DS Journal of Digital Science and Technology
Volume 4 Issue 4, 1-32, Oct - Dec 2025
ISSN: 2583-5416/ https://doi.org/10.59232/DST-V4I4P101

Original Article

Securing Data against Quantum Threats: Post-Quantum Cryptography Approaches

Taban Habibu[1,2*], Francis Xavier Ovoni[1,3*]

[1]*Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda.*
[2]*Department of Computer Science, Islamic University in Uganda, Kampala, Uganda.*
[3]*Department of Marketing and Management, Makerere University Business School, Arua, Uganda.*

[2]*hamitech2019@gmail.com

Received: 08 October 2025; Revised: 09 November 2025; Accepted: 12 December 2025; Published: 30 December 2025

Abstract - Quantum computing is rapidly advancing and threatens the cryptographic systems that secure digital communications. Classical cryptosystems, such as RSA and ECC, rely on mathematical problems that are difficult for classical computers but can be solved easily by quantum algorithms, such as Shor's. This challenge underscores the pressing need for Post-Quantum Cryptography (PQC) to safeguard data against both classical and quantum threats. This study provides a comprehensive review of PQC Approaches in securing data against quantum threats by analyzing reviewed journals, conference proceedings, book chapters, and websites. Several researchers reviewed relevant literature published between 2019 and 2026 using the ACM Digital Library, Wiley Online Library, Taylor & Francis, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, and Google Scholar. The review evaluates lattice-based, code-based, Hash-based, multivariate, and isogeny-based schemes across security strength, performance, interoperability, and deployment feasibility in heterogeneous environments, including cloud platforms and Internet of Things devices. The findings indicate that lattice-based schemes, particularly CRYSTALS-Kyber and CRYSTALS-Dilithium, currently offer the most balanced trade-off between efficiency and quantum resistance, while Hash-based schemes such as SPHINCS+ prioritize conservative security at notable performance cost. Code-based approaches, including McEliece, demonstrate strong long-term security but remain constrained by large key sizes. The review highlights implementation, energy, migration, and governance barriers that must be addressed before adoption. The review concludes by emphasizing that transitioning to PQC requires a collaborative effort from academia, industry, and government. Future research should focus on integrating lightweight PQC in IoT, 5G/6G, and cloud environments, as well as developing hybrid models that combine classical and quantum-safe systems. Addressing these issues is crucial for establishing secure data protection in the quantum era.

Keywords - Quantum Computing, Post-Quantum Cryptography, NIST PQC Standards, Quantum-Resistant Algorithms, Data Security.

1. Introduction

The theory of quantum computing emerged in the early 1980s, when researchers, Paul Benioff, Richard Feynman, and David Deutsch proposed quantum mechanical principles, spurring research that led to small quantum models that could be modified to improve the efficiency of physical systems over classical computers (Toxvaerd, 2024; Yang et al., 2023). This field, although initially viewed as a theoretical curiosity, gained traction with Peter Shor's algorithm in 1994. Through his work, Shor demonstrated that an adequately powerful quantum computer would be able to compute discrete logarithms and factor large integers in polynomial time, both of which are at the core of the security of the current public-key cryptography (Bastos & Kowada, 2021). Since the discovery

of Shor's algorithm, scientists have created more quantum algorithms to increase the boundaries of quantum advantage. Among the most remarkable ones was Grover's algorithm, which provides a quadratic acceleration to brute-force search problems (Khanal et al., 2023). Both Shor's and Grover's discoveries, for public-key systems and symmetric systems, respectively, made quantum computing more of a reality, leading to a cybersecurity concern. According to Glassner (2024), nowadays, quantum computing is an important change in the computational paradigm because it entails the application of the principles of quantum mechanics that are not similar to those of classical computers. In contrast to classical computers, which process data using bits that take the values either 0 or 1, quantum computers process data using quantum bits (qubits), which make use of the quantum principle of superposition to exist in multiple states at the same time (Vasantrao & Saxena, 2025; Pandey et al., 2023). Besides superposition, entanglement forms the second principle of quantum computing, where, when two or more qubits are entangled, the state of one immediately correlates with the state of the other even when they are separated by large distances (Chae et al., 2024). This increases their computational efficiency because quantum systems are able to solve multiple computations simultaneously, offering exponential speedups to specific problems (Singh et al., 2025). These principles of superposition and entanglement empower quantum computers to outperform classical computers through quickening processes and advancing industries, leading to the collaborative effort by governments, academia, and industries into developing scalable quantum computers (Preskill,2023).

Today's modern Security is based on traditional cryptographic techniques of Rivest-Shamir-Adleman (RSA) cryptosystem, Elliptic Curve Cryptography (ECC), and Diffie-Hellman as the foundations of secure communication and transactions (Tarawneh, 2023). These are based on the mathematical infeasibility of integer factorization, the discrete logarithm problem in finite fields, or the elliptic curve problem to provide security in communications and transactions (Jain, 2021; Al Busafi & Kumar, 2020). RSA is constructed on the factoring problem of large composite numbers, and the secret key is taken out of the prime factors (Singh et al., 2024). On the other hand, communication is secured by Diffie-Hellman key exchange, by taking advantage of the challenge of calculating discrete logarithms in finite fields, where two parties are willing to share a common secret (base generator and prime modulus), and exchange the values exponentiated to build a common secret (Ajeena, 2024). The Elliptic Curve Cryptography enhances cryptographic efficiency based on the elliptic curve discrete logarithm problem and the group operation. The group operation is an operation on infeasible points, which defines security (Shah & Gor, 2025; Al Busafi & Kumar, 2020). So, the strength of many classical cryptographic techniques is essentially linked to the computational hardness of factoring large integers and discrete logarithms in classical computers, but the emergence of quantum algorithms, most notably Shor's algorithm, fundamentally alters this security landscape by enabling these problems to be solved efficiently on sufficiently powerful quantum computers (Olaoye, 2025).

As quantum computers capable of breaking contemporary cryptosystems become widely available, the threat they pose is neither speculative nor distant. Encrypted data captured today could be stored and decrypted in the future once quantum capabilities mature, a risk commonly described as the "harvest-now, decrypt-later" threat (Singh, 2024; Mascelli & Rodden, 2025; Kagai et al., 2025). This is particularly concerning for data requiring long-term confidentiality, including government records, healthcare data, intellectual property, and financial transactions (Shingari & Mago, 2024; Portovaras et al., 2024). As a result, the cryptographic community increasingly recognizes that proactive migration toward quantum-resistant security mechanisms is both necessary and time-critical (Gilbert & Gilbert, 2024). Post-Quantum Cryptography (PQC) has emerged as a leading approach to addressing this challenge. Unlike Quantum Key Distribution (QKD), which depends on specialized hardware and quantum channels, PQC aims to develop cryptographic algorithms that can be executed on classical computing platforms while remaining secure against both classical and quantum adversaries (Mamatha et al., 2024; Dervisevic et al., 2025).

Several research studies on PQC have produced several families of candidate algorithms, including lattice-based, code-based, Hash-based, multivariate, and isogeny-based cryptographic schemes (Hosseini & Pilaram, 2024;

Alagic et al., 2025). International standardization efforts, particularly those led by the National Institute of Standards and Technology (NIST), have played a pivotal role in evaluating and selecting promising candidates for widespread adoption (NIST, 2026).

Despite these advances, significant gaps remain in the existing body of research. Much of the literature concentrates on algorithmic design, theoretical security proofs, or isolated performance benchmarks. While such contributions are essential, they provide limited insight into how post-quantum algorithms perform in real-world systems or how they can be integrated into existing digital infrastructures. Emerging issues such as cross-platform compatibility, energy consumption on constrained devices, side-channel and implementation vulnerabilities, migration complexity, and organizational readiness are often treated in isolation. Consequently, governments and industries lack a consolidated, evidence-based understanding of the practical implications of adopting post-quantum cryptography at scale. Furthermore, many studies adopt a narrow focus on standardization outcomes, particularly NIST finalists, without sufficiently examining alternative proposals, hybrid cryptographic deployments, or comparative evaluations across heterogeneous environments such as cloud platforms, Internet of Things (IoT) devices, mobile systems, and embedded hardware. Socio-technical factors, including regulatory compliance, legal accountability, and human expertise, are also underrepresented, despite their critical role in successful cryptographic transitions.

This study seeks to address these limitations through a comprehensive review of post-quantum cryptography approaches. Through synthesizing recent peer-reviewed research, technical reports, and empirical evaluations, the study examines not only the cryptographic strength of post-quantum algorithms but also their performance characteristics, deployment challenges, and operational implications. Extending beyond theoretical analysis to include practical considerations such as side-channel resistance, energy efficiency, interoperability, and migration strategies, as well as emerging applications in areas such as IoT systems. Rather than evaluating post-quantum cryptographic schemes in isolation, the study provides a comparative framework that connects algorithmic properties with real-world deployment contexts and organizational constraints. By doing so, it offers a more comprehensive understanding of the readiness of post-quantum cryptography to replace or augment existing security mechanisms.

The remainder of this paper is organized as follows. Section 2 reviews related work on quantum computing fundamentals, quantum threats, the NIST Standardization Process, and post-quantum cryptographic Algorithms. Section 3 describes the materials and methods. Section 4 discusses the findings across cryptographic approaches and application domains. Section 5 compares Post-Quantum Cryptography and Quantum Key Distribution. Section 6 discusses the energy efficiency of Post-Quantum Cryptography on constrained devices. Section 7 discusses the socio-technical and regulatory implications. Finally, Section 8 concludes the paper by summarizing key insights and outlining directions for future research.

2. Related Work

2.1. Quantum Computing Fundamentals

Quantum computing is a developing field that uses quantum mechanics principles to process information in ways classical computers cannot. Quantum computers use qubits that exist in superpositions of both states at the same time, i.e., they have both 0 and 1 values at the same time, unlike classical computer bits that are represented by either 0 or 1. This inherent feature allows simultaneous investigation of various computational routes, which significantly increases their computational efficiency and potential (Stanescu, 2024; Elani, 2021). Qubits also exhibit entanglement, which builds correlations in order to facilitate instant interaction of spatially separated qubits and quantum interference, which enhances the right calculation paths and blocks the wrong ones (Parmer et al., 2023; Bhat et al., 2022; Easttom, 2021). This phenomenon forms the foundation on which quantum computers can address selectively challenging problems exponentially quicker than classical ones, producing new computational potential

in practically any area. Quantum algorithms take advantage of these special quantum qualities to gain performance advantages with respect to classical techniques (Egger et al., 2020; Bravyi et al., 2022). For example, Shor's algorithm is effective in decomposing large numbers, thus compromising the classical cryptographic techniques such as RSA and ECC, while Glover's algorithm provides a quadratic speedup for brute-force searches (Junagade et al., 2024). As these algorithms highlight the pressing need for quantum-resistant alternatives, significant advances have been achieved in quantum hardware in recent years. By early 2025, IBM had defined a path to a scalable, quantum-centric supercomputer to surpass 4000 qubits with enhanced modular architectures and circuit fidelity. Similarly, Google has already shown a major step forward with its Willow quantum processor, which can perform an operation that would take a classical supercomputer an estimated 10 septillion years to complete (Columbus Chinnappan et al., 2025; AbuGhanem, 2025; Valavandis, 2024). D-Wave has expanded the deployment of its advantage system, employing quantum annealing with European partners, demonstrating the growing availability of commercial quantum computing (Wang et al., 2024; McGeoch et al., 2024).

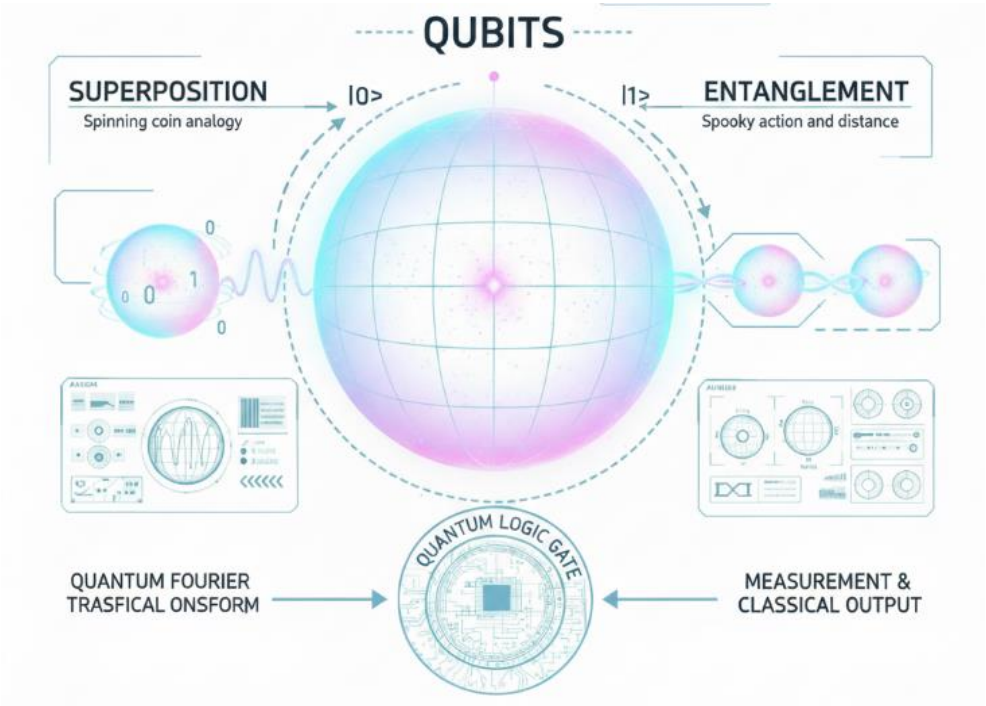


Fig. 1 Quantum computing process

2.2. Quantum Threats to Classical Cryptography

Quantum computing has introduced both transformational potential and existential challenges to contemporary cryptographic systems. The main challenge arises from the fact that quantum algorithms can solve mathematical problems that form the basis of the security provisions of classical cryptography. In Particular, the algorithms proposed by Shor and Grover are the most significant quantum developments that have direct implications for cryptographic systems. These algorithms circumvent the computational hardness conjectures of cryptography, both in terms of public-key and symmetric-key algorithms (Azhari & Salsabila, 2024; Alagic et al., 2025).

