems*.
32. Lee, W. K., Seo, H., Hwang, S. O., Achar, R., Karmakar, A., & Mera, J. M. B. (2022). DPCrypto: Acceleration of post-quantum cryptography using dot-product instructions on GPUs. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *69*(9), 3591-3604.
33. Kumar, A., Ottaviani, C., Gill, S. S., & Buyya, R. (2022). Securing the future internet of things with post-quantum cryptography. *Security and Privacy*, *5*(2), e200.
34. Ullah, M., Ali, A., & Jadoon, A. K. (2025). Quantum computing and blockchain security: A critical assessment of cryptographic vulnerabilities and post-quantum migration strategies.
35. Kong, I., Janssen, M., & Bharosa, N. (2022, June). Challenges in the Transition towards a Quantum-safe Government. In *Proceedings of the 23rd Annual International Conference on Digital Government Research* (pp. 282-292).
36. Ojetunde, B., Kurihara, T., Yano, K., Sakano, T., & Yokoyama, H. (2025, January). Performance Evaluation of Post-Quantum Cryptography Algorithms for Secure Communication in Wireless Networks. In *2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC)* (pp. 1-9). IEEE.
37. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... & Stehlé, D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In *2018 IEEE European symposium on security and privacy (EuroS&P)* (pp. 353-367). IEEE.

38. Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). Crystals–dilithium: Digital signatures from module lattices.
39. Kannwischer, M. J., Rijneveld, J., Schwabe, P., & Stoffelen, K. (2019). pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4.
40. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key {Exchange—A} new hope. In *25th USENIX security symposium (USENIX Security 16)* (pp. 327-343).
41. Montenegro, J. A., Rios, R., & Lopez-Cerezo, J. (2025). A performance evaluation framework for post-quantum TLS. *Future Generation Computer Systems*, 108062.
42. Banerjee, U., & Chandrakasan, A. P. (2020, June). Efficient post-quantum TLS handshakes using identity-based key exchange from lattices. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.
43. Imran, M., Altamimi, A. B., Khan, W., Hussain, S., & Alsaffar, M. (2024). Quantum cryptography for future networks security: A systematic review. *IEEE Access*, *12*, 180048-180078.
44. Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., ... & Xiong, N. (2023). Post-quantum security: Opportunities and challenges. *Sensors*, *23*(21), 8744.
45. Mahdi, L. H., & Abdullah, A. A. (2025). Fortifying future IoT security: A comprehensive review on lightweight post-quantum cryptography. *Engineering, Technology & Applied Science Research*, *15*(2), 21812-21821.
46. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE access*, *8*, 21091-21116.
47. Pulipati, K. K. (2026). Post-Quantum Cryptography in Identity and Access Management: Readiness, Transition Strategies, and Compliance Implications. *Frontiers in Emerging Engineering & Technologies*, *3*(01), 01-12.
48. Facon, A., Guilley, S., Lec'Hvien, M., Schaub, A., & Souissi, Y. (2018, July). Detecting cache-timing vulnerabilities in post-quantum cryptography algorithms. In *2018 IEEE 3rd International Verification and Security Workshop (IVSW)* (pp. 7-12). IEEE.
49. Olaluwe, A., Nabilah, N. N., Tareq, S., Kulkarni, A. R., & Annamalai, A. (2025). Machine Learning and Side-Channel Attacks on Post-Quantum Cryptography. *Cryptology ePrint Archive*.
50. Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in industry*, *102*, 14-22.
51. Giron, A. A., Custódio, R., & Rodríguez-Henríquez, F. (2023). Post-quantum hybrid key exchange: a systematic mapping study. *Journal of Cryptographic Engineering*, *13*(1), 71-88.
52. Campagna, M., Chen, L., Dagdelen, O., Ding, J., Fernick, J., Gisin, N., ... & Zhang, Z. (2015). Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges. *European Telecommunications Standards Institute*, *8*, 1-64.
53. Sjöberg, M. (2017). Post-quantum algorithms for digital signing in Public Key Infrastructures.

54. Alnahawi, N., Wiesmaier, A., Grasmeyer, T., Geißler, J., Zeier, A., Bauspieß, P., & Heinemann, A. (2021). On the state of post-quantum cryptography migration. In *INFORMATIK 2021* (pp. 907-941). Gesellschaft für Informatik, Bonn.
55. Näther, C., Herzinger, D., Gazdag, S. L., Steghöfer, J. P., Daum, S., & Loebenberger, D. (2024). Migrating software systems toward post-quantum cryptography-a systematic literature review. *IEEE access*, *12*, 132107-132126.
56. Amador, S., Pardo, C., & Mazo, R. (2026). Cybersecurity of Cyber-Physical Systems in the Quantum Era: A Systematic Literature Review-Based Approach. *Future Internet*, *18*(3), 125.
57. Gupta, M. (2026). Security Risks for Enterprises in the Post-Quantum Computing World. *International Journal of Emerging Trends in Computer Science and Information Technology*, *7*(1), 328-337.
58. ßler, J., Zeier, A., Bauspieß, P., & Heinemann, A. (2021).