JOURNAL OF POST-QUANTUM CRYPTOGRAPHY AND SYSTEMS

RESEARCH ARTICLE

Volume 01, Issue 01, 2026

A Comprehensive Review of Post-Quantum Cryptographic Algorithms: Design, Implementation, Performance, and Real-World Deployment Challenges

Liyth H. Mahdi[1*], Alharith A. Abdullah[2]

[1*]College of Information Technology, Department of Information Networks, University of Babylon, Babil, Iraq.
Email:liythhaiderm.net@student.uobabylon.edu.iq (corresponding author)

[2]College of Information Technology, Department of Information Network, University of Babylon, Babil, Iraq.
Email: alharith@uobabylon.edu.iq

ABSTRACT

The rapid advancement of quantum computing poses a significant threat to classical cryptographic systems, necessitating the development of quantum-resistant security solutions. This review provides a comprehensive analysis of post-quantum cryptographic (PQC) algorithms, focusing on their design, implementation, performance evaluation, and real-world deployment challenges. The study examines major PQC algorithm families, including lattice-based, code-based, hash-based, multivariate, and isogeny-based approaches, highlighting their underlying mathematical foundations, security properties, and practical trade-offs. In addition to theoretical aspects, the review explores implementation strategies across software and hardware platforms, emphasising hybrid cryptographic systems and system-level integration for smooth transition from classical infrastructures. Performance evaluation is discussed through key metrics such as computational efficiency, memory usage, and scalability, along with benchmarking frameworks used to assess real-world applicability. Furthermore, the paper analyses critical security aspects, including cryptanalysis, side-channel attacks, and fault-based vulnerabilities, demonstrating that secure implementation is as important as algorithmic strength. Real-world deployment challenges, such as migration complexity, interoperability issues, resource constraints, and evolving standardisation efforts, are also examined in detail. The review identifies key research gaps, particularly the need for improved efficiency, standardised evaluation methods, and large-scale deployment studies. Overall, this work bridges the gap between theoretical advancements and practical implementation, providing insights into the future direction of PQC and its role in securing next-generation digital infrastructures against emerging quantum threats.

Keywords: Post-Quantum Cryptography (PQC); Quantum-Resistant Algorithms; Cryptographic Security; Performance Evaluation; Secure System Deployment Quantum Cryptography (PQC); Quantum-Resistant Algorithms; Cryptographic Security; Performance Evaluation; Secure System Deployment Authentication, Quantum-Resistant Algorithms.

1. Introduction

With the development of communication systems and technology in the modern world, there is a need for cryptography in providing information security. Examples of traditional methods used in cryptography include the RSA method, the Diffie-Hellman method, and the Elliptic Curve Cryptography (ECC). This is due to the nature of these cryptosystems, which is based on solving complex mathematical computations that go beyond the computational capability of conventional computers (Chen et al., 2016).

However, the introduction of quantum computing technology is a paradigm shift that brings risks to the fundamental principles underpinning classical cryptography techniques. The power of quantum algorithms, especially Shor's algorithm, has proven theoretically capable of solving the problems of integer factorisation and discrete logarithms, thus jeopardising the security of public key cryptosystems. Moreover, Grover's algorithm has provided an advantage in searching problems, leading to a quadratic reduction in the security level of symmetric cryptosystems. Even though the realisation of practical quantum computers remains in its early stages, recent advancements in quantum technology suggest that these abilities could soon be feasible, posing serious challenges to the security of current cryptographic systems (Bernstein, 2025; Dam et al., 2023).

To address these issues, Post-Quantum Cryptography (PQC) has become a significant field of research involving the creation of cryptographic algorithms resilient to quantum computing threats. It uses mathematical problems known to be immune to quantum computation, such as lattice-, code-, hash-, multivariate-, and isogeny-based schemes. Different from quantum cryptography, which requires quantum channels of communication, PQC provides an implementable solution for quantum computing by allowing implementation of quantum-resistant algorithms in classical computers (Chen et al., 2016; Bavdekar et al., 2022).

In the last ten years, tremendous progress has been made towards the design and analysis of post-quantum cryptography algorithms owing to worldwide efforts at researching and setting post-quantum cryptography standards. More specifically, a considerable amount of research has taken place under the supervision of the NIST, which is one of the major players behind standardising the post-quantum cryptography algorithms, resulting in the adoption of several quantum-resistant algorithms (Alagic et al., 2022; Alagic et al., 2024; Moody, 2025). Meanwhile, many other researchers have focused on theoretical analyses as well as implementation and performance of various PQC techniques (Nejatollahi et al., 2019; Alvarado et al., 2023; Chhetri et al., 2025).

Despite all this progress, however, the deployment and application of PQC algorithms face some difficulties. The areas where these difficulties emerge include those concerning computational efficiency, large keys, communication overhead, and integration with current cryptographic systems and protocols. In addition, there is an urgent need for a proper transition to quantum-resistant cryptography to address these problems. Researchers in recent times have suggested that improvements should be made in terms of benchmarking schemes and implementation of such systems in cryptographic software libraries (Ahmed et al., 2025; Bavdekar et al., 2022).

Considering the above factors, the current paper presents a critical analysis of various post-quantum cryptographic techniques in an attempt to understand their underlying principles, implementation, performance, and potential operational obstacles. The objective of this research is to address the issue of translating the developments made in this field from a purely theoretical basis to their practical implementations by highlighting the existing gaps in the area under consideration. Thus, apart from the discussion of various PQC techniques and their comparisons, emphasis is put on the feasibility aspect of using these techniques within practical conditions.

The rest of the paper is structured so that these issues can be systematically tackled. This starts off with a review of previous studies done in the field before discussing some of the other elements, such as theoretical concepts, algorithms, implementation, performance assessment, security assessment, and deployment.

2. Literature Review

Post-quantum cryptography is a relatively new but rapidly developing area of research within the last decade, which has emerged mainly due to the ever-growing realisation of vulnerabilities in classical cryptographic schemes resulting from advances in quantum computing. Initially, this research area mainly concerned itself with finding out mathematical issues that were resilient to being solved through quantum computing, which helped create a whole new paradigm in cryptography that did not rely on integer factorisation or discrete logarithm-based approaches. This research opened the door to a great variety of

quantum-resistant cryptographic approaches (Alkim et al., 2016; Hülsing et al., 2016).