2.2.1. Shor's Algorithm

In 1994, Peter Shor suggested an algorithm that changed the outlook of quantum computational power as compared with cryptographic security, popularly known as Shor's Algorithm. This algorithm is an efficient factorization of large integers and discrete logarithms in polynomial time, making it difficult to consider the security

assumptions behind most cryptographic systems, especially those using the public key systems (Wong, 2023). Traditional Cryptographic techniques such as RSA, DH key exchange, ECC, and Digital Signatures are susceptible to the power of this quantum algorithm (Bastos & Kowada, 2021). Shor's algorithm is particularly concerning because it can efficiently solve problems that are difficult to solve in exponential time or create credentials that are otherwise hard to crack by classical techniques (Kumar & Mondal, 2024). For instance, an RSA key, 2048 bits in size, considered hard to crack by classical techniques, might be broken in seconds by a quantum computer of sufficient size. This quantum superiority means it is possible to have a perfect cryptanalytic break in traditional public-key cryptography, and thus, alternative solutions must be immediately sought (Gouzien & Sangouard, 2021; Junagade et al., 2024). This has virtually undermined popular public-key algorithms like RSA, Diffie-Hellman, and ECC, which depend on the infeasibility of factoring and discrete logarithm problems to be secure (Akande, 2025). As companies like IBM advance in improving qubit fidelity and error correction, the threat of a "quantum breakthrough" that could compromise classical public-key infrastructures becomes increasingly imminent (AbuGhanem, 2024).

2.2.2. Glover's Algorithm

The algorithm of Lov Grover, introduced in 1996, provides a different version of quantum acceleration. It allows quadratic speed-ups on unstructured search problems, and the time taken in brute-force searches is significantly shorter (Khanal et al., 2023). Unlike Shor's algorithm, which threatens asymmetric cryptography, Grover's algorithm impacts symmetric algorithms and cryptographic hash functions. Its influence is particularly relevant for algorithms like the Advanced Encryption Standard (AES), SHA-2, SHA-3, and HMAC. By reducing brute-force complexity from O(N) to O(√N), Grover's algorithm effectively halves the security of symmetric keys and hash outputs (Olaoye, 2025). This means that AES256, which classically offers 256 bits of security, would provide only 128 bits of protection against a quantum adversary, still acceptable but closer to the security margin. Therefore, while symmetric cryptography can remain viable in the post-quantum era, it requires larger key sizes and adjusted parameters to maintain adequate levels of protection (Ganesh et al., 2025). The combined effects of Shor's and Grover's algorithms extend beyond mere computational efficiency; they fundamentally erode the trust model of modern digital communications. Yet, Public Key Infrastructures (PKIs), digital signatures, and key exchange mechanisms form the backbone of online authentication, financial systems, and national security frameworks (Banoth & Regar, 2023) as summarized in Table 1 below;

Table 1. Shor's and grover's algorithms and their cryptographic impact

Algorithm	Description	Impact on Cryptography	Affected Algorithms	Implications
Shor's	Employs quantum superposition, entanglement, and the Fourier transform for factoring and logarithms. Requires a large-scale quantum computer.	Compromises public-key schemes by breaking encryption and digital signature integrity.	RSA, Diffie-Hellman, ECDSA, DSA, ECC	Requires transition to quantum-resistant cryptography, significant impact on secure communication, and data integrity.
Grover's	Utilizes quantum superposition and amplitude amplification for quadratic speedup in searching unstructured data; needs a large-scale quantum setup.	Reduces key strength in symmetric schemes by halving the effective key size.	AES, SHA-2, SHA-3	Requires longer key sizes in symmetric cryptography, moderate adjustment compared to Shor's impact, and emphasizes the need for enhanced security measures.

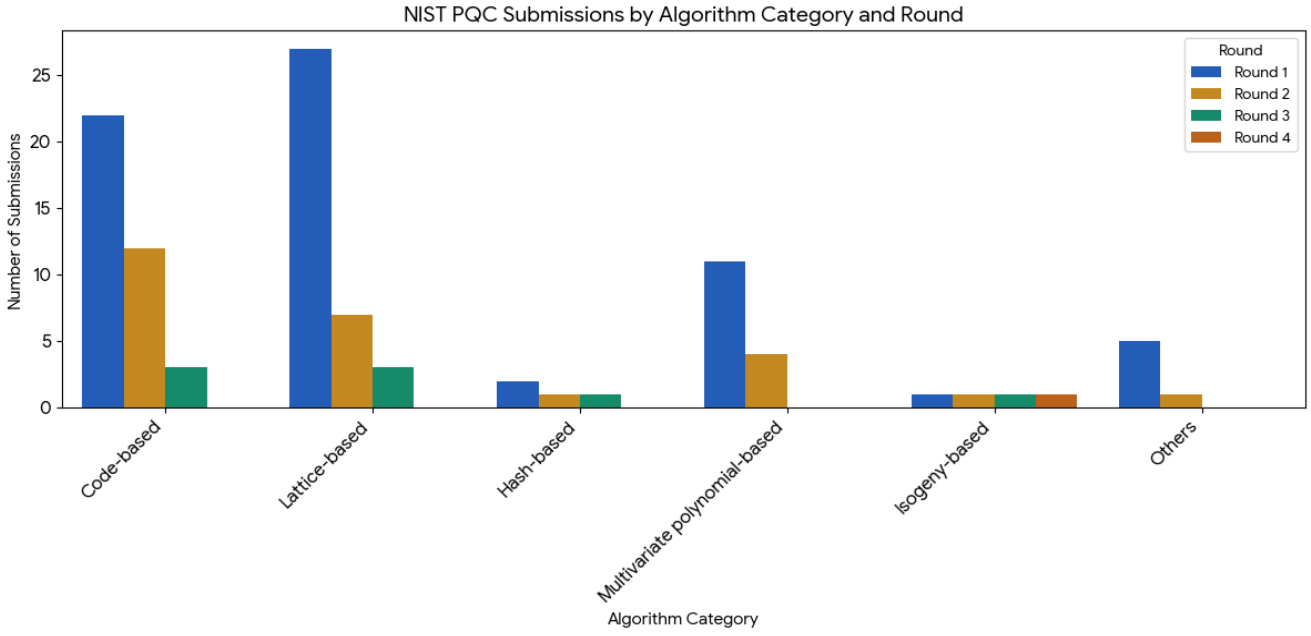
2.3. Post-Quantum Cryptography

Post-Quantum Cryptography (PQC) is a new type of cryptographic algorithm designed to be efficient on a conventional computer as well as be resistant to the possible attack of a quantum computer in the future. The pressing need to implement PQC is demonstrated by the so-called harvest now, decrypt later risk, where the coded information transmitted today may be retained by unscrupulous people to be decrypted by quantum computing at the time of its realization (NIST, 2025). Consequently, there are ongoing intensive research and standardization efforts by organizations like the National Institute of Standards and Technology (NIST) to find and deploy powerful PQC solutions on various mathematical foundations, such as lattices, hash functions, and code-based systems, to ensure the continued confidentiality, integrity, and authenticity of digital communications worldwide (Alagic et. al, 2025).

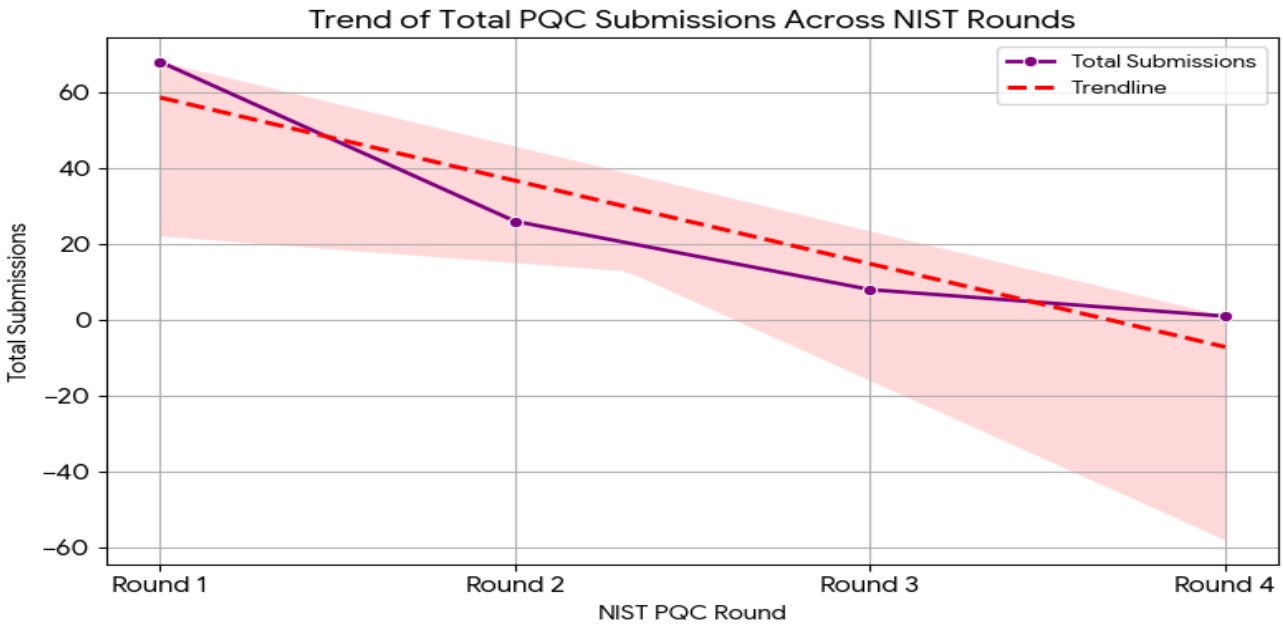
2.3.1. NIST PQC Standardization Project

In December 2016, the National Institute of Standards and Technology (NIST) launched a process to discover, examine, and standardize quantum-resistant cryptographic algorithms that can be successfully integrated with existing networks and communication protocols. These algorithms are quantum and classical threat-resistant. This is still in its fourth implementation process, whereby a few algorithms have been removed, and the others have been scrutinized. Among the 82 algorithms that were submitted to NIST during the first round, only 69 were found to meet the submission requirements of the agency and the minimum acceptance requirements. These submissions, as indicated in Figure 2 below, involved a range of cryptographic approaches, such as lattice-based, hash-based, and multivariate poly systems, each of which applies to a different quantum resistance issue.

The first round of NIST post-quantum cryptography (PQC) standardization saw preliminary assessments of 69 entries in the first round. This aimed at finding out algorithms that could be susceptible to quantum attacks in terms of their security assurances and performance measurements. This round was designed to weed out the options that were evidently inappropriate either by efficiency or complexity considerations, and those that did not otherwise satisfy the high security standards required to combat the threat of quantum computers. The round one ended on January 30, 2019, where 26 algorithms continued to the second round, and 43 were eliminated (Alagic et al., 2024, 2025; NIST, 2025).



(a)



(b)

Fig. 2 (a) PQC algorithms and NIST Round, and (b) Algorithm submissions across NIST Rounds.

The second round of algorithms chosen was reviewed more thoroughly between January and July 2019. This stage involved assessment of performance related to different platforms, test of the complexity of implementation, and thorough evaluation of security against the possibility of quantum attacks. The submissions that exhibited a moderate degree of security, efficiency, and practical utility were only retained, which meant 15 algorithms advanced to the third round, with 11 eliminated. The finalists were vetted on greater security guarantees and deployability in the third phase, which lasted between July 2020 and July 2022. NIST and the cryptography community critically examined each algorithm in many areas, including side-channel attack resistance, compatibility with multiple hardware and software, and compatibility with existing protocols. The contribution of both the public and the private sectors was critical in coming up with any form of latent flaws or performance problems. Finally, NIST chose a single public Key Encapsulation Mechanism (KEM), CRYSTALS-Kyber, and three digital signature algorithms: CRYSTALS-Dilithium, the recommended algorithm; Falcon, which can be used in applications with smaller signature sizes; and SPHINCS, a less fast and heavier algorithm than the first two, but based on a distinct mathematical strategy, and used as a failure mode. Four alternative KEM algorithms progressed to the fourth evaluation phase.

In July 2022, NIST named nominees to this stage of its PQC standardization process. After the first round of selection, four more candidate KEM algorithms went to a Fourth Evaluation Phase, which began in July 2022. This is the current phase of evaluation of these candidates that would potentially be standardized in the future. Simultaneously, NIST stated that it was planning to enlarge its collection of signature algorithms and requested new submissions of public key digital signature algorithms (Alagic et al., 2024; NIST, 2025). Furthermore, NIST adopted three Federal Information Processing Standards (FIPS): FIPS 203, the CRYSTALS-Kyber key-encapsulation mechanism; FIPS 204, the CRYSTALS-Dilithium digital signature standard; and FIPS 205, the SPHINCS+ stateless Hash-based digital signature standard. These drafts were to be reviewed and commented on by the public until November 2023. NIST made improvements upon the feedback obtained and formally adopted the standards after the review. Currently, NIST is working on a new FIPS on the digital signature methodology using Falcon that will likely be published in the near future (Alagic et al., 2024; NIST, 2025).

2.3.2. Post-Quantum Cryptography Algorithms

The emergence of quantum computing poses a significant threat to classical public-key cryptographic systems, including RSA and Elliptic Curve Cryptography (ECC). The PQC community has reacted to this by developing encryption algorithms that are resistant to classical as well as quantum attacks. PQC focuses on solving mathematical problems that are thought to be unresponsive to quantum computers, such as lattice-based, code-based, hash-based, multivariate, and isogeny-based constructions as described below.

Lattice-Based Quantum-Resistant Algorithms

Lattice-based cryptography has become the most studied and most popular type of algorithm to generate a post-quantum public key, due to its solid security principles and realistic performance. A lattice is a geometrical net of infinitely many points, which are regularly spaced, and each point is represented by a vector, and the group of vectors that produce the lattice is a basis. Billions of points are often contained in these multidimensional geometric structures, and information can be encoded and decoded by viewing messages as vectors and the public keys as matrices that process these vectors to ciphertext. Since lattice patterns are characterised by their indefiniteness, these include schemes such as Learning-With-Errors (LWE), Ring-LWE, and NTRU. These lattice-based schemes are incredibly hard to crack even for quantum computers (Liu et al., 2024; Prajapat et al., 2025). This strength has resulted in three large types of lattice-based cryptographic primitives: encryption schemes (e.g., LWE, Ring-LWE, NTRU), signature schemes (e.g., Falcon, Rainbow, Dilithium), and key-exchange mechanisms (e.g., Kyber, Frodo). Their complexity by nature provides high security levels as well as enables efficient implementation on hardware, which leads to reduced power consumption and quicker calculation than most of their classical counterparts (Liu et al., 2024; Wang et al., 2023; Cherkaoui Dekkaki et al., 2024). As a result of such benefits, lattice-based cryptography has been proposed, deployed, and implemented in many applications, including homomorphic encryption, public key encryption, hash functions, digital signatures, and secure key exchange. It is interesting to note that three out of four candidates that were chosen by NIST to undergo post-quantum standardization were lattice-based, reflecting their maturity and reliability.

Table 2. Selected lattice-based quantum-resistant algorithms

Category	Algorithm	Description
Key Exchange	CRYSTALS–Kyber	Secure KEM based on Module-LWE, which offers small keys, fast performance, and strong quantum resistance.
	FrodoKEM	Unstructured LWE-based KEM is extremely secure, but computationally infeasible.
	NTRU Prime	A variant of NTRU that has a better security structure; it has moderate performance, but slower key generation and decapsulation.
	SABER	A variant of KEM requiring less randomness and bandwidth.
Digital Signature	CRYSTALS–Dilithium	Signature scheme based on finding short vectors in lattices. Its larger matrices provide stronger keys.

Moreover, NIST (2024) chose the CRYSTALS-Kyber as the key-exchange algorithm that was to be standardized as the most secure and efficient algorithm according to its high security levels and real-life applicability. Kyber facilitates the creation of an encryption key shared safely without the transfer of the key, through a secure key-encapsulation scheme that is quantum-resistant (Huang et al., 2020). It is secure based on the degree of difficulty of the Learning-With-Errors (LWE) problem on module lattices. Kyber has three different variants, such as Kyber-512, Kyber-768, and Kyber-1024, that have security strengths similar to AES-128, AES-192, and AES-256, respectively (Wang et al., 2023). NIST is standardizing the scheme as the next Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) standard (Alagic et al., 2024). ML-KEM, though grounded on Kyber, has changes to the way

randomness is generated, encapsulation, and key-handling processes. It requires NIST-approved sources of randomness as well, and a different variant of the Fujisaki-Okamoto transform to enhance security (Huang et al., 2020).

NIST tested three more lattice-based KEMs, such as FrodoKEM, NTRU Prime, and SABER, in the process of standardization, but none were adopted. Based on an unstructured version of LWE, FrodoKEM provides a conservative security positioning that can be as secure as the structured lattice assumptions themselves are weak. Nevertheless, it was not suitable to be deployed on a large scale due to its much higher cost in terms of computational power and bandwidth. Modernization of the traditional NTRU system, called NTRU Prime, adopts both the NTRU Prime Ring and deterministic decryption to minimize vulnerability points. Although it has two variants, Streamlined NTRU Prime (SNTRUP), which is a slow key generation algorithm, and NTRU LPrime, which is a faster key generation algorithm than SABER and Kyber, it failed to prove useful performance and maturity to be standardized. SABER, which is founded on the Module Learning with Rounding (MLWR) problem that has low randomness requirements and less bandwidth requirements, comes in three security levels: LightSABER, SABER, and FireSABER. SABER is efficient and well-designed; however, NIST chose Kyber due to the longer and better-studied history of security provided by the Module Learning With Errors (MLWE) foundation (Unsal, 2025; Hu et al., 2025; Lee et al., 2021).

In the case of digital signatures, NIST (2024) is standardizing three algorithms, SPHINCS +, Falcon, and CRYSTALS-Dilithium. SPHINCS+ is a hash-based algorithm that offers higher security at the expense of reduced performance and increased signature sizes. Falcon has the benefit of being more compact in signature and size in small public keys, but less transmission overhead. It uses significant computational accuracy and memory, which makes it impractical to use on limited hardware, such as IoT systems. The most recommended signature scheme is CRYSTALS-Dilithium, which is faster in signature generation and more flexible in implementation, but the size of signatures is too large to fit in a single network packet in certain applications (Lyubashevsky et al., 2020; Gajland et al., 2024; Perlner et al., 2022; Cherkaoui Dekkaki et al., 2024).

Code-based Quantum-Resistant Algorithms

Code-based cryptography refers to cryptographic systems whose security relies on error-correcting codes, with the McEliece and Niederreiter schemes being the most prominent examples (Yu, 2024; Widodo et al., 2024). These systems use the hardness of decoding random linear codes, a problem believed to remain intractable even for quantum computers, to achieve post-quantum security. In the classic McEliece cryptosystem, security is ensured by randomizing messages with deliberately added errors: the private key consists of a binary Goppa code, the public key is a generator matrix derived from a random permutation of that code, and the resulting ciphertext is an error-added codeword that only the private-key holder can correctly decode. Although proposed decades ago, McEliece remains secure against both classical and quantum attacks, leading NIST to advance it to the fourth round of PQC evaluation.

According to Bindal & Singh (2024), McEliece offers fast encryption and decryption and is immune to Shor's algorithm, but it suffers from drawbacks such as very large public keys and ciphertext expansion, which increases bandwidth usage and the potential for transmission errors. While McEliece is not directly suitable for authentication, related signature constructions exist based on the Niederreiter scheme, which provides faster ciphering (Sharifov et al., 2021; Cherkaoui Dekkaki et al., 2024). More recent developments, such as the Bit Flipping Key Encapsulation (BIKE) algorithm, extend the McEliece and Niederreiter ideas by using quasi-cyclic Moderate-Density Parity-Check (MDPC) codes to achieve strong quantum resistance with improved efficiency. BIKE uses a bit-flipping decoding algorithm, cuts down on key sizes, and has likewise advanced to the fourth-round assessment of NIST (Aragon et al., 2022).

Hash-based Quantum-Resistant Algorithms

Cryptography based on hashes is based on the safety of cryptographic hash functions that were initially trendy in the 1970s for their integrity and authentication in digital signatures. The importance of post-quantum cryptography is that it is resistant to quantum attacks. There are two main types of hash-based signature schemes: One-Time Signatures (OTS), where a single privately-owned key can safely sign one message, and Many-Time Signatures (MTS), where hierarchically-organized sets of multiple privately-owned keys are used to allow a single public key to safely verify many messages (Panthi & Bhuyan, 2023; Fathalla & Azab, 2024; Noel et al., 2022). These schemes are based on the property of hash functions to reduce messages of variable length to fixed-length output, which resists collisions such that different messages have different hash values. Earlier literature by Merkle proposed hash-based signatures and the Merkle tree format, which enables the aggregation of a large number of one-time keys, where the bottom tree levels in the tree sign messages and the upper levels in the tree authenticate the bottom tree roots. Even though the early schemes had been affected by the drawbacks of limited signature counts and stateful key management, in which the private keys need to be updated upon use, the hash-based cryptography was again the subject of attention with the emergence of quantum threats. Current hash-based schemes include Extended Merkle Signature Scheme (XMSS), WOTS, and LMS, which are based on the same framework as Merkle and provide successful, low-computation signatures, whereas stateless variants are easier to use at the expense of larger signatures and longer processing times (Cao et al., 2021; Soni et al., 2020). The most sophisticated design in this category is SPHINCS+, which is a stateless hash-based signature scheme and was chosen by NIST at the conclusion of the third round to be post-quantum standardized because of its high-level security and feasible performance.

Isogeny-based Quantum-Resistant Algorithms

Isogenic cryptography builds on the difficulty of locating isogenies between elliptic curves. Some of the important cryptographic systems based on the isogeny theory include the Super singular Isogeny Diffie-Hellman (SIDH), Super singular Isogeny Key Encapsulation (SIKE), and Commutative Super singular Isogeny Diffie-Hellman (CSIDH). A major exchange protocol that warrants mention is SIDH, which makes use of the mathematical characteristics of the supersingular elliptic curves and isogenies, and which provides a secure way of establishing keys that may be resistant to quantum factorization algorithms (Mishra et al., 2025; Drzazga and Krzywiecki, 2022; Varnita et al., 2024). SIKE generalizes the idea into a major encapsulation scheme and ties the distinctive qualities of super singular elliptic curves to create and share cryptographic keys safely (Seo et al., 2020). CSIDH is based on the concepts of SIDH but adds commutative traits of isogenies to support the efficacy and safety of the key generation procedure (Krishnaprabha, 2025). Its protocol is unique in the sense that it investigates such commutative properties, which, in addition to making key generation more efficient, enhance the system's resistance against quantum attacks. SIKE has also been shown to operate well with traditional ECC, with optimized code utilization being used to perform operations on these curves. This incorporation makes it possible to come up with hybrid schemes that successfully combine classical and PQC principles, which demonstrates its promise in preserving cryptographic security in the unleashing of quantum computing. Unlike other encryption schemes and key encapsulation schemes, SIKE is characterized by a very small public key, a much smaller ciphertext size, and is a small component of a cryptographic application (Mishra et al., 2025). Nonetheless, there are also a number of drawbacks of SIKE, and they can be attributed, in large part, to the comparatively uncharted security environment. As an example, the fact that SIKE uses finding isogenies between supersingular elliptic curves of supersingular has not been explored in-depth to date (Drzazga & Krzywiecki, 2022; Cherkaoui Dekkaki et al., 2024). Besides, SIKE has low encapsulation and decapsulation speeds in comparison with other proposed schemes. More to the point, the protocol mandates that auxiliary torsion points should be disclosed publicly, which is operationally necessary and allows exposing more information to attackers (Mishra et al., 2025). In spite of its promising performance and small key and ciphertext sizes, SIKE has had severe security concerns despite being selected as an alternative candidate by NIST during the fourth round of its Post-Quantum Cryptography standardization process (Varnita et al., 2024).

Multivariate Quantum-Resistant Algorithms

This is based on multivariate polynomials over a finite field, which is a kind of system of public key cryptography. These techniques code communications with a group of publicly known multivariate polynomial functions and transform them into a set of values of a polynomial that can be decoded by the recipient using corresponding decryption functions. Because it is known that solving multivariate systems of polynomial equations is an NP-complete problem, the inversion of these functions in the absence of specific inputs is hard to solve and resistant to both classical and quantum computational attacks. This is the primary problem and safety measure of such schemes (Yu, 2024; Widodo et al., 2024; Kuang et al., 2022).

Like RSA, multivariate encryption systems have also been faced with the problem of speed and public key size, and are therefore better adapted to a digital signature system, in which they can offer smaller signature sizes than the other post-quantum methods. Various attempts have been made in the past to develop safe multivariate encryption schemes, but they have failed. The Unbalanced Oil and Vinegar (UOV) that was compromised because of design flaws, the Hidden Field Equations (HFE), which has been successfully attacked against some of its variants, the Merkle-Hellman, which was later broken, and based its security on the knapsack problem, and the more recent Rainbow that relies on multiple layers of polynomial equations, are notable examples of those that have been attacked against successfully (Kuang et al., 2022).

Even with these weaknesses, multivariate cryptography has been gaining popularity in recent years due to its resistance to quantum attackers and the ability to generate smaller signatures. The 19 signature schemes that were submitted to the NIST PQC standardization project include seven multivariate schemes, which advanced to the second round, and only one of them reached the finalist stage. The four last finalists in the second round were Multivariate Quadratic Digital Signature Scheme (MQDSS), Lifted Unbalanced Oil and Vinegar (LUOV), the Great Multivariate Short Signature (GeMSS), and Rainbow. Nevertheless, because of severe security violations that undermined its reliability, Rainbow was eventually excluded from the final selection list (NIST, 2024; Alagic et al, 2024, 2025). Rainbow ciphers out and deciphers messages with multiple layers of a set of polynomial equations. By applying multiple layers, which add more and more layers of complexity to the equations, and subsequently, to the security of the system, Rainbow increases the efficiency and security of the Unbalanced Oil-Vinegar (UOV) scheme. Nevertheless, key sizes of Rainbow are very large, and it has a significantly slow key-producing rate that predisposes it to not fit all applications. In spite of these shortcomings, it remains interesting that Rainbow is proposed to be used in applications in which one requires fast verification or small signatures, which led Rainbow to be a finalist in the NIST PQC standardization process. However, in the course of the competition, the fatal flaws were revealed, and consequently, it was not added to the definitive choice due to the fact of security failures that turned out to be proven (Preucil, 2022).

GeMSS, on the other hand, is characterized by short signatures, fast verification, a slow signing process, and a large public key. To improve resilience against cryptographic assaults, its security model includes the Hidden Field Equations version (HFEv-), iterative Feistel–Patarin permutations that provide unpredictability and nonlinearity, and the hash and sign technique. Even with these sophisticated capabilities, GEMSS's noticeably bigger public key makes it difficult to implement on low-resource devices. Key recovery attacks were launched against GEMSS during NIST's standardization process, just like they were against Rainbow. By revealing the scheme's private key structure, these attacks, which introduced new MinRank instances, seriously undermined its security, eroding trust in its resilience and ultimately causing it to be disregarded (Wu et al., 2025; Thanalakshmi et al, 2023; Cherkaoui Dekkaki et al., 2024). Table 3 below shows PQC algorithm categories, their covered algorithms, strengths, and challenges.

Table 3. PQC categories, algorithms, their strengths and challenges

PQC Category	Algorithms Covered	Strengths	Challenges
Lattice-based	Kyber, Dilithium, FrodoKEM, NTRU	Quantum-resistant	Key sizes, performance
Code-based	McEliece, BIKE	Long-term security	Large public keys
Multivariate	Rainbow, MQDSS	Fast signatures	Broken by recent attacks
Hash-based	SPHINCS+, XMSS	Stateless & secure	Slow signing
Isogeny-based	SIKE	Small keys	Vulnerable to attacks

2.4. Adoption Challenges

2.4.1. Key Sizes and Bandwidth/Storage Implications

Larger public keys, signatures, or ciphertexts are produced by several PQC algorithms than by their classical counterparts. Small ECC keys are smaller than lattice-based public keys and code-based public keys (Classic McEliece) can be hundreds of kilobytes (Kara et al., 2025; Berger et al., 2025). Larger certificates in PKI, more storage, higher bandwidth usage for TLS handshakes, and larger boot/firmware sizes for devices with limitations are all consequences of these increases. Controlling these resource implications is a major engineering challenge, particularly in embedded, mobile, and Internet of Things systems where storage and packet size constraints are severe. (Chhetri et al., 2025).