Numerous academic papers have addressed the most significant groups of post-quantum cryptographic schemes, including lattice-based systems, which have become one of the leading candidates for future use because of their high level of security and versatility. The lattice-based cryptography techniques have been reviewed in various publications, and it is stated that they are resistant to quantum computer attacks and can be utilized in encryption and the digital signature (Liu et al., 2024; Wang et al., 2023). Additionally, scientific literature exists about the lattice-based cryptosystems, which delineates some key problems and difficulties related to the systems (Malygina et al., 2023).

The literature to date has made comparative studies of the trade-offs that may occur when using different post-quantum cryptographic algorithms, particularly concerning their security, computational needs, and implementation issues. Although there are certain schemes with excellent security properties, these have been known to have large keys or high computational cost, making them less applicable in certain scenarios. Some methods try to balance both efficient performance and adequate security, thus emphasising the importance of selecting the right algorithms based on the specific situation. Important foundational research in the use of lattice-based cryptography for signing messages has improved efficiency and minimised signatures (Ducas & Micciancio, 2014).

Apart from theoretical advances, there have also been an increasing number of studies concentrating on the implementation-related aspects of post-quantum cryptography. The research in the implementation-oriented area has considered both software and hardware implementations of PQCs, with special attention being paid to achieving high performance. In this context, implementations in constrained environments have proven that it is possible to use lattice-based signature schemes in resource-constrained scenarios (Oder et al., 2014). Likewise, performance evaluation tools for microcontrollers and embedded systems have been created to understand how the performance and memory consumption of PQCs can be improved (Kannwischer et al., 2019).

A further interesting area within this literature is the inclusion of post-quantum cryptographic algorithms into current communication protocols. This can be achieved using hybrid methods, where classical cryptography and post-quantum cryptography methods are used together in order to provide backwards compatibility while improving future security by protecting against attacks using a quantum computer. One particular application of post-quantum cryptography within current protocols is the incorporation of lattice-based key exchange algorithms into the TLS communication protocol, and the proof that this process is indeed feasible (Bindel et al., 2019; Bos et al., 2015).

Moreover, there is still an urgent need for further studies related to the security analysis and cryptanalysis of post-quantum cryptography. Several researchers have analysed possible threats based on classical and quantum attack techniques and highlighted the significance of security analysis in post-quantum cryptography. For instance, Jaques et al. (2020) conducted studies focusing on the implications of quantum attacks using Grover's search on the security level of symmetric cryptography. On the other hand, Hülsing et al. (2016) discussed the problems of applying hash-based signature schemes to multi-target attacks and proposed efficient approaches for overcoming these problems.

Though great strides have been made by researchers in this field, there are still a number of issues that should be explored further in the available literature. Though a lot has already been done regarding algorithms and analysis of their performance, there still seems to be a dearth of holistic studies in which both the design and implementation aspects are taken into account, along with other factors such as evaluation and deployment. Another issue concerns the paucity of actual deployment and experimentally validated research in real-life settings.

3. Fundamentals of Post-Quantum Cryptography

3.1 Quantum Threat Model

With the advent of quantum computing, there arises a completely new framework for computation, which has far-reaching implications for the security of cryptographic systems used today. Whereas traditional computers employ bits to encode data and process computations, quantum computers utilise quantum bits, also referred to as qubits. Qubits harness the properties of superposition and entanglement to undertake computations at lightning-fast speeds. Quantum computing is exponentially quicker than classical computing in this respect. In this way, cryptographic systems that have relied on the difficulty of solving certain mathematical problems become highly susceptible to attacks using quantum computers. Public key cryptography

systems such as RSA and Elliptic Curve Cryptography are easily compromised by large-scale quantum computers due to the efficiency gains offered by quantum computing. Even symmetric cryptographic systems are impacted, albeit not as severely, since quantum computing algorithms can effectively degrade their security level. Hence, the quantum threat model relies on the assumption that an adversary has access to adequate quantum computing resources, necessitating the development of quantum-resistant cryptographic systems (Mosca, 2018; National Academies of Sciences et al., 2019).

3.2 Security Foundations of Post-Quantum Cryptography

The post-quantum cryptography algorithm is grounded in math problems that are immune to attacks by classical computers as well as quantum computers. In contrast to conventional cryptographic methods, which depend on mathematical assumptions related to numbers, the post-quantum cryptography algorithm utilises alternative computational problems like lattice problems, multivariate polynomials, and hash functions. Specifically, the lattice-based cryptography system has attracted more attention than other types of post-quantum cryptosystems because it is grounded in solid theory and is immune to known quantum attacks after more than a decade of thorough research (Peikert, 2016). Multivariate cryptography systems are dependent on the complexity of solving systems of nonlinear polynomials and offer efficient computation, but proper selection of parameters is required to ensure security (Ding et al., 2020). Post-quantum cryptography algorithms grounded in hash functions are secure because of the features of these cryptographic methods, thus being an appropriate choice for digital signatures (Hülsing, 2013). The design of post-quantum cryptography algorithms is facilitated by systematic analyses of their security features and applications (Chen et al., 2016; Bernstein, 2025).

3.3 Classification of Post-Quantum Cryptographic Algorithms

The post-quantum cryptographic algorithms can be classified into a number of groups, which include the following: lattice-based, code-based, hash-based, multivariate, and isogeny-based cryptosystems, as indicated in Figure 2 below. Lattice-based cryptography is considered one of the most investigated and efficient groups in the field that has practical applications for encryption, key exchanges, and digital signatures. The code-based cryptography is derived from error-correcting codes and belongs to the class of established cryptosystems. This group is noted for the highest level of security yet tends to use enormous keys (Ding et al., 2020). The hash-based cryptography mainly targets the problem of digital signatures and is appreciated for its straightforwardness and proven security. Multivariate cryptography is associated with solving a system of polynomial equations and implies fast computations, yet may encounter problems with key length and cryptanalysis (Ding et al., 2020).