2.4.2. Performance Overhead and Computational Cost

The use of extra resources, such as memory space and CPU cycles, is often required to make post-quantum cryptography (PQC) algorithms effective and secure. Although the overall performance of lattice-based systems is also of interest, their implementation in a resource-constrained environment, e.g., a low-power microcontroller, may be characterized by considerable performance drawbacks. On the other hand, latency may be increased more in high-throughput server configurations due to the absence of hardware support or special optimizations (Lopez et al., 2025; Abbasi et al., 2025)

2.4.3. Backward Compatibility and Protocol Integration

PQC integration into familiar protocols (TLS, SSH, VPNs, and PKI) requires a protocol design to be carefully considered, including the consideration of interoperability with legacy endpoints, certificate formats, and handshake message size. Lopez et al (2025) note that hybrid modes are a viable short-term solution, although they introduce complexity and possibly even more vectors of attack without being properly defined. Organizations need to design a migration sequence to sustain cross-domain trust relationships, certificate lifecycle management, and service availability.

2.4.4. Implementation Security and Maturity

Security and maturity are needed to provide PQC algorithms with the ability to resist newer threats, such as cryptanalysis and side-channel attacks, since they have a shorter lifetime than more proven algorithms (such as RSA). Whereas implementation security focuses on the practical concerns, such as managing larger keys, complex key management, and any possible side-channel vulnerabilities that these large keys might expose, and the need to be resolved to stop attacks, maturity is required to ensure the algorithms are practical to be applied in the real world (Berger et al., 2025).

2.5. Research Gaps

2.5.1. Lack of Deployment Strategies in Real-World Networks

The real-life networks do not use deployment strategies due to several factors, including performance reasons, especially in those machines with limited resources; security reasons, including side-channel vulnerabilities and huge key sizes; legacy system incompatibility; and the lack of formal migration plans. These factors are a big menace

and would require active interventions such as testing, hybrid operations, and the upskilling of staff members to ensure a safe conversion to the real-world networks (Egbuagha & Ikwunna, 2025).

2.5.2. Limited Cross-Industry Performance Benchmarks

Up until now, benchmarks have frequently been vendor demos or microbenchmarks. There is a lack of thorough, repeatable benchmarking across realistic application situations (TLS connections per second, VPN performance, confined telemetry) and platforms (cloud servers, ARM mobile, microcontrollers, network appliances). Organizations cannot properly evaluate trade-offs among PQC candidates for their specific workload or regulatory context in the absence of cross-industry comparisons. (Egbuagha & Ikwunna, 2025; Barrett-Danes et al., 2025). Table 4 below shows selected literature on Post-Quantum Cryptography (PQC), summarizing techniques, findings, limitations, and relevance to quantum-era security.

Table 4. Summary of key studies on PQC and quantum threats

Author & Year	Focus of Study	Post Quantum Technique	Key Findings	Gap / Limitation	Relevance to Quantum Threats
Wang et al., 2023	NIST PQC standardization	Lattice-based cryptography	Lattice schemes are resistant to the Shor algorithm	High computational cost	Critical for long-term data security
Kannan & Rohithkanna, 2025	Hybrid cryptography transition	Lattice + ECC	Improves classical-PQC transition	Key size overhead	Bridges classical → PQC gap
Ehsan et al., 2025	Key exchange in IoT	Kyber KEM (lattice-based)	Efficient for IoT devices	Side channel risks	PQC ready communication
Chhetri et al., 2025	Quantum decryption risks	Code-based (McEliece)	McEliece remains quantum safe	Large key storage	Useful for critical infrastructure
Iavich et al., 2025	Signature schemes PQC	Hash based (SPHINCS+, XMSS)	Stateless & highly secure	Slow signing	Integrity against quantum attacks
Drzazga & Krzywiecki, 2022	Isogeny-based cryptography	SIKE	Very small keys	Vulnerability exposed in SIKE	Key exchange in constrained environments
Liu et al., 2024	Lattice-based digital signatures	Lattice-based signatures	Practical and secure with ring, blind signatures	Implementation complexity	Post-quantum signature viability
Lopez et al., 2025	PQC implications review	Across families	Broad survey of PQC status	Mostly high-level, limited benchmarks	Snapshot of PQC landscape
Asif & Agal, 2025	Performance & integration studies	Lattice, hash-based, code-based	Lattice shows the lowest overhead vs hash-based	Small sample size	Performance trade-offs in PQC deployment
Aquina et al., 2025	Industry adoption analysis	Multiple PQC schemes	Identifies adoption barriers	Low industry readiness	Transition readiness for quantum threat

Ahmed et al., 2025	PQC support in libraries	Kyber, Dilithium, SPHINCS+	Varied library support across platforms	Many libraries are not ready	Practical deployment of PQC
Gharavi et al., 2024	Post-quantum & quantum blockchains	PQC in blockchain	PQC is viable for blockchain use	Complex hybrid systems	Blockchain resilience to quantum attacks
Chhetri et al., 2025	PQC methods survey	All major families	Comprehensive taxonomy	Limited novel empirical results	Mapping PQC research progress
Abbasi et al., 2025	Performance evaluation of PQC	Lattice, hash, code-based	Comparative overhead analysis	Limited hardware diversity	Real-world feasibility in PQC
Le et al., 2025	Enterprise readiness survey	PQC awareness/strategy	High awareness, low readiness	Survey-based, limited depth	Organizational quantum cryptography risk
Dawson, 2025	PKI & PQC trends	PQC adoption in PKI	Industry not moving fast enough	Survey limits	Sector readiness for quantum threats
Geremew & Mohammad, 2024	PQC transition roadmap	PQC transition frameworks	Identifies that migration planning is needed	Lacks sector-specific guides	National scale quantum preparedness

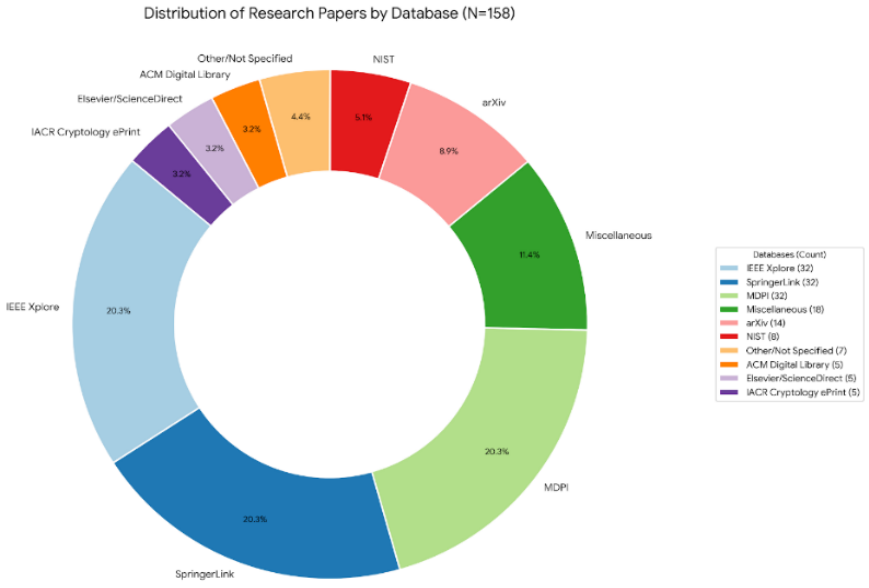
3. Materials and Methods

The study uses insights from computer science, information security, communication technologies, and physics to provide a multi-dimensional perspective. This establishes a foundation for understanding how Quantum Cryptographic approaches can strengthen data security, while addressing adoption challenges and implementation strategies. The primary objective was to identify, evaluate, and synthesize key research articles published between 2019 and 2026, with a focus on PQC approaches in securing data. To ensure thorough coverage, the researchers utilized targeted keywords to gather relevant literature from several scientific databases, including IEEE Xplore, ACM Digital Library, Springer Link, Wiley Online Library, ScienceDirect, MDPI, Digital Library, Emerald Insight, Scopus, Web of Science, and Google Scholar. They used specific search terms and Boolean operators, such as ("post-quantum cryptography" OR "quantum-resistant cryptography") AND ("quantum threat" OR "Shor's algorithm") AND ("IoT" OR "cloud computing" OR "embedded systems" OR "blockchain" OR "migration") ("Internet of things" OR "IoT") AND ("Security" OR "Privacy"), ("PQC" AND "DATA" AND "Security"), ("Post-Quantum Cryptography" OR "Quantum-Safe" OR "Lattice-based cryptography") AND "Data Security" to refine the search results including only relevant papers. The researchers further adjusted keywords to match the search features of each database. The researchers selected these databases because they extensively cover peer-reviewed computer science, engineering, and cybersecurity publications. Relevant research papers were retrieved from the selected databases based on this predefined criteria, including (1) the title, authors, and publication year; (2) objectives and research questions; (3) study design; (4) Data Security; (5) PQC Algorithms; (6) PQC In Data security; (7) applications in Securing Data; (8) case studies and practical implementations; (9) challenges and limitations; (10) future trends and research directions; and (11) conclusions. The collected information was systematically organized to ensure consistency and accuracy. Relevant review materials were selected based on defined inclusion and exclusion criteria, ensuring careful literature screening. These criteria ensured that the chosen research papers were of high quality, directly applicable, and relevant to securing Data using PQC Approaches as detailed in Table 5.

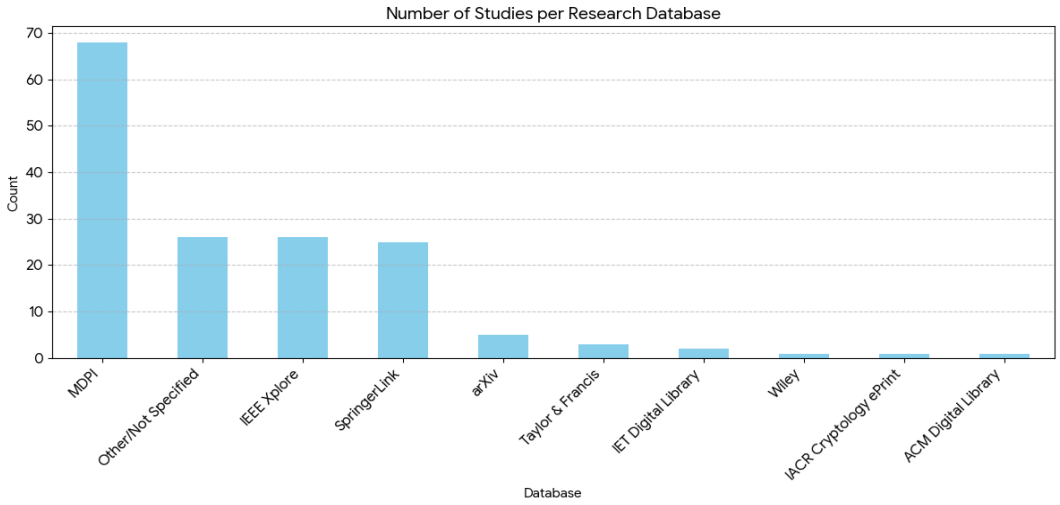
Table 5. Summary of the inclusion and exclusion criteria for choosing relevant research papers

S. No.		Inclusion Criteria	Exclusion Criteria
1	Relevance to the topic	Studies discussing PQC in securing data against quantum threats.	Studies that do not involve PQC in Data security.
2	Publication type	Peer-reviewed journal articles, conference papers, books, and chapters.	Non-peer-reviewed articles, opinion pieces, or blogs
3	Time frame	Publications from 2019 to 2016, capturing the latest advancements	Publications before 2019.
4	Methodology	Empirical studies, simulations, theoretical models, case studies, and frameworks.	Studies that lack robust methodology, experiments, or analysis.
5	Language	Publications in English	Publications not in English.
6	Quality and depth	High-quality research studies with transparent methodology and significant theoretical or empirical contributions.	Low-quality studies with insufficient details, unclear

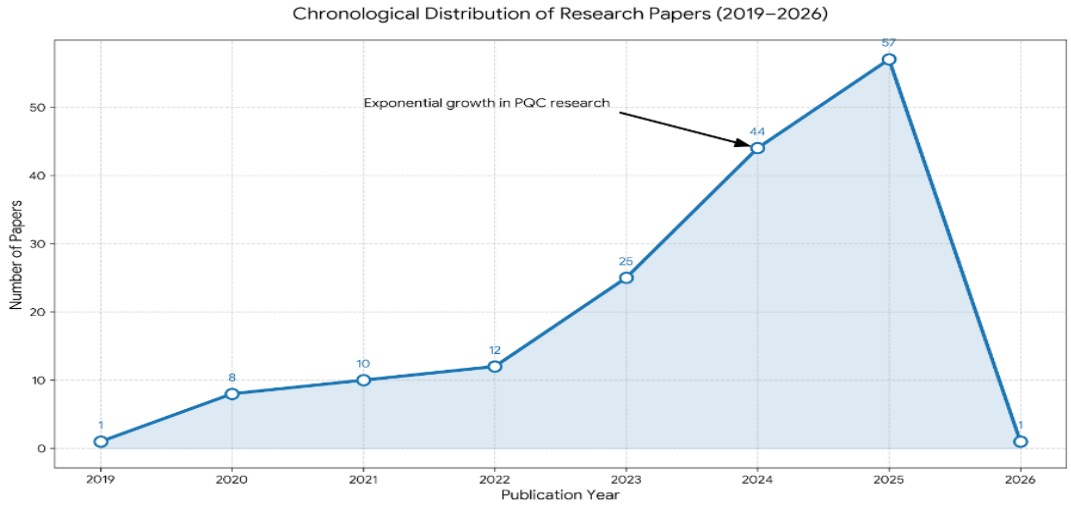
All retrieved articles were carefully screened to identify and remove duplicates. The remaining research papers underwent a preliminary review to extract relevant information from each study, including Authors, Abstracts, year of publication, Study aim and context, Methodology and data sources, and Key findings. Research papers considered suitable were then subjected to a detailed full-text review to confirm their eligibility based on the above inclusion and exclusion criteria. This screening and selection process was carried out independently by several reviewers. A test-retest approach was implemented to reduce potential biases when applying exclusion criteria. Randomly selected papers were re-evaluated multiple times to ensure consistency and accuracy in the selection process. Ultimately, 158 relevant publications were included in the review, comprising 68 from MDPI, 26 from IEEE Xplore, 25 from Springer Link/ Nature, 5 from arXiv prePrint, 3 from Taylor & Francis, 2 from IET Digital Library, 1 from Wiley, 1 from IACR Cryptography ePrint, 1 from ACM Digital Library, and 26 from other Preprint servers (SSRN, ResearchGate), including conference papers, books, and Industry Reports/White papers. The selected studies were systematically analysed, evaluated, and categorized based on their relevance to securing data against quantum threats using PQC approaches. The categorization of these research papers is shown in Figure 3 below.