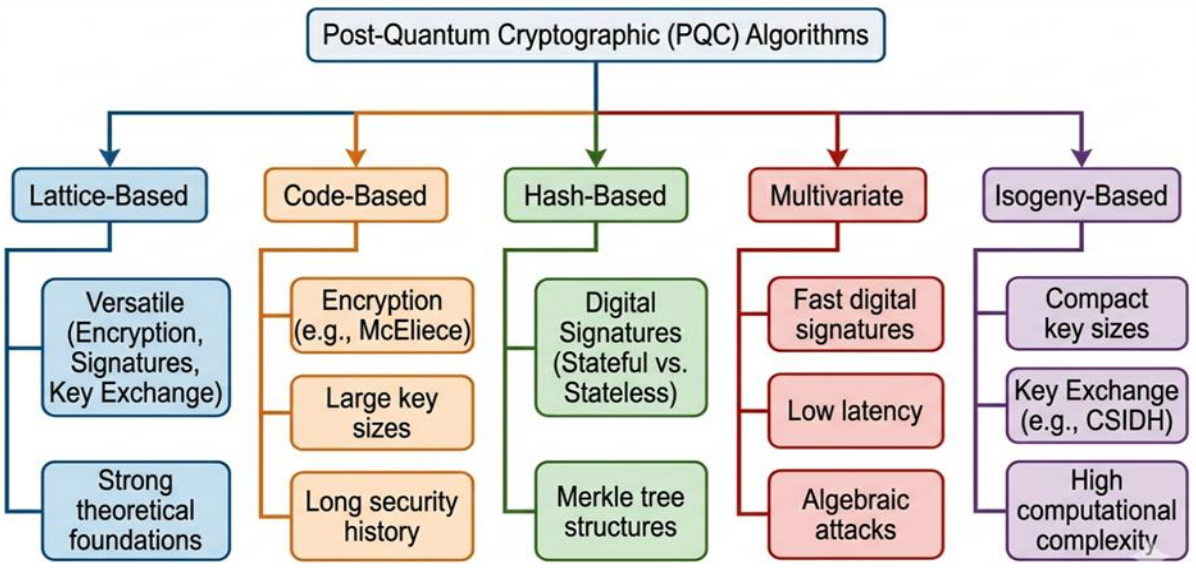

Figure 2. Taxonomy of Post-Quantum Cryptographic Algorithms

All of these have their own pros and cons when it comes to security, performance, and difficulty of implementation. Lattice-based cryptography is usually viewed as the most universal one, but at the same time, the hash-based scheme guarantees high security, which can be achieved using rather easy techniques. Multivariate and code-based cryptography also have an important role to play in particular cases. It is crucial to understand all these classifications in order to determine which public key cryptography system will be the most suitable choice for specific situations (Chen et al., 2016; Bernstein, 2025).

4. Design and Development of Post-Quantum Cryptographic Algorithms

4.1 Lattice-Based Cryptography

Lattice-based cryptosystems have become one of the most reliable solutions in the field of post-quantum cryptography because of their high level of security and flexibility. The underlying principles of the algorithm construction are mainly associated with difficult-to-solve mathematical tasks, such as the Learning With Errors (LWE), Ring-LWE, and Shortest Vector Problem (SVP), which cannot be solved either classically or using quantum computing. In general, the construction of the cryptosystem takes into account two aspects – security and speed, which allows implementing the developed algorithms in the area of encryption, key exchange, and digital signature systems. Moreover, modern approaches aim at designing a modular structure that provides higher performance and reliability compared to classical systems. Finally, the application of lattice-based schemes is justified by their high efficiency and compatibility with other cryptographic standards, making them potential tools for the future (Meyer, 2025; Singh et al., 2025).

4.2 Code-Based Cryptography

Code-based cryptography represents one of the oldest methods in designing quantum-safe cryptographic primitives that make use of the problem of decoding linear codes. In developing code-based cryptosystems, the most commonly used technique is the implementation of error-correction codes like the Goppa code to design encryption schemes. One of the main advantages of code-based cryptography is the history of resistance to cryptanalysis attacks that it offers, thereby ensuring a very high degree of security. Nevertheless, the biggest problem in designing code-based schemes is the need for huge keys that could affect performance. There have been many efforts to develop efficient algorithms and designs for code-based cryptography (Meyer, 2025; Singh et al., 2025).

4.3 Hash-Based Cryptography

Hash cryptography concentrates mainly on schemes used in digital signatures and is based on characteristics of cryptographic hash functions. Security of schemes that are created in this domain is achieved through simplicity, security, and resistance to quantum attacks. Most signature schemes based on a hash function use Merkle trees as a way to achieve fast signature verification. Hash-based schemes are divided into two classes, namely, stateful and stateless schemes. Management of signing states is required when implementing stateful schemes, while there is no need for managing states when working with stateless schemes, though there will be some additional computing and communication costs involved.

4.4 Multivariate Cryptography

The underlying principle of multivariate cryptography is the hardness of solving multivariate polynomials over finite fields, and this problem is believed to be hard even for quantum and conventional computing machines. The development of multivariate cryptographic systems centres on the creation of highly effective signature schemes that require less processing time. Multivariate schemes are appealing because they have minimal latency and easy mathematical computations. Nonetheless, there are limitations such as large key size and vulnerability to certain types of algebraic attacks, that pose security risks to these cryptographic schemes.

The need for better ways of designing multivariate cryptographic schemes has been emphasized in recent research efforts (Singh et al., 2025).

4.5 Isogeny-Based Cryptography

Isogeny-based cryptography is another type of post-quantum cryptographic algorithms that utilize the properties of elliptic curves along with the computational hardness of finding an isogeny between elliptic curves. The main advantage of these algorithms lies in their ability to generate relatively small keys in comparison with other classes of post-quantum cryptographic algorithms. The design of isogeny-based algorithms is primarily concerned with developing key exchange and encryption protocols through the use of complicated algebraic constructs. New research in recent times has been conducted into effective isogeny computation techniques on more sophisticated curves. Nevertheless, the computational complexity associated with these algorithms and possible cryptanalytic attacks calls for further analysis of their security in the long term (Baraka & Ezzouak, 2025). The following table summarises a comparative discussion of various families of post-quantum cryptographic algorithms and their security and application domains.

Table 1. Comparison of Post-Quantum Cryptographic Algorithms

Algorithm Type	Security Basis	Key Size	Performance	Applications	References
Lattice-Based	LWE, SVP	Medium	High	Encryption, Signatures	(Peikert, 2016; Liu et al., 2024; Wang et al., 2023)
Code-Based	Error-correcting codes	Large	Moderate	Encryption	(Chen et al., 2016; Bavdekar et al., 2022)
Hash-Based	Hash functions	Small	Moderate	Digital Signatures	(Hülsing et al., 2016; Hülsing, 2013)
Multivariate	Polynomial equations	Medium	High	Signatures	(Ding et al., 2020; Beullens, 2021)
Isogeny-Based	Elliptic curve isogenies	Small	Low	Key Exchange	(Baraka & Ezzouak, 2025)

4.6 Security Proofs and Theoretical Analysis

The development of post-quantum cryptographic protocols is intrinsically linked to their security proofs and theoretical foundations. The majority of post-quantum protocols are designed to attain provable security by reducing the task of compromising the protocol to solving a difficult mathematical problem, which ensures that any attack on the cryptographic protocol would be at least as hard as solving the problem. Security proofs are usually established using formal security frameworks that take into account attacks from classical and quantum computers. Apart from the theoretical foundations, the design process incorporates cryptanalysis to reveal potential vulnerabilities in the protocol (Alnaseri et al., 2025). Recent studies have highlighted the need for the examination of computational complexity and optimisation of performance, especially in resource-constrained settings such as embedded systems.

5. Implementation Strategies and System Integration

5.1 Software Implementations

Implementation of post-quantum cryptographic algorithms in software is of crucial significance for their practical realisation and deployment. PQC algorithm implementation Software Implementation: Implementation of PQC algorithms is focused on integrating the algorithms into popular cryptography libraries and protocols. It proposed the concept of incorporating quantum-resistant algorithms into the normal architecture, e.g. cryptographic communication protocols, web security layers, and virtual private networks. As an example, the application of lattices to key exchange algorithms has shown

that it can and is efficient in real-life situations (Alkim et al., 2016). The Open Quantum Safe project may be regarded as an essential landmark in the implementation of post-quantum cryptography algorithms due to its significant role in developing software solutions for employing quantum-resistant technology in cryptography (Stebila & Mosca, 2016). It should be noted that implementing PQC algorithms requires high optimisation levels due to their greater computational complexity and larger keys.

5.2 Hardware Implementations

The application of PQC algorithms using hardware components is very important to ensure the best performance of such algorithms. FPGAs, ASICs, and microcontrollers are common hardware components used for the optimisation of encryption processes. It has also been possible to analyse and optimise the performance of PQC algorithms by applying benchmarking tools like PQM4, which have taken into consideration the computing efficiency, memory usage, and energy consumption (Kannwischer et al., 2019). Hardware application of PQC algorithms becomes even more necessary in embedded and IoT systems because of challenges posed by resource constraints.

5.3 Hybrid Cryptographic Systems

The hybrid approach to cryptosystems represents a bridging technology that aims to include post-quantum cryptographic technologies into already existing structures. These hybrid systems involve using classical and post-quantum cryptographic methods to offer protection from modern and future attacks. For instance, hybrid key exchanges have already been suggested and incorporated into protocols like TLS 1.3, ensuring that classical and post-quantum cryptography can coexist (Stebila et al., 2020). The advantage of hybrid cryptosystems is that they can be used while transitioning to full post-quantum encryption.

5.4 Architectural Considerations

Post-quantum cryptographic algorithms must be integrated into modern computers through proper architecture design to guarantee efficient, scalable, and interoperable solutions. The system architecture should be able to cater for both the computation and storage intensities of post-quantum cryptographic algorithms and maintain a good level of performance. Practical solutions for generating certificates and deploying post-quantum cryptography algorithms in large scale and in industrial settings have been developed to ensure seamless integration into existing computer infrastructure (Ricchizzi et al., 2025). Moreover, there have been investigations in practical use cases of post-quantum cryptography to identify key concerns such as migration strategies and challenges in real networks (Sowa et al., 2024). Additionally, some practical studies have examined the integration of post-quantum cryptographic techniques into highly complex and highly specialised systems, such as ITSs (Al Mamun et al., 2026).

There are various components that can be used to integrate post-quantum cryptographic algorithms into modern computer architecture, which include software libraries, hardware accelerators, and hybrid cryptographic frameworks, as shown in Figure 3.

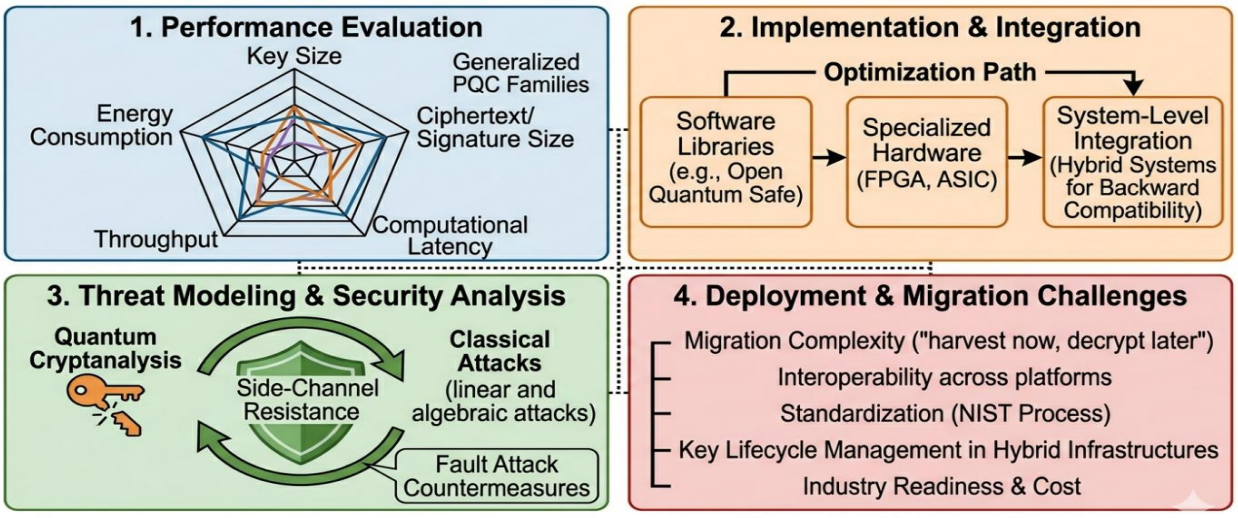

Figure 3. Multidimensional Challenges in Real-World PQC Deployment

Furthermore, the implementation of PQC in constrained computing settings, such as IoT devices, demands the use of efficient algorithms and optimisation techniques to achieve feasibility without sacrificing security (Lopez et al., 2025). It is thus evident that quantum cryptography demands system architectures that can adapt and accommodate evolving needs as new technologies emerge and new cryptographic approaches become necessary.