(a)



(b)



c

(c)

Fig. 3 (a) Distribution of research papers by database, (b) Number of studies per research database, and (c) Chronological distribution of research papers.

The researchers extracted data from each selected study to collect relevant information for thematic synthesis. Data fields included publication details, study focus, technologies (PQC, QKD, IoT, Mobile, and Edge computing), applications (specifically leveraging these technologies for Data security), and methodologies. Thematic analysis was conducted to categorize the studies based on application areas and domains within data Security. Additionally, the research was classified according to technological approaches, highlighting the PQC applications within data security. Qualitative synthesis and thematic analysis methods were used to analyze the data. To validate the review findings, subject matter experts were consulted, the results were cross-referenced with literature, and the robustness of the conclusions was critically assessed. Each study was evaluated for quality based on its methodological rigor, the reliability and validity of its findings, and its relevance to securing data against Quantum threats using PQC approaches.

Since the review focused on analysing literature, no primary data was collected, eliminating the need for ethical approval. However, ethical standards were maintained by properly citing sources and avoiding plagiarism. A subset of studies emphasizing methodologies and performance measures was closely examined to explore PQC

approaches in securing data. The factors considered during the evaluation included the technologies applied, their integration within Data security, the relevance of the insights provided, and the robustness of the methodologies used.

Despite the study's comprehensive approach, it was limited by the rapid advancements in key technologies considered for the study, i.e., PQC, QKD, IoT, mobile, and edge computing, which are evolving rapidly, meaning that some recent developments might have been overlooked. Only studies published in English and accessible through major scientific databases were included, potentially excluding relevant research published in languages other than English or niche outlets. The lack of quantitative analysis or empirical data may weaken the review's robustness, as qualitative evaluations can only partially support the claims. The review may overlook practical challenges associated with real-world implementation by emphasizing theoretical applications. Additionally, as Data security evolves, emerging technological approaches and challenges may impact the relevance and applicability of this analysis.

4. Discussion

This section presents the findings of the review, organized according to cryptographic families, deployment environments, and practical implementation considerations.

4.1. Findings

4.1.1. Distribution of Studies by Cryptographic Family

Analysis of the selected studies reveals a strong concentration of research on lattice-based cryptography (e.g., Wang et al., 2023; Eid & Ismail, 2025; Lei et al., 2023; de Boer & Woerden, 2025; John et al., 2023; Kwala et al., 2024; Cisneros & Olazabal, 2023), which accounts for the majority of empirical evaluations. This dominance reflects both the maturity of lattice-based constructions and their favourable balance between security, performance, and implementation flexibility. For instance, Wang et al. (2023) and Eid & Ismail (2025) conclude that lattice-based cryptography offers strong post-quantum security by relying on worst-case lattice problems that are widely believed to remain intractable even for quantum adversaries, positioning these schemes as leading candidates for future cryptographic standards. The authors also characterize lattice-based schemes as sufficiently efficient for practical deployment, with a favourable balance between computational cost and high security guarantees. In addition, the surveys highlight the implementation flexibility of lattice-based cryptography, noting its suitability for a wide range of cryptographic primitives, such as key encapsulation and digital signatures, and its adaptability across diverse application scenarios and computing environments. Hash-based schemes represent the second most studied family (e.g., Srivastava et al., 2023; Lahraoui et al., 2024; Nagarajan et al., 2024; Tandel & Nasriwala, 2025), primarily in the context of digital signatures requiring long-term assurance. Code-based cryptography appears less frequently due to its large key sizes, while multivariate and isogeny-based schemes are increasingly approached with caution following recent cryptanalytic developments. Across the literature, researchers consistently emphasize that no single cryptographic family is universally optimal. Instead, suitability depends on deployment context, resource constraints, and threat models.

4.1.2. Performance and Deployment Across Heterogeneous Environments

A key finding of the review is the performance variability of PQC schemes across platforms. Studies (e.g., Abbasi et al., 2025; Giron et al., 2023; Bajwa et al., 2025; Carter et al., 2023) evaluating PQC in cloud and server-class environments generally report acceptable latency and throughput overheads, particularly for lattice-based key encapsulation mechanisms integrated into TLS handshakes. In contrast, deployments on IoT and embedded devices highlight challenges related to memory usage, computational overhead, and energy consumption. Several studies demonstrate that hybrid classical–post-quantum configurations offer a practical transitional approach, enabling backward compatibility while improving quantum resilience. For instance, Giron et al. (2023) combine established classical key exchange protocols with post-quantum schemes to retain backward compatibility while

progressively strengthening resistance to quantum attacks. Their analysis shows that by integrating a classical key exchange with a post-quantum mechanism, hybrid constructions support smoother migration from today's infrastructure toward quantum-resilient systems without requiring immediate abandonment of trusted classical protocols, and they can be incorporated into widely used network protocols with acceptable performance and security trade-offs. This transitional approach effectively balances existing interoperability with enhanced quantum resilience, making hybrid key exchange a practical strategy for advancing toward post-quantum security. However, hybrid deployments introduce additional complexity in protocol design and key management, underscoring the need for careful engineering and testing.

4.1.3. Security Beyond Mathematical Resistance

While mathematical resistance to quantum attacks is a necessary condition for post-quantum security, the literature underscores that it is not sufficient (e.g., Jenefa et al., 2023; Owen & Pearson, 2025). Multiple studies (e.g., Mainali & Ghimire, 2025; Olaluwe et al., 2025; Parikh & Parikh, 2025) report vulnerabilities arising from side-channel attacks, including timing, power analysis, and cache-based leakage, particularly in lattice-based implementations. These findings highlight the importance of constant-time implementations, masking techniques, and platform-specific hardening. Implementation-level weaknesses are shown to pose a more immediate risk than quantum cryptanalysis in many real-world contexts. Consequently, several authors argue that deployment readiness should be evaluated holistically, incorporating both cryptographic and systems-security perspectives.

4.1.4. Energy Efficiency and Resource Constraints

Energy efficiency emerges as a critical factor in post-quantum adoption, especially for battery-powered and resource-constrained devices. The reviewed studies (e.g., Patterson et al., 2025; Mahendran, 2025; Abbasi et al., 2025; Lakhan, 2023) indicate that lattice-based schemes generally consume more energy than elliptic curve cryptography but remain feasible for mid-range IoT devices when optimized. Hash-based signature schemes, while secure, often exhibit higher energy and communication costs, limiting their suitability for frequent authentication scenarios. These findings suggest that energy-aware parameter selection and hardware acceleration may play an essential role in enabling scalable PQC deployment.

4.1.5. Migration, Interoperability, and Organizational Readiness

Beyond technical metrics, the literature (e.g., Campbell, 2025; Erol, 2025; Couzens, 2025) identifies migration planning and organizational readiness as major determinants of success. Few studies provide detailed migration roadmaps, but those that do emphasize cryptographic agility, inventory assessment, and staged deployment. Regulatory considerations such as compliance with data protection laws and national cybersecurity frameworks are increasingly cited as influencing algorithm selection and deployment timelines (e.g., Adewale, 2023; Alessa et al., 2025; Sowa et al., 2024). Overall, the synthesis reveals a gap between cryptographic innovation and operational adoption, reinforcing the need for interdisciplinary approaches.

4.2. Comparative Analysis

Table 6. Comparative summary of representative post-quantum cryptography studies

Study	PQC Family	Algorithm(s)	Context	Metrics Evaluated	Findings
Abbasi et al. (2025)	Lattice, Hash, Code	Kyber, Dilithium, SPHINCS+, McEliece	Cloud, edge, embedded	Latency, throughput, memory	Lattice schemes offer the best performance–security balance
Ehsan et al. (2025)	Lattice	Kyber, NTRU	IoT microcontrollers	Execution time, energy	Kyber is feasible on constrained IoT devices

Lopez et al. (2025)	Lattice, Hash	Kyber, Dilithium, SPHINCS+	Embedded systems	RAM, flash, energy	Hash-based schemes are less suitable for frequent ops
Berger et al. (2025)	Lattice	Kyber	Tor network (TLS)	Latency, compatibility	Hybrid PQC deployment is feasible in real systems
Ahmed et al. (2025)	Multiple	Kyber, Dilithium, Falcon	Cryptographic libraries	API support, usability	Uneven PQC library readiness
Aquina et al. (2025)	Lattice vs QKD	Kyber vs QKD	Enterprise networks	Scalability, cost	PQC is more scalable than QKD
Bindel et al. (2023)	Lattice	Kyber	ARM Cortex-M	Cycles, memory	Optimized lattice viable on MCUs
Fathalla & Azab (2024)	Hash-based	SPHINCS+	General platforms	Signature size, time	Strong security, high overhead
Liu et al. (2024)	Lattice	Dilithium, Falcon	Software systems	Size, speed	Dilithium is more robust than Falcon
Dam et al. (2023)	All families	Multiple	Survey	Qualitative metrics	Lattice dominates practicality
Cherkaoui Dekkaki et al. (2024)	Lattice, Hash	Kyber, Dilithium	Migration contexts	Readiness, agility	Hybrid transition essential
Gharavi et al. (2024)	Lattice	Kyber, Dilithium	IoT blockchain	Security, scalability	PQC critical for IoT ledgers
Prajapat et al. (2025)	Lattice	Lightweight lattice signatures	IoT	Energy, memory	Tailored lattice viable for IoT
Bindel & Singh (2024)	Code-based	McEliece variant	Software	Key size, security	Reduced keys but still large
Aragon et al. (2022)	Code-based	BIKE	Network protocols	Bandwidth	Key size remains limiting
Seo et al. (2020)	Isogeny	SIKE	ARM Cortex-M4	Time, memory	High overhead for constrained devices
Cao et al. (2021)	Hash-based	XMSS, Merkle	Hardware	Area, power	Hardware acceleration improves feasibility
Huang et al. (2020)	Lattice	Kyber	FPGA	Resource utilization	Efficient hardware reuse is possible
Lee et al. (2021)	Lattice	SABER	GPU	Throughput	GPUs accelerate lattice KEMs

Hu et al. (2025)	Lattice	NTRU-Prime	TLS	Handshake latency	Optimized PQC improves TLS performance
Egbuagha & Ikwunna (2025)	Lattice	Kyber	Protocol migration	Compatibility	TLS migration is still complex
Singh et al. (2025)	All families	Multiple	Survey	Qualitative	Confirms lattice maturity
Asif & Agal (2025)	Lattice, Code, Hash	Kyber, McEliece, SPHINCS+	Practical apps	Performance	Lattice best all-round
Geremew & Mohammad (2024)	Lattice	Kyber	Critical infrastructure	Risk, readiness	Early adoption recommended
Mascelli & Rodden (2025)	Lattice	Kyber	Blockchain	Privacy, integrity	PQC is essential for long-term ledger security

5. Post-Quantum Cryptography Vs Quantum Key Distribution

As organizations prepare for the security implications of large-scale quantum computing, two primary approaches have emerged to protect cryptographic communications: Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). While both aim to address quantum-enabled threats, they are grounded in fundamentally different security models and impose distinct technical, operational, and economic requirements. Understanding their comparative strengths and limitations is essential for informed decision-making and long-term security planning.

5.1. Security Foundations

Post-quantum cryptography is based on mathematical problems believed to be resistant to both classical and quantum attacks (Wang et al., 2023; Owen & Pearson, 2025). PQC schemes are executed entirely on classical computing platforms and integrated into existing cryptographic protocols using conventional hardware and software stacks (Erol, 2025; Couzens, 2025). Their security relies on unproven but extensively analyzed hardness assumptions, such as lattice problems (Cherkaoui Dekkaki et al., 2024).

In contrast, quantum key distribution derives its security from the laws of quantum mechanics (Kalnina et al., 2025). QKD protocols enable two parties to establish a shared secret key by transmitting quantum states, with the guarantee that any eavesdropping attempt introduces detectable disturbances. This information-theoretic security distinguishes QKD from both classical and post-quantum cryptographic approaches, which rely on computational assumptions (Chen & Tsai, 2025; Kalnina et al., 2025).

5.2. Practical Deployment Considerations

Despite its strong theoretical security guarantees, QKD faces significant barriers to large-scale adoption, such as distance limitations, sensitivity to signal loss, and infrastructure costs, which restrict its deployment primarily to niche scenarios such as government networks, financial interconnects, or metropolitan fiber links. (Kish et al., 2025; Nwaga & Nwagwughiagwu, 2024). Many QKD implementations require specialized quantum hardware, dedicated optical channels, and carefully controlled physical environments (Kish et al., 2025). By contrast, PQC is inherently software-based, enabling deployment across a wide range of platforms, including cloud infrastructures, mobile devices, and Internet of Things (IoT) systems (Stanescu, 2024; Liu et al., 2024; Preskill, 2023). Most PQC schemes can be integrated into existing protocols such as TLS, IPsec, and secure email with minimal architectural

changes. This compatibility significantly lowers the barrier to adoption and enables incremental migration strategies (Chen & Tsai, 2025).

5.3. Performance, Scalability, and Cost

Performance evaluations reported in the literature consistently indicate that PQC schemes introduce measurable but manageable overheads in terms of computation, memory usage, and communication bandwidth. These overheads vary across cryptographic families and platforms but remain within acceptable limits for many real-world applications when appropriately optimized (Preskill, 2023; Liu et al., 2024; Akande, 2025). QKD systems, on the other hand, incur substantial capital and operational costs due to the need for specialized equipment and maintenance. Scalability remains a persistent challenge, as extending QKD beyond point-to-point links often requires trusted relay nodes or quantum repeaters, which are not yet mature technologies (Chen & Tsai, 2025; Kalnina et al., 2025; Kish et al., 2025; Nwaga & Nwagwughiagwu, 2024).