6. Performance Evaluation and Benchmarking

6.1 Evaluation Metrics

The performance of post-quantum cryptographic algorithms can be measured by multiple criteria such as the key size, latency, and power, as presented in Table 2 below. In contrast to traditional cryptographic systems, post-quantum cryptographic algorithms often consume extra computing resources; hence, the necessity to conduct a performance analysis to measure their efficiency through established metrics. The key parameters used to evaluate post-quantum cryptography algorithms include the key size, the size of the ciphertext, the size of the signature, latency, memory, and energy requirements. Some post-quantum cryptography algorithms have relatively large key sizes and a higher communication overhead, which makes it important to consider these aspects carefully while choosing an appropriate post-quantum algorithm for practical application (Commey et al., 2025; Abbasi et al., 2025).

Table 2. Performance Evaluation Metrics in PQC

Metric	Description	Importance	References
Key Size	Size of public/private keys	Storage, communication cost	(Abbasi et al., 2025; Commey et al., 2025)
Ciphertext Size	Size of encrypted data	Bandwidth efficiency	(Abbasi et al., 2025)
Signature Size	Size of digital signature	Transmission overhead	(Chhetri, 2026)
Computational Time	Encryption/Decryption time	System performance	(Turino et al., 2025; Bae et al., 2022)
Memory Usage	RAM required	Embedded systems	(Kannwischer et al., 2019; Lopez et al., 2025)
Energy Consumption	Power usage	IoT & mobile devices	(Lopez et al., 2025; Commey et al., 2025)

6.2 Comparative Performance Analysis

Comparison of algorithm performances helps in understanding both the advantages and weaknesses of post-quantum cryptography techniques. With a detailed comparative analysis, one can easily determine which algorithm is the most efficient and practical. While lattice algorithms have shown good performance in computation, code-based algorithms have relatively large key sizes but also provide great security. Signature algorithms include other trade-offs when compared to the other two types, including signature sizes and computational complexity. The choice of a particular algorithm will depend on the use case and environment. Comparative performance testing conducted using various computer systems has shown the difference in efficiency depending on hardware capabilities (Abbasi et al., 2025).

6.3 Experimental Studies and Benchmarking Frameworks

Performance assessments through experimental studies and benchmarking tools are key to assessing the performance capabilities of post-quantum cryptographic systems. This involves implementing such cryptographic algorithms in controlled environments and assessing their performance attributes under different conditions. Several benchmarking tools have been developed to evaluate execution time, memory utilisation, and throughput on various types of

hardware, including microprocessors and Internet of Things devices. It is worth noting that some recent benchmarking tests have found that although possible, the performance attributes of some PQC algorithms are limited when implemented in constrained environments (Chhetri, 2026). It has been proposed that a standard benchmarking tool be designed to aid the evaluation process and make a fair comparison among cryptographic algorithms (Turino et al., 2025). Lastly, the analysis of the protocol performance, such as IPsec/TLS compatibility with PQC algorithms, can give additional information regarding the feasibility of these algorithms (Bae et al., 2022; Kwiatkowski and Valenta, 2019).

6.4 Scalability and Efficiency Considerations

The first thing to take into account while implementing PQC systems is scalability. As complexity increases, the important thing is that all algorithms will be performed effectively without an additional load. Hence, scalability is an essential feature of PQC systems, making it possible for them to handle high-throughput operations like cloud computing, encrypted communication, and Internet of Things (IoT). Various approaches can enhance performance, using algorithms, hardware acceleration, and parallelisation techniques. Also, some studies have emphasised the necessity of researching the possibility of implementing PQC into consumer devices and large infrastructures to examine the performance constraints and barriers to adoption (Commey et al., 2025).

7. Threat Modelling and Cryptanalysis

7.1 Classical and Quantum Attack Models

For post-quantum cryptographic algorithms to be secure, it is essential that their security is analysed from the point of view of both the classical attack model and the quantum attack model. The classical attack model describes an attacker who has access to classical computers and uses methods of attack, including exhaustive search, algebraic attacks, and statistical attacks. The quantum attack model describes an attacker who is using quantum computers and has access to powerful quantum computing algorithms, which make the process of solving certain cryptographic problems much easier. Therefore, the challenge posed by these two models of attack requires that cryptography algorithms be designed to resist them (Albrecht et al., 2015).

7.2 Cryptanalysis of Post-Quantum Algorithms

Analysis is an important factor in assessing the strength of post-quantum cryptography. Different forms of cryptanalysis have been used to analyse various families of post-quantum cryptography algorithms, such as lattice-based cryptography, code-based cryptography, and multivariate cryptography. The study of the problem of hardness in lattice-based cryptography is one way of studying the security of such algorithms (Albrecht et al., 2015). In addition, there have been attempts at analysing multivariate cryptography using algebraic cryptanalysis, which has shown some vulnerabilities in certain systems. This has underscored the need for proper implementation of such algorithms (Beullens, 2021). Finally, analysis of hybrid cryptographic and key encapsulation schemes can help to understand how to integrate them into current algorithms.

7.3 Side-Channel Attacks

Side-channel attacks are considered a critical challenge in the application of post-quantum cryptography (PQC) schemes. While conventional cryptanalysis involves attacking the mathematical nature of algorithms, side-channel attacks focus on physical aspects of implementation, such as timing, power consumption, and electromagnetic emanations. The literature has shown that well-known cryptographic schemes are vulnerable to side channel attacks, with examples including acoustic and electromagnetic attacks that have resulted in leakage of cryptographic keys (Genkin et al., 2014). Specifically, concerning PQC, it is known that lattice-based schemes, among others, are also susceptible to side-channel attacks, due to implementation-dependent issues that allow the leakage of secrets from the implementations (Espitau et al., 2017). Additionally, research work has emphasised the growing need to ensure side-channel resilience in the implementation of PQC (Richmond et al., 2019).

7.4 Fault Attacks and Countermeasures

A fault attack is an attack where errors are intentionally induced into cryptographic systems to reveal confidential data or disrupt system functionality. This attack may be directed at either the hardware or software implementation of cryptographic algorithms, exploiting security holes that occur during computations. Fault attacks on post-quantum cryptography have revealed that lattice-based key encapsulation schemes may leak secret data (Prokop & Peßl, 2021). Defensive strategies against fault attacks comprise the use of redundant methods, error detection measures, and designing algorithms that can withstand or identify errors during the process of execution.

7.5 Security Resilience and Robustness Evaluation

Assessment of the resilience and robustness of PQC schemes calls for a multidimensional approach that should consider different ways of attacking a cryptographic scheme and take into account various circumstances in which a cryptographic system operates. The assessment of security should include both theoretical analysis and practical implementation aspects to guarantee that the algorithms used can withstand not only current but also future attacks. The experience of past instances of vulnerability of standardised cryptographic schemes, for instance, the case of the Dual EC backdoor, shows the significance of a multidimensional approach and the need for transparent cryptography design (Bernstein et al., 2016).

8. Real-World Deployment Challenges

8.1 Migration to Quantum-Safe Systems

The move from classic cryptographic solutions to post-quantum cryptographic (PQC) ones comes with several difficulties for organisations and IT infrastructure. Classic cryptographic solutions are integrated into systems, making a changeover difficult and requiring extensive efforts on the part of organisations. Not only do they have to replace or update their cryptosystems, but they also have to ensure that sensitive information will stay protected not just now but, in the future, when quantum computers become a reality (Mosca & Piani, 2022). It is important to ensure that no one will be able to use quantum computers to break modern encryption and get access to old data – this is why it is often called "harvest now, decrypt later."

8.2 Compatibility and Interoperability Issues

Nevertheless, among the largest issues related to the implementation of PQC-based solutions is their connection to the current infrastructure and compatibility with it. The use of PQC is impractical in practice because many modern communication protocols, applications and hardware employ the traditional cryptographic techniques. The variations in the size of the key, data format and calculations can lead to numerous issues. In addition, interoperability between two systems based on different PQC schemes, or between hybrids of these schemes, requires standardisation activities. The abovementioned issue is a significant move towards the solution of the problem, which is the development of a quantum-proof public key infrastructure.

8.3 Resource Constraints and Performance Overhead

Typically, post-quantum cryptographic algorithms are more computationally intensive and have larger key sizes than their equivalents in conventional cryptography algorithms. This is a problem in situations where there is a lack of computational capabilities, storage capacity, and energy, such as IoT devices, embedded systems, and mobile computing applications. Another challenge is the overhead due to the transmission of large-sized cypher texts and signatures. The need for overcoming these performance issues is important for the wider adoption of PQC schemes.

8.4 Key Management and Infrastructure Challenges

Among the most significant requirements in terms of implementing cryptographic solutions that could deliver secure data transfer are key management. The introduction of PQC brings some challenges concerning this process.

Specifically, the requirement of bigger keys and alteration of algorithm design necessitates the readjustment of PKI processes to support the process of certificate creation, maintenance and deployment. Besides, existing best practices in key derivation and management ought to be modified to align with post-quantum cryptography solutions (Barker et al., 2018). At the same time, the use of keys on a larger scale presents additional difficulties as well.

8.5 Standardisation and Regulatory Challenges

Effective implementation of post-quantum cryptographic mechanisms relies extensively on global standards and regulatory measures. Despite considerable advancements toward standardising PQC protocols, the path toward reaching consensus remains a work-in-progress. The use of differing standards by different regions and sectors can result in conflicts and incompatibility. Cybersecurity agencies report that unified standards and quantum threat mitigation methods must be developed through collaborative initiatives (ENISA, 2021). Organisations need to adapt to the changing regulatory environments while maintaining cryptographic compliance for present and future needs.

8.6 Adoption Barriers and Industry Readiness

Even though more attention is being paid to the threats posed by quantum computers, the use of post-quantum cryptography still faces numerous obstacles within different industries. The reasons for that may be explained by the absence of required knowledge, uncertainties regarding the development of the post-quantum cryptography field, as well as potential difficulties associated with its implementation. For instance, many enterprises are unwilling to switch to new forms of cryptography without having the necessary information and recommendations, as well as knowing whether they will work effectively in practice (Mosca & Piani, 2022). This means that apart from adopting new methods, some companies may also face other issues related to training employees, upgrading existing systems, etc. The transition from research to implementation requires much collaboration on the part of all the parties involved. The practical adoption of PQC raises numerous challenges, which are highlighted in Table 3 below.

Table 3. Deployment Challenges and Solutions

Challenge	Description	Possible Solution	References
Migration Complexity	Transition from classical systems	Hybrid cryptography approach	(Mosca & Piani, 2022; Bindel et al., 2017)
Large Key Sizes	High storage and transmission cost	Compression & optimization techniques	(Bavdekar et al., 2022; Ahmed et al., 2025)
Performance Overhead	Increased computation time	Hardware acceleration (FPGA/ASIC)	(Kannwischer et al., 2019; Abbasi et al., 2025)
Interoperability Issues	Compatibility with legacy systems	Standardized protocols (TLS hybrid)	(Bindel et al., 2019; Stebila et al., 2020)
Key Management Complexity	Managing large and complex keys	Updated PKI frameworks	(Barker et al., 2018)
Lack of Expertise	Limited PQC knowledge in industry	Training and awareness programs	(Mosca & Piani, 2022; ENISA, 2021)