5.4. Hybrid Approaches and Complementarity

Recent research highlights the potential of hybrid security architectures that combine PQC and QKD to leverage the strengths of both approaches. In such systems, QKD can be used to establish symmetric keys with information-theoretic security over limited, high-value links, while PQC secures broader network communication and authentication mechanisms (Zeng et al., 2024; Marchsreiter & Sepúlveda, 2023; Comin, 2025). The Hybrid PQC-QKD models are particularly attractive in environments requiring layered security assurances, such as critical infrastructure or inter-data-center communication (Comin, 2025). However, these architectures introduce additional complexity in system design, key management, and governance, necessitating careful evaluation of cost–benefit trade-offs (Zeng et al., 2024).

5.5. Comparative Summary

Table 7. Summarizes the key differences between PQC and QKD across technical and operational dimensions

Aspect	Post-Quantum Cryptography (PQC)	Quantum Key Distribution (QKD)
Security basis	Computational hardness	Laws of quantum mechanics
Hardware requirements	Classical hardware only	Specialized quantum hardware
Scalability	High	Limited
Deployment cost	Low to moderate	High
Integration with existing systems	High	Limited
Suitability for IoT and mobile	High	Low
Maturity for widespread use	Near-term	Experimental to niche

6. Energy Efficiency of Post-Quantum Cryptography on Constrained Devices

Energy efficiency is a critical determinant of cryptographic feasibility in constrained environments such as Internet of Things (IoT) devices, embedded systems, and mobile platforms (Tasopoulos et al., 2023). Unlike server-class systems, these devices operate under strict limitations in terms of power consumption, memory capacity, and computational resources (Fitzgibbon & Ottaviani, 2024). Consequently, the energy overhead introduced by post-quantum cryptographic algorithms represents a key practical challenge for widespread adoption.

The review indicates that post-quantum schemes generally incur higher computational costs than classical elliptic curve cryptography, primarily due to larger key sizes, more complex arithmetic operations, and increased memory access patterns (Akande, 2025; Azhari & Salsabila, 2024). Among the various families, lattice-based schemes, particularly those based on Module-LWE, demonstrate comparatively favourable energy profiles when implemented with optimized parameters and hardware-aware techniques (Liu et al., 2024; Wang et al., 2023; Cherkaoui Dekkaki et al., 2024). Experimental evaluations on ARM Cortex-M and similar microcontroller platforms

show that key encapsulation and signature operations remain feasible within acceptable energy budgets for mid-range IoT devices (Moura et al., 2023).

Hash-based signature schemes, while offering strong long-term security assurances, tend to exhibit higher energy consumption due to repeated hash computations and larger signature sizes. This makes them less suitable for scenarios involving frequent authentication or real-time communication (Fathalla & Azab, 2024; Noel et al., 2022; Panthi & Bhuyan, 2023). Code-based cryptography, although computationally efficient during encryption and decryption, suffers from large public keys that increase transmission energy costs, which can be prohibitive for low-bandwidth wireless links (Widodo et al., 2024; Sharifov et al., 2021; Bindal & Singh, 2024; Yu, 2024).

The reviewed studies consistently emphasize the importance of implementation-level optimizations, including constant-time arithmetic, memory-efficient data structures, and selective use of hardware acceleration (e.g., Dong et al., 2024; Egbuagha & Ikwunna, 2025; Erol, 2025; Singh, 2025; Brohet et al., 2023). Energy-aware parameter selection and hybrid cryptographic deployments are identified as practical strategies for balancing security requirements with device constraints. Overall, the evidence suggests that energy efficiency is not an inherent barrier to post-quantum cryptography but rather a design consideration that must be addressed through careful algorithm selection and system-level optimization.

7. Socio-Technical and Regulatory Implications

The transition to post-quantum cryptography is not solely a technical endeavour; it is fundamentally socio-technical in nature. Cryptographic systems operate within organizational, legal, and human contexts that shape their effectiveness and sustainability. The literature highlights that successful adoption of post-quantum cryptography requires coordinated action across technical teams, management structures, and regulatory bodies (Campbell, 2025; Erol, 2025; Couzens, 2025).

From a regulatory perspective, data protection frameworks such as the General Data Protection Regulation (GDPR), sector-specific cybersecurity mandates, and national data sovereignty laws increasingly emphasize long-term confidentiality and cryptographic resilience (Toussaint et al., 2024; Oluoha et al., 2023). Organizations responsible for protecting sensitive data may face legal and reputational risks if they fail to anticipate foreseeable cryptographic threats (Tsantikidou & Sklavos, 2024). Several studies argue that proactive migration to quantum-resistant mechanisms aligns with principles of due diligence and risk management embedded in modern compliance regimes (Couzens, 2025; Bishwas & Sen, 2024; Lim & Buselli, 2024).

Human and organizational factors further influence adoption outcomes. The complexity of post-quantum algorithms, coupled with limited practitioner familiarity, introduces risks related to misconfiguration, improper parameter selection, and insecure implementations (Okunola & Litty, 2025; Alessa et al., 2025). Training, documentation, and cryptographic agility are therefore identified as essential enablers of secure deployment. Additionally, procurement decisions, vendor support, and standardization timelines shape the pace and scope of migration efforts (Sangari et al., 2025).

Therefore, these findings reinforce the need to view post-quantum cryptography as an organizational transformation rather than a simple security upgrade. Integrating technical readiness with policy alignment and human capacity building is critical to achieving sustainable quantum-resilient security.

7.1. Adoption Insights

This study presents the strategic role of quantum-safe cryptography in protecting the digital infrastructure of the world. With the ongoing development of quantum computing, the data that used to be considered secure, especially encrypted archives, can be vulnerable to “store-now, decrypt-later” attacks. PQC adoption is therefore

an active security concept that guarantees the confidentiality, integrity, and authenticity of information during the quantum era. Moreover, the combination of the PQC with the blockchain systems, IoT networks, and cloud structures is promising for future work. These findings indicate that PQC-based algorithms are scalable with few trade-offs on efficiency, which makes them suitable to be used in both enterprise and government-scale cybersecurity. These findings confirm that post-quantum cryptography is a practical and relevant defence against new quantum threats. Although PQC algorithms require more computational power than classical algorithms, they provide unprecedented resistance to quantum-based attacks. Lattice-based algorithms in particular offer optimal performance-security trade-offs, and they can be incorporated efficiently and effectively with communication protocols like TLS and VPNs. This research confirms the view that the post-quantum shift must give priority to the use of hybrid cryptography, constant benchmarking, and global standardisation to provide the safety of digital communication during the quantum computing era.

8. Conclusion

8.1. Summary

Quantum computing presents a fundamental challenge to the cryptographic foundations of modern digital systems. This study has reviewed post-quantum cryptographic approaches, synthesizing recent research to assess their security, performance, and readiness for real-world deployment. The findings confirm that post-quantum cryptography offers a viable and scalable path toward quantum-resilient security, particularly when integrated through hybrid and phased migration strategies. By bridging cryptographic theory with operational, energy, and socio-technical considerations, this work contributes a comprehensive framework for understanding and evaluating post-quantum adoption. As quantum technologies continue to advance, early and informed engagement with post-quantum cryptography will be critical to preserving trust, confidentiality, and resilience in future digital data infrastructures.

8.2. Recommendations

According to the findings in this study, the following are some of the main recommendations to researchers, policymakers, and cybersecurity practitioners:

1. Organisations should start adopting a hybrid configuration of PQC schemes with classical schemes. It is a gradual migration mechanism that avoids interfering with existing infrastructure to transition to the fully post-quantum level.
2. Governments and research institutions should aid the development of standardised PQC benchmarking frameworks. These standards will allow comparable evaluation of performance and interoperability, and increase the trust of the world in PQC implementation.
3. The use of quantum-resistant key-exchange, encryption algorithms, and protocols should be prioritised in critical sectors of the economy like banking, healthcare, and national defence. This involves updating firmware, cryptographic libraries, and communication systems as a way of supporting PQC preparations.
4. PQC algorithms require more computational power and memory; thus, more studies are required to find lightweight post-quantum cryptography that can fit the Internet of Things (IoT) and mobile contexts. Such resource-limited devices constitute a major fraction of the new network infrastructure and should not be left exposed.
5. Quantum cryptography and PQC training should be taught as part of cybersecurity education in academic establishments and industry organisations. The creation of awareness among the future professionals will help accelerate the process of more informed accommodation with quantum-safe technologies.
6. Finally, data security is an international issue; International collaboration is needed to standardise PQCs, exchange threat information, and align policy reactions. Governments, research organisations, and the private sector should work together to speed up PQC preparedness on the international level.

8.3. Future Work

Despite the fact that this study reviewed literature on PQC approaches in Data security, several areas still need to be explored.

1. Future studies should examine PQC algorithms' long-term scalability in large-scale networks, their energy efficiency, and their real-time performance in embedded and mobile devices. It is also crucial to conduct more research on developing hybrid authentication protocols and quantum-resistant key management systems.
2. Future studies should also investigate the integration of PQC with blockchain, cloud computing, and edge computing frameworks. These combinations could enhance the security of distributed systems while ensuring scalable quantum resistance across digital ecosystems.
3. The smooth integration of PQC algorithms into new digital ecosystems, including cloud-based architectures, 5G/6G networks, and the Internet of Things (IoT), should be the main emphasis of future research. This entails assessing performance trade-offs in practical implementations and making sure security improvements do not impair energy efficiency, scalability, or latency.
4. To evaluate PQC algorithms' resilience to both classical and quantum attacks, ongoing benchmarking in expansive and diverse settings is also required. For the post-quantum future to have a robust cryptographic environment, innovation, and interoperability, cooperation between government, industry, and academia will be essential.

Authors' Contributions

Conceptualization, O.F.X. and T.H.; methodology, O.F.X.; software, O.F.X.; validation, O.F.X. and T.H.; data curation, O.F.X.; writing-original draft preparation, O.F.X. and T.H.; writing-review and editing, O.F.X., and T.H.; supervision, T.H. Every author has gone through and accepted the final version of the manuscript.

Declaration of Generative AI and AI-Assisted Technologies

During the preparation of this manuscript, the authors used Grammarly to enhance clarity and correct language, and OpenAI tools to improve readability and refine expression. After using these services, the author(s) carefully reviewed and edited the text as necessary and take full responsibility for the content of this publication.

Acknowledgments

The authors thank their respective university institutions that supported them. They also acknowledge the contributions of colleagues and reviewers whose feedback helped improve the quality of this manuscript.

References

[1] Maryam Abbasi et al., "A Practical Performance Benchmark of Post-Quantum Cryptography across Heterogeneous Computing Environments," *Cryptography*, vol. 9, no. 2, pp. 1-27, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mohammad Abudalou, "Enhancing Data Security through Advanced Cryptographic Techniques," *International Journal of Computer Science and Mobile Computing - IJCSMC*, vol. 13, no. 1, pp. 88-92, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] M. AbuGhanem, "IBM Quantum Computers: Evolution, Performance, and Future Directions," *The Journal of Supercomputing*, vol. 81, no. 5, pp. 1-29, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Muhammad AbuGhanem, "Superconducting Quantum Computers: Who is Leading the Future?," *EPJ Quantum Technology*, vol. 12, no. 1, pp. 1-75, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] Temitope Adewale, "Post-Quantum Cryptography Standards: Evaluating Industry Adoption and Implementation Challenges," 2023. [Google Scholar]

[6] Nadeem Ahmed, Lei Zhang, and Aryya Gangopadhyay, "A Survey of Post-Quantum Cryptography Support in Cryptographic Libraries," *2025 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Albuquerque, NM, USA, pp. 906-917, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[7] Ruma Kareem K. Ajeena, "A Proposed Modification of Diffie-Hellman Key Exchange based on Integer Matrices," *International Journal of Mathematics and Computer Science*, vol. 19, no. 1, 211-218, 2024. [Google Scholar] [Publisher Link]

[8] Babatunde Akande, "The Impact of Quantum Computing on Encryption: How Quantum Computers can Break Current Encryption Methods, such as RSA and ECC, and What this Means for Data Security," 2025. [Google Scholar]

[9] Samya Al Busafi, and Basant Kumar, "Review and Analysis of Cryptography Techniques," *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, Moradabad, India, pp. 323-327, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Gorjan Alagic et al., "Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process," *NIST Internal Report: NIST IR 8545*, pp. 1-27, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Gorjan Alagic et al., "Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process," *National Institute of Standards and Technology*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Abdullah Saad Alessa, Mohammad Hammoudeh, and Harbaksh Singh, *A Peek into the Post-Quantum Era-PQA PQC: What will Happen in 2030*, 1st ed., Quantum Technology Applications, Impact, and Future Challenges, pp. 163-180, CRC Press, 2025. [Google Scholar] [Publisher Link]

[13] Nick Aquina et al., "A Critical Analysis of Deployed Use Cases for Quantum Key Distribution and Comparison with Post-Quantum Cryptography," *EPJ Quantum Technology*, vol. 12, no. 1, pp. 1-42, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[14] Nicolas Aragon et al., "BIKE: Bit Flipping Key Encapsulation, *HAL Open Science*, 2022. [Google Scholar] [Publisher Link]