9. Open Challenges and Future Research Directions

Although considerable progress has been made within the realm of PQC, a number of unresolved issues persist, which need to be resolved for the latter to become a reliable and practical solution in the real world. Firstly, there is an urgent requirement to optimise the performance of PQC algorithms, which will certainly pose challenges because of their bulky keys and high demands for computations in case of resource-limited systems like IoT networks. Second, although the majority of PQC methodologies were based on solid mathematical principles, research is needed to enhance the level of their resilience to modern threats to classical and quantum cryptosystems. The main problem with integrating PQC into the current communication platforms is that it creates numerous problems, the most significant one being compatibility, interoperability and cryptographic agility. In addition to this, studies are also acutely required to come up with quantum-resistant protocols rather than merely algorithms to offer quantum-proof solutions in the end-to-end sense. The interdisciplinary approach to work becomes even more crucial when addressing various problems, such as the security of chips design, protection against side-channel attacks, and deployment issues. Finally, the continuous improvement of quantum technology also creates a need to monitor the new threats and implement dynamic defences to achieve quantum safety.

10. Conclusion

Post-quantum cryptography has emerged as a critical field of research in response to the growing threat posed by quantum computing to traditional cryptographic systems. This review has provided a comprehensive analysis of post-quantum cryptographic algorithms, encompassing their fundamental design principles, implementation strategies, performance evaluation, and real-world deployment challenges. Various algorithmic families, including lattice-based, code-based, hash-based, multivariate, and isogeny-based cryptography, have been examined, each offering unique advantages and trade-offs in terms of security, efficiency, and practicality. While significant progress has been made in developing quantum-resistant cryptographic solutions, challenges related to computational overhead, large key sizes, and system integration remain key obstacles to widespread adoption. Furthermore, the analysis highlights that ensuring security extends beyond theoretical robustness, requiring careful attention to implementation-level vulnerabilities such as side-channel and fault attacks. The transition to quantum-safe systems also involves complex considerations, including interoperability, standardization, and regulatory compliance, which necessitate coordinated efforts across academia, industry, and government bodies. As global standardization initiatives continue to evolve, particularly in the selection and deployment of PQC algorithms, the need for scalable, efficient, and secure cryptographic solutions becomes increasingly important. Ultimately, the successful adoption of post-quantum cryptography will depend on bridging the gap between theoretical innovation and practical implementation, ensuring that future digital infrastructures remain secure in the face of advancing quantum technologies.

References

1. Abbasi, M., Cardoso, F., Váz, P., Silva, J., & Martins, P. (2025). A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. *Cryptography*, *9*(2), 32.
2. Ahmed, N., Zhang, L., & Gangopadhyay, A. (2025, August). A survey of post-quantum cryptography support in cryptographic libraries. In *2025 IEEE International Conference on Quantum Computing and Engineering (QCE)* (Vol. 1, pp. 906-917). IEEE.
3. Al Mamun, A., Abrar, A., Rahman, M., Salek, M. S., & Chowdhury, M. (2026). Post-Quantum Cryptography for Intelligent Transportation Systems: An Implementation-Focused Review. *Vehicular Communications*, 101028.
4. 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.

5. Alagic, G., Dang, Q., Moody, D., Robinson, A., Silberg, H., & Smith-Tone, D. (2024). Module-lattice-based key-encapsulation mechanism standard.
6. Albrecht, M. R., Player, R., & Scott, S. (2015). On the concrete hardness of learning with errors. *Cryptology ePrint Archive*.
7. 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).
8. Alnaseri, O., Himeur, Y., Atalla, S., & Mansoor, W. (2025, May). Complexity of post-quantum cryptography in embedded systems and its optimization strategies. In *2025 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 776-781). IEEE.
9. 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*.
10. Bae, S., Chang, Y., Park, H., Kim, M., & Shin, Y. (2022, November). A performance evaluation of ipsec with post-quantum cryptography. In *International Conference on Information Security and Cryptology* (pp. 249-266). Cham: Springer Nature Switzerland.
11. Baraka, M. E., & Ezzouak, S. (2025). Efficient Algorithms for Isogeny Computation on Hyperelliptic Curves: Their Applications in Post-Quantum Cryptography. *arXiv preprint arXiv:2504.04559*.
12. Barker, E., Chen, L., & Davis, R. (2018). Recommendation for key-derivation methods in key-establishment schemes. *NIST Special Publication*, *800*, 56C.
13. 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*.
14. Bernstein, D. J. (2025). Post-quantum cryptography. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1846-1847). Cham: Springer Nature Switzerland.
15. Bernstein, D. J., Lange, T., & Niederhagen, R. (2016). Dual EC: A standardized back door. In *The new codebreakers: essays dedicated to David Kahn on the occasion of his 85th birthday* (pp. 256-281). Berlin, Heidelberg: Springer Berlin Heidelberg.
16. Beullens, W. (2021, June). Improved cryptanalysis of UOV and rainbow. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 348-373). Cham: Springer International Publishing.
17. Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., & Stebila, D. (2019). Hybrid key exchange in TLS 1.3. In *Proceedings of the International Conference on Applied Cryptography and Network Security (ACNS)*.
18. Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., & Stebila, D. (2019, May). Hybrid key encapsulation mechanisms and authenticated key exchange. In *International Conference on Post-Quantum Cryptography* (pp. 206-226). Cham: Springer International Publishing.
19. Bindel, N., Herath, U., McKague, M., & Stebila, D. (2017, June). Transitioning to a quantum-resistant public key infrastructure. In *International Workshop on Post-Quantum Cryptography* (pp. 384-405). Cham: Springer International Publishing.