[15] Mohammad Asif, and Sanjay Agal, "A Comprehensive Study on Lattice, Code, and Hash-based Cryptographic Algorithms in Post-Quantum Security with Practical Applications," *IET Conference Proceedings*, vol. 2025, no. 7, pp. 1176-1183, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[16] Rama Azhari, and Agita Nisa Salsabila, "Analyzing the Impact of Quantum Computing on Current Encryption Techniques," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 148-157, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Muhammad Talha Tahir Bajwa et al., "Post-Quantum Cryptography for Big Data Security," *The Asian Bulletin of Big Data Management*, vol. 5, no. 3, pp. 81-94, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Rajkumar Banoth, and Rekha Regar, *Asymmetric Key Cryptography*, Classical and Modern Cryptography for Beginners, Springer, Cham, pp. 109-165, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Freddie Barrett-Danes, and Fahad Ahmad, "Quantum Computing and Cybersecurity: A Rigorous Systematic Review of Emerging Threats, Post-Quantum Solutions, and Research Directions (2019–2024)," *Discover Applied Sciences*, vol. 7, no. 10, pp. 1-20, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] Daniel Chicayban Bastos, and Luis Antonio Brasil Kowada, "How to Detect Whether Shor's Algorithm Succeeds Against Large Integers Without a Quantum Computer," *Procedia Computer Science*, vol. 195, pp. 145-151, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Denis Berger, Mouad Lemoudden, and William J. Buchanan, "Post-Quantum Migration of the Tor Application," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, pp. 1-38, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[22] Hilal Ahmad Bhat et al., "Quantum Computing: Fundamentals, Implementations and Applications," *IEEE Open Journal of Nanotechnology*, vol. 3, pp. 61-77, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Ekta Bindal, and Abhay Kumar Singh, "Secure and Compact: A new Variant of McEliece Cryptosystem," *IEEE Access*, vol. 12, pp. 35586-35596, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Arit Kumar Bishwas, and Mousumi Sen, "Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat," *arXiv Preprint*, pp. 1-30, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Sergey Bravyi et al., "The Future of Quantum Computing with Superconducting Qubits," *Journal of Applied Physics*, vol. 132, no. 16, pp. 1-18, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Marco Brohet, Felipe Valencia, and Francesco Regazzoni, "Instruction Set Extensions for Post-Quantum Cryptography," *2023 IEEE/ACM International Conference on Computer Aided Design (ICCAD)*, San Francisco, CA, USA, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] Robert Campbell, "Enterprise Migration to Post-Quantum Cryptography: Timeline Analysis and Strategic Frameworks," *Computers*, vol. 15, no. 1, pp. 1-23, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[28] Yuan Cao et al., "An Efficient Full Hardware Implementation of Extended Merkle Signature Scheme," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 2, pp. 682-693, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[29] Emily R. Carter et al., "Hybrid Cryptographic Models for Quantum and Classical Interoperability," 2023. [Google Scholar]

[30] Eunmi Chae, Joonhee Choi, and Junki Kim, "An Elementary Review on Basic Principles and Developments of Qubits for Quantum Computing," *Nano Convergence*, vol. 11, no. 1, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[31] Kanza Cherkaoui Dekkaki, Igor Tasic, and Maria-Dolores Cano, "Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process," *Technologies*, vol. 12, no. 12, pp. 1-23, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[32] Gaurab Chhetri et al., "Post-Quantum Cryptography and Quantum-Safe Security: A Comprehensive Survey," *arXiv Preprint*, pp. 1-33, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[33] Mauricio Cisneros, and Javier Olazabal, "Lattice-based Cryptography in the Quantum Era: A Survey," *Interfases*, vol. 18, pp. 281-299, 2023. [Google Scholar]

[34] Christopher Columbus Chinnappan et al., "Quantum Computing: Foundations, Architecture and Applications," *Engineering Reports*, vol. 7, no. 8, pp. 1-27, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[35] Alberto Comin, "Hybrid Quantum Security: Integrating QKD and PQC in Brownfield Optical Networks," *Quantum Information Technologies Journal*, pp. 105-122, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[36] Brian Couzens, "Quantum Risk: A Strategic Framework for PQC Migration and Board Accountability," *SSRN*, pp. 1-78, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[37] Duc-Thuan Dam et al., "A Survey of Post-Quantum Cryptography: Start of a New Race," *Cryptography*, vol. 7, no. 3, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[38] Aisling Dawson, Redefining Public Key Infrastructure (PKI) in the Post-Quantum Era, ABI Research, 2025. [Online]. Available: https://www.abiresearch.com/blog/post-quantum-cryptography-public-key-infrastructure#:~:text=PQC%20is%20destined%20to%20be,legacy%20systems%20remain%20an%20inhibitor

[39] Koen de Boer, and Wessel van Woerden, "Lattice-based Cryptography: A Survey on the Security of the Lattice-based NIST Finalists," *Cryptology ePrint Archive*, pp. 1-125, 2025. [Google Scholar] [Publisher Link]

[40] Jiankuo Dong et al., "Eco-Bike: Bridging the Gap between PQC Bike and GPU Acceleration," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 8952-8965, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[41] Victor Dorojan, "A General Introduction to Shor's Algorithm and its Applications," *SSRN*, pp. 1-4, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[42] Bartosz Drzazga, and Lukasz Krzywiecki, "Review of Chosen Isogeny-based Cryptographic Schemes," *Cryptography*, vol. 6, no. 2, pp. 1-39, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[43] William Chuck Easttom, *Quantum Computing Fundamentals*, Addison-Wesley Professional, 2021. [Google Scholar]

[44] Obianuju Egbuagha, and Emmanuel Ikwunna, "Post-Quantum Cryptography in Practice: A Literature Review of Protocol-Level Transitions and Readiness," *Cryptology ePrint Archive*, pp. 1-40, 2025. [Google Scholar] [Publisher Link]

[45] Daniel J. Egger et al., "Quantum Computing for Finance: State-of-the-Art and Future Prospects," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1-24, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[46] M. Awais Ehsan et al., "Post-Quantum KEMs for IoT: A Study of Kyber and NTRU," *Symmetry*, vol. 17, no. 6, pp. 1-13, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[47] Ahmed Hossam Eid, and A.S. Ismail, "An Analytical Review on Lattice-based Cryptography," *Journal of Physics: Conference Series*, vol. 3075, no. 1, pp. 1-13, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[48] Zion Elani, "Qubit, Quantum Entanglement and All that: Quantum Computing Made Simple," *American Research Journal of Physics*, vol. 7, no. 1, pp. 1-9, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[49] Volkan Erol, "Quantum Readiness in Cryptography: A Maturity-based Framework for Post-Quantum Transition," pp. 1-27, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[50] Efat Fathalla, and Mohamed Azab, "Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-based Signature Schemes, Security, and Optimizations," *IEEE Access*, vol. 12, pp. 175969-175987, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[51] Gregory Fitzgibbon, and Carlo Ottaviani, "Constrained Device Performance Benchmarking with the Implementation of Post-Quantum Cryptography," *Cryptography*, vol. 8, no. 2, pp. 1-17, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[52] Pierre-Alain Fouque et al., "A Closer Look at Falcon," *Cryptology ePrint Archive*, pp. 1-45, 2024. [Google Scholar] [Publisher Link]

[53] Rahoul Ganesh et al., "A Panoramic Survey of the Advanced Encryption Standard: from Architecture to Security Analysis, Key Management, Real-World Applications, and Post-Quantum Challenges," *International Journal of Information Security*, vol. 24, no. 5, pp. 1-45, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[54] Linus Gasser, *Post-Quantum Cryptography*, Trends in Data Protection and Encryption Technologies, Springer, Cham, pp. 47-52, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[55] Amare Geremew, and Atif Mohammad, "Preparing Critical Infrastructure for Post-Quantum Cryptography: Strategies for Transitioning Ahead of Cryptanalytically Relevant Quantum Computing," *International Journal on Engineering, Science and Technology*, vol. 6, no. 4, pp. 338-365, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[56] Hadi Gharavi, Jorge Granjal, and Edmundo Monteiro, "Post-Quantum Blockchain Security for the Internet of Things: Survey and Research Directions," *IEEE Communications Surveys and Tutorials*, vol. 26, no. 3, pp. 1748-1774, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[57] Chris Gilbert, and Mercy Abiola Gilbert, "Investigating the Challenges and Solutions in Cybersecurity using Quantum Computing and Cryptography," *International Research Journal of Advanced Engineering and Science*, vol. 9, no. 4, pp. 291-315, 2024. [Google Scholar] [Publisher Link]

[58] Alexandre Augusto Giron, Ricardo Custódio, and Francisco Rodríguez-Henríquez, "Post-Quantum Hybrid Key Exchange: A Systematic Mapping Study," *Journal of Cryptographic Engineering*, vol. 13, no. 1, pp. 71-88, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[59] Andrew Glassner, "An Introduction to Quantum Computing," *ACM SIGGRAPH 2024 Courses*, pp. 1-65, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[60] Élie Gouzien, and Nicolas Sangouard, "Factoring 2048-Bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory," *Physical Review Letters*, vol. 127, no. 14, pp. 1-20, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[61] Mayank Gupta, and Manisha J. Nene, "Quantum Computing: An Entanglement Measurement," *2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI)*, Buldhana, India, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[62] Dylan Herman et al., "Quantum Computing for Finance," *Nature Reviews Physics*, vol. 5, no. 8, pp. 450-465, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[63] Meng-Leong How, and Sin-Mei Cheah, "Forging the Future: Strategic Approaches to Quantum AI Integration for Industry Transformation," vol. 5, no. 1, pp. 290-323, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[64] Xiaowen Hu et al., "FPTRU: Optimization of NTRU-Prime and TLS Performance Assessment," *Progress in Cryptology - AFRICACRYPT 2025: 16th International Conference on Cryptology in Africa*, Rabat, Morocco, vol. 15651, pp. 216-241, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[65] Yiming Huang et al., "A Pure Hardware Implementation of CRYSTALS-KYBER PQC Algorithm through Resource Reuse," *IEICE Electronics Express*, vol. 17, no. 7, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[66] Maksim Iavich, Tamari Kuchukhidze, and Razvan Bocu, "Post-Quantum Digital Signature: Verkle-based HORST," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, pp. 1-23, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[67] Vipin Jain, "A Review on Different Types of Cryptography Techniques," *ACADEMICIA: An International Multidisciplinary Research Journal*, vol. 11, no. 11, pp. 1087-1094, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[68] A. Jenefa et al., "PQC Secure: Strategies for Defending Against Quantum Threats," *2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS)*, Pudukkottai, India, pp. 1799-1804, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[69] Michael Nsikan John et al., "Lattices in Quantum-ERA Cryptography," *International Journal of Research Publication and Reviews*, vol. 11, no. 4, pp. 2175-2179, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[70] Neha Junagade, Sheetal U. Bhandari, and Rachana Y. Patil, "Comparative Study of Quantum Algorithms: A Comprehensive Analysis," *2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, Pune, India, pp. 1-5, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[71] Francis Kagai et al., "Harvest-Now, Decrypt-Later: A Temporal Cybersecurity Risk in the Quantum Transition," *Telecom*, vol. 6, no. 4, pp. 1-23, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[72] Elina Kalnina et al., "Integration of PQC and QKD: Applications, Challenges and Implementation Frameworks," *Applied Cryptography and Network Security Workshops: ACNS 2025 Satellite Workshops: AIHWS, AIoTS, QSHC, SCI, PrivCrypt, SPIQE, SiMLA, and CIMSS*, Munich, Germany, vol. 15653, pp. 266-284, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[73] Yoshito Kanamori, and Seong-Moo Yoo, "Quantum Computing: Principles and Applications," *Journal of International Technology and Information Management*, vol. 29, no. 2, pp. 43-71, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[74] P. Rajesh Kannan et al., "Advancing Post-Quantum Cryptography: A Hybrid Lattice-Hash Approach," *2025 6th International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, pp. 423-428, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[75] Bikram Khanal et al., "Supercomputing Leverages Quantum Machine Learning and Grover's Algorithm," *The Journal of Supercomputing*, vol. 79, no. 6, pp. 6918-6940, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[76] Sebastian Kish, Josef Pieprzyk, and Seyit Camtepe, *Trends in Quantum Key Distribution (QKD)*, Quantum Technologies: Trends in Quantum Key Distribution (QKD), Springer, Cham, pp. 119-131, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[77] R. Krishnaprabha, "Masked Torsion Point Supersingular Isogeny Diffie-Hellman: A Technique for Preventing Castryck-Decru Attack Against SIDH," *AIP Conference Proceedings*, vol. 3283, no. 1, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[78] Randy Kuang, Maria Perepechaenko, and Michel Barbeau, "A New Quantum-Safe Multivariate Polynomial Public Key Digital Signature Algorithm," *Scientific Reports*, vol. 12, no. 1, pp. 1-21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[79] Mandeep Kumar, and Bhaskar Mondal, "Study on Implementation of Shor's Factorization Algorithm on Quantum Computer," *SN Computer Science*, vol. 5, no. 4, pp. 1-20, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[80] Alvary Kefas Kwala, Shri Kant, and Alpna Mishra, "Comparative Analysis of Lattice-based Cryptographic Schemes for Secure IoT Communications," *Discover Internet of Things*, vol. 4, no. 1, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[81] Younes Lahraoui et al., "Securing Data Exchange with Elliptic Curve Cryptography: A Novel Hash-based Method for Message Mapping and Integrity Assurance," *Cryptography*, vol. 8, no. 2, pp. 1-31, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[82] Atinderpal Singh Lakhan, "*A Comparative Study on Post-Quantum Cryptographic Digital Signature Algorithms: Network Performance, Key Robustness, and Energy Consumption*," Doctoral Dissertation, Carleton University, pp. 1-119, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[83] Tran Duc Le et al., "Are Enterprises Ready for Quantum-Safe Cybersecurity?," *arXiv Preprint*, pp. 1-29, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[84] Kaitlyn Lee, Michael Gowanlock, and Bertr Cambou, "SABER-GPU: A Response-based Cryptography Algorithm for SABER on the GPU," *2021 IEEE 26th Pacific Rim International Symposium on Dependable Computing (PRDC)*, Perth, Australia, pp. 123-132, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[85] Douwei Lei et al., "Faster Implementation of Ideal Lattice-based Cryptography using AVX512," *ACM Transactions on Embedded Computing Systems*, vol. 22, no. 5, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[86] Hoon Wei Lim, and John Busell, "Managing Risks and Opportunities for Quantum Safe Development," *NCS. Pte. Ltd and IBM Quantum, Tech. Rep*, pp. 1-20, 2024. [Google Scholar]

[87] Fengxia Liu et al., "A Survey on Lattice-based Digital Signature," *Cybersecurity*, vol. 7, no. 1, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[88] Jesus Lopez et al., "Evaluating Post-Quantum Cryptographic Algorithms on Resource-Constrained Devices," *2025 IEEE International Conference on Quantum Computing and Engineering (QCE)*, USA, pp. 918-925, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[89] Vadim Lyubashevsky et al., "Crystals-Dilithium," *Algorithm Specifications and Supporting Documentation*, 2020. [Google Scholar]