20. Bos, J. W., Costello, C., Naehrig, M., & Stebila, D. (2015, May). Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In *2015 IEEE symposium on security and privacy* (pp. 553-570). IEEE.
21. 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.
22. 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.
23. 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*.
24. Chhetri, R. (2026). Benchmarking Post-Quantum Cryptography on Resource-Constrained IoT Devices: ML-KEM and ML-DSA on ARM Cortex-M0+. *arXiv preprint arXiv:2603.19340*.
25. Commey, D., Appiah, B., Klogo, G. S., Bagyl-Bac, W., Gadze, J. D., Alsenani, Y., & Crosby, G. V. (2025). Performance analysis and deployment considerations of post-quantum cryptography for consumer electronics. *arXiv preprint arXiv:2505.02239*.
26. Dam, D. T., Tran, T. H., Hoang, V. P., Pham, C. K., & Hoang, T. T. (2023). A survey of post-quantum cryptography: Start of a new race. *Cryptography*, *7*(3), 40.
27. Ding, J., Petzoldt, A., & Schmidt, D. S. (2020). *Multivariate public key cryptosystems*. Springer Nature.
28. Ducas, L., & Micciancio, D. (2014, August). Improved short lattice signatures in the standard model. In *Annual Cryptology Conference* (pp. 335-352). Berlin, Heidelberg: Springer Berlin Heidelberg.
29. ENISA, P. Q. C., & Cryptography, Q. (2021, February). *Current state and quantum mitigation*.
30. Espitau, T., Fouque, P. A., Gérard, B., & Tibouchi, M. (2017, October). Side-channel attacks on BLISS lattice-based signatures: Exploiting branch tracing against strongswan and electromagnetic emanations in microcontrollers. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1857-1874).
31. Genkin, D., Shamir, A., & Tromer, E. (2014, August). RSA key extraction via low-bandwidth acoustic cryptanalysis. In *Annual cryptology conference* (pp. 444-461). Berlin, Heidelberg: Springer Berlin Heidelberg.
32. Hülsing, A. (2013, June). W-OTS+–shorter signatures for hash-based signature schemes. In *International Conference on Cryptology in Africa* (pp. 173-188). Berlin, Heidelberg: Springer Berlin Heidelberg.
33. Hülsing, A., Rijneveld, J., & Song, F. (2016, February). Mitigating multi-target attacks in hash-based signatures. In *Public-Key Cryptography–PKC 2016: 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I* (pp. 387-416). Berlin, Heidelberg: Springer Berlin Heidelberg.

34. Jaques, S., Naehrig, M., Roetteler, M., & Virdia, F. (2020, May). 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.
35. Kannwischer, M. J., Rijneveld, J., Schwabe, P., & Stoffelen, K. (2019). pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4.
36. Kwiatkowski, K., & Valenta, L. (2019, August). Towards post-quantum cryptography in TLS. In *Proceedings of the The NIST Second PQC Standardization Conference, University of California, Santa Barbara, CA, USA* (pp. 22-25).
37. Liu, F., Zheng, Z., Gong, Z., Tian, K., Zhang, Y., Hu, Z., ... & Xu, Q. (2024). A survey on lattice-based digital signature. *Cybersecurity*, *7*(1), 7.
38. Lopez, J., Cadena, V., & Rahman, M. S. (2025, August). Evaluating post-quantum cryptographic algorithms on resource-constrained devices. In *2025 IEEE International Conference on Quantum Computing and Engineering (QCE)* (Vol. 1, pp. 918-925). IEEE.
39. Malygina, E. S., Kutsenko, A. V., Novoselov, S. A., Kolesnikov, N. S., Bakharev, A. O., Khilchuk, I. S., & Tokareva, N. N. (2023). Post-quantum cryptosystems: Open problems and solutions. Lattice-based cryptosystems. *Journal of Applied and Industrial Mathematics*, *17*(4), 767-790.
40. Meyer, A. (2025). Post-Quantum Cryptography: An Analysis of Code-Based and Lattice-Based Cryptosystems. *arXiv preprint arXiv:2505.08791*.
41. Moody, D. (2025, October). Advancing Post-Quantum Cryptography: NIST's Standardization Efforts. In *Proceedings of the 2025 1st Workshop on Quantum-Resistant Cryptography and Security* (pp. 5-5).
42. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready?. *IEEE Security & Privacy*, *16*(5), 38-41.
43. Mosca, M., & Piani, M. (2022). 2021 quantum threat timeline report. *Global Risk Institute*.
44. National Academies of Sciences, Medicine, Division on Engineering, Physical Sciences, Board on Physics, National Materials, & A Decadal Survey. (2019). *frontiers of materials research: A decadal survey*. National Academies Press.
45. Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey. *ACM Computing Surveys (CSUR)*, *51*(6), 1-41.
46. Oder, T., Pöppelmann, T., & Güneysu, T. (2014, June). Beyond ECDSA and RSA: Lattice-based digital signatures on constrained devices. In *Proceedings of the 51st Annual Design Automation Conference* (pp. 1-6).
47. Peikert, C. (2016). A decade of lattice cryptography. *Foundations and TrendsŴ in Theoretical Computer Science*, *10*(4), 283-424.
48. Prokop, L., & Peßl, P. (2021). Fault attacks on CCA-secure lattice KEMs. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2021*(2), 37-60.
49. Ricchizzi, N., Schwinne, C., & Pelzl, J. (2025). Applied Post Quantum Cryptography: A Practical Approach for Generating Certificates in Industrial Environments. *arXiv preprint arXiv:2505.04333*.

50. Richmond, T., Heuser, A., & Gérard, B. (2019, January). Side-Channel Analysis of Post-Quantum Cryptography. In *SecDays 2019-Security Days* (p. 1).
51. 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.
52. Sowa, J., Hoang, B., Yeluru, A., Qie, S., Nikolich, A., Iyer, R., & Cao, P. (2024, September). Post-quantum cryptography (pqc) network instrument: Measuring pqc adoption rates and identifying migration pathways. In *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)* (Vol. 1, pp. 1835-1846). IEEE.
53. Stebila, D., & Mosca, M. (2016, August). Post-quantum key exchange for the internet and the open quantum safe project. In *International Conference on Selected Areas in Cryptography* (pp. 14-37). Cham: Springer International Publishing.
54. Stebila, D., Fluhrer, S., & Gueron, S. (2020). Hybrid key exchange in TLS 1.3. *IETF draft*.
55. Turino, C., Buchanan, W. J., Lo, O., & Thümmler, C. (2025, November). PQC-LEO: An Evaluation Framework for Post-Quantum Cryptographic Algorithms. In *2025 IEEE 7th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)* (pp. 237-247). IEEE.
56. Wang, X., Xu, G., & Yu, Y. (2023). Lattice-based cryptography: A survey. *Chinese Annals of Mathematics, Series B, 44*(6), 945–960.