[90] A. Mahendran, "Design and Simulation of an Energy-Efficient Adaptive Lightweight Post-Quantum Cryptographic Framework for Resource-Constrained IoT Devices," *Research Square*, pp. 1-15, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[91] Aayush Mainali, and Sirjan Ghimire, "A Statistical Side-Channel Risk Model for Timing Variability in Lattice-based Post-Quantum Cryptography," *arXiv Preprint*, pp. 1-21, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[92] Surajit Mandal et al., "Implementing Grover's on AES-based AEAD Schemes," *Scientific Reports*, vol. 14, no. 1, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[93] Dominik Marchsreiter, and Johanna Sepúlveda, "A PQC and QKD Hybridization for Quantum-Secure Communications," *2023 26th Euromicro Conference on Digital System Design (DSD)*, Golem, Albania, pp. 545-552, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[94] Jillian Mascelli, and Megan Rodden, "Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks," *SSRN*, pp. 1-21, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[95] Catherine C. McGeoch et al., "A Comment on Comparing Optimization on D-Wave and IBM Quantum Processors," *arXiv Preprint*, pp. 1-5, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[96] Qurban A. Memon, Mahmoud Al Ahmad, and Michael Pecht, "Quantum Computing: Navigating the Future of Computation, Challenges, and Technological Breakthroughs," *Quantum Reports*, vol. 6, no. 4, pp. 627-663, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[97] Sweta Mishra, Bhaskar Mondal, and Rishi Kumar Jha, "A Survey on Isogeny-based Cryptographic Protocols," *Wireless Networks*, vol. 31, no. 3, pp. 2993-3024, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[98] Dustin Moody et al., "Transition to Post-Quantum Cryptography Standards," *NIST Internal or Interagency Report (NISTIR) 8547 (Draft). National Institute of Standards and Technology*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[99] Nicolas Moura et al., "Assessment of Lightweight Cryptography Algorithms on ARM Cortex-M Processors," *2023 36th SBC/SBMicro/IEEE/ACM Symposium on Integrated Circuits and Systems Design (SBCCI)*, Rio de Janeiro, Brazil, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[100] G. Nagarajan, R. Madan Gopi, and R. Sanjai, "Role of Hash-based Signatures in Quantum Cryptography," *AIP Conference Proceedings*, vol. 3075, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[101] What is Post-Quantum Cryptography?, National Institute of Standards and Technology (NIST), 2025. [Online]. Available: https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

[102] National Institute of Standards and Technology, Post-Quantum Cryptography, Information Technology Laboratory, CSRC, 2026. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[103] National Institute of Standards and Technology, Post-Quantum Cryptography, Information Technology, 2026. [Online]. Available: https://www.nist.gov/pqc

[104] Moses Dogonyaro Noel et al., "Review and Analysis of Classical Algorithms and Hash-based Post-Quantum Algorithm," *Journal of Reliable Intelligent Environments*, vol. 8, no. 4, pp. 397-414, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[105] Philip Chidozie Nwaga, and Stephen Nwagwughiagwu, "Exploring the Significance of Quantum Cryptography in Future Network Security Protocols," *World Journal of Advanced Research and Reviews*, vol. 24, no. 3, pp. 817-833, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[106] Abiodun Okunola, and Abey Litty, "The Human Factor in Quantum-Safe Cryptography Adoption: Assessing user Perceptions and Training Needs within Enterprise Environments," *SSRN*, pp. 1-13, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[107] Abiodun Olaluwe et al., "Machine Learning and Side-Channel Attacks on Post-Quantum Cryptography," *Cryptology ePrint Archive*, pp. 1-31, 2025. [Google Scholar] [Publisher Link]

[108] Godwin Olaoye, "Quantum Cryptanalysis: Breaking Classical Encryption with Shor's and Grover's Algorithms," *Authorea*, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[109] Oluchukwu Modesta Oluoha et al., "A Privacy-First Framework for Data Protection and Compliance Assurance in Digital Ecosystems," *Iconic Research and Engineering Journals*, vol. 7, no. 4, pp. 620-646, 2023. [Google Scholar] [Publisher Link]

[110] Anthony Owen, and Davids Pearson, "*Investigate Quantum-Resistant Cryptography and Secure Communication Protocols*," IU International University of Applied Science, Erfurt, Germany, pp. 1-37, 2025. [Google Scholar]

[111] Rajiv Pandey et al., *Quantum Computing: A Shift from Bits to Qubits*, 1st ed., Springer Singapore, vol. 1085, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[112] Swarna Panthi, and Bubu Bhuyan, "Quantum-Resistant Hash-based Digital Signature Schemes: A Review," *Proceedings of 4th International Conference on Frontiers in Computing and Systems: COMSYS*, Goa, India, vol. 974, pp. 637-655, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[113] Raj Parikh, and Khushi Parikh, "Survey on Hardware Security: PUFs, Trojans, and Side-Channel Attacks," *Preprints.org*, pp. 1-11, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[114] Sahib J. Parmar et al., "Quantum Computing: Exploring Superposition and Entanglement for Cutting-Edge Applications," *2023 16th International Conference on Security of Information and Networks (SIN)*, Jaipur, India, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[115] J. Cameron Patterson, William J. Buchanan, and Callum Turino, "Energy Consumption Framework and Analysis of Post-Quantum Key-Generation on Embedded Devices," *Journal of Cybersecurity and Privacy*, vol. 5, no. 3, pp. 1-25, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[116] Ray Perlner, John Kelsey, and David Cooper, "Breaking Category Five SPHINCS+ with SHA-256," *Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022, Virtual Event*, Springer, Cham, vol. 13512, pp. 501-522, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[117] Tetiana Portovaras et al., "Ensuring Confidentiality and Data Security in Economic Analysis of Business Entities: Challenges and Solutions," *Multidisciplinary Reviews*, vol. 7, no. 10, pp. 1-8, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[118] Sunil Prajapat et al., "Secure Lattice-based Signature Scheme for Internet of Things Applications," *IEEE Access*, vol. 13, pp. 75985-75999, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[119] John Preskill, *Quantum Computing 40 Years Later*, 2nd ed., Feynman Lectures on Computation, CRC Press, pp. 193-244, 2023. [Google Scholar] [Publisher Link]

[120] Tomas Preucil, Petr Socha, and Martin Novotny, "Implementation of the Rainbow Signature Scheme on SoC FPGA," *2022 25th Euromicro Conference on Digital System Design (DSD)*, Maspalomas, Spain, pp. 513-519, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[121] Mohamad Sadegh Sangari, Michael Lee, and Atefeh Mashatan, "Towards Quantum Threat Mitigation: An Empirical Investigation of the Factors Influencing Organizational Preparation Intentions," *Cybersecurity and Privacy*, 2025. [Google Scholar] [Publisher Link]

[122] Hwajeong Seo et al., "Supersingular Isogeny key Encapsulation (SIKE) Round 2 on ARM Cortex-M4," *IEEE Transactions on Computers*, vol. 70, no. 10, pp. 1705-1718, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[123] Ami M. Shah, and Ashishkumar Gor, "Comprehensive Survey of Symmetric and Public-Key Cryptographic Algorithms: Foundations, Attacks, and Applications," *International Journal of Informative & Futuristic Research (IJIFR)*, vol. 12, no. 10, pp. 20-39, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[124] Parviz Sharifov et al., "Post-Quantum Cryptosystem of Niederreiter, Algorithm and Encryption Scheme: Modification and Optimization," *XIV International Scientific Conference "INTERAGROMASH 2021"*, pp. 173-183, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[125] Shiang-Jiun Chen, and Yi-Hsueh Tsai, "Quantum-Safe Networks for 6G: An Integrated Survey on PQC, QKD, and Satellite QKD with Future Perspectives," *Computing&AI Connect*, vol. 2, no. 1, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[126] Nitin Kumar Shingari, and Beenu Mago, "The Importance of Data Encryption in Ensuring the Confidentiality and Security of Financial Records of Medical Health," *2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, Gwalior, India, pp. 1-6, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[127] Harbaksh Singh, *Managing the Quantum Cybersecurity Threat: Harvest Now, Decrypt Later*, Quantum Computing, CRC Press, 1st ed., pp. 142-158, 2024. [Google Scholar] [Publisher Link]

[128] Manmohan Singh, Sandeep Kumar Sood, and Munish Bhatia, "Post-Quantum Cryptography: A Review on Cryptographic Solutions for the Era of Quantum Computing," *Archives of Computational Methods in Engineering*, pp. 1-42, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[129] Nehal Narendra Singh, "Post-Quantum Cryptography-Safe Network Architectures: Design Frameworks and Implementation Strategies for Enterprise Zero-Trust Environments," *Sarcouncil Journal of Engineering and Computer Sciences*, vol. 4, no. 8, pp. 807-820, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[130] Pawandeep Singh et al., "*Understanding RSA Algorithm in Cryptography*," Thesis, University of Jammu, 2024. [Google Scholar]

[131] Gyeongju Song, and Hwajeong Seo, "Grover on Scrypt," *Electronics*, vol. 13, no. 16, pp. 1-12, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[132] Deepraj Soni et al., *Hardware Architectures for Post-Quantum Digital Signature Schemes*, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[133] Mostefa Kara et al., "A Post-Quantum Public-Key Signcryption Scheme over Scalar Integers based on a Modified LWE Structure," *Sensors*, vol. 25, no. 15, pp. 1-17, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[134] Jakub Sowa et al., "Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways," *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Montreal, QC, Canada, pp. 1835-1846, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[135] Vikas Srivastava, Anubhab Baksi, and Sumit Kumar Debnath, "An Overview of Hash based Signatures," *Cryptology ePrint Archive*, 2023. [Google Scholar] [Publisher Link]

[136] Tudor D. Stanescu, *Introduction to Topological Quantum Matter & Quantum Computation*, CRC Press, 2nd ed., Boca Raton, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[137] Purvi Tandel, and Jitendra Nasriwala, "Secure Authentication Framework for IoT Applications using a Hash-based Post-Quantum Signature Scheme," *Service Oriented Computing and Applications*, vol. 19, no. 3, pp. 251-262, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[138] Monther Tarawneh, *Perspective Chapter: Cryptography–Recent Advances and Research Perspectives*, Biometrics and Cryptography, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[139] George Tasopoulos et al., "Energy Consumption Evaluation of Post-Quantum TLS 1.3 for Resource-Constrained Embedded Devices," *Proceedings of the 20th ACM International Conference on Computing Frontiers*, pp. 366-374, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[140] P. Thanalakshmi et al., "A Quantum-Resistant Blockchain System: A Comparative Analysis," *Mathematics*, vol. 11, no. 18, pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[141] Joshua J. Tom et al., "Quantum Computers and Algorithms: A Threat to Classical Cryptographic Systems," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 12, no. 5, pp. 25-38, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[142] Marion Toussaint, Sylvère Krima, and Hervé Panetto, "Industry 4.0 Data Security: A Cybersecurity Frameworks Review," *Journal of Industrial Information Integration*, vol. 39, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[143] Søren Toxvaerd, "Simulating Physics with Computers," *arXiv Preprint*, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[144] Kyriaki Tsantikidou, and Nicolas Sklavos, "Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures," *Cryptography*, vol. 8, no. 1, pp. 1-24, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[145] Samet Ünsal, "A Comparative Performance Evaluation of Kyber, sntrup761, and FrodoKEM for Post-Quantum Cryptography," *arXiv Preprint*, pp. 1-5, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[146] Athanasios – Valavanidis, "Quantum Computin:. A Revolutionary Computing Capability to Sift through Huge Numbers of Possibilities and Extract Potential Solutions to Complex Problems," vol. 1, pp. 1-25, 2024. [Google Scholar]

[147] Lakkavaram S. M. Shriya Varnita et al., "A Study on Isogeny based Cryptography," *2024 International Conference on Electronics, Computing, Communication and Control Technology (ICECCC)*, Bengaluru, India, pp. 1-6, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[148] Kendre Saraswati Vasantrao, and Amit Saxena, "Bits to Qubits: An Overview of Quantum Computing," *2025 International Conference on Intelligent Control, Computing and Communications (IC3)*, Mathura, India, pp. 120-124, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[149] Anyu Wang, Dianyan Xiao, and Yang Yu, "Lattice-based Cryptosystems in Standardisation Processes: A Survey," *IET Information Security*, vol. 17, no. 2, pp. 227-243, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[150] Chao Wang et al., "A First Successful Factorization of RSA-2048 Integer by D-Wave Quantum Computer," *Tsinghua Science and Technology*, vol. 30, no. 3, pp. 1270-1282, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[151] Xiaoyun Wang, Guangwu Xu, and Yang Yu, "Lattice-based Cryptography: A Survey," *Chinese Annals of Mathematics, Series B*, vol. 44, no. 6, pp. 945-960, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[152] Agung Mulyo Widodo et al., "Quantum-Resistant Cryptography," *Innovations in Modern Cryptography*, pp. 101-132, 2024. [Google Scholar]

[153] Hiu Yung Wong, *Introduction to Quantum Computing: from a Layperson to a Programmer in 30 Steps*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[154] Faguo Wu et al., "Quantum-Resistant Blockchain and Performance Analysis," *The Journal of Supercomputing*, vol. 81, no. 3, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[155] Zebo Yang, Maede Zolanvari, and Raj Jain, "A Survey of Important Issues in Quantum Computing and Communications," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1059-1094, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[156] Zhouke Yu, "Research on Cryptography based on Quantum-Resistant Algorithms," *2024 International Conference on Electronics and Devices, Computational Science (ICEDCS)*, Marseille, France, pp. 149-154, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[157] Pei Zeng et al., "Practical Hybrid PQC-QKD Protocols with Enhanced Security and Performance," *arXiv Preprint*, pp. 1-12, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[158] Amirul Asyraf Zhahir et al., "Quantum Computing in the Cloud-A Systematic Literature Review," *International Journal of Electrical and Computer Engineering Systems*, vol. 15, no. 2, pp. 185-200, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[159] Xiaokang Zhou et al., "Edge-Enabled Two-Stage Scheduling based on Deep Reinforcement Learning for Internet of Everything," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3295-3304, 2022. [CrossRef] [Google Scholar] [Publisher Link]