JOURNAL OF POST-QUANTUM CRYPTOGRAPHY AND SYSTEMS

RESEARCH ARTICLE

Volume 01, Issue 02, 2026

Quantum-Resistant Cryptographic Systems: A Comprehensive Review of Lattice-Based, Code-Based, Hash-Based, and Multivariate Approaches

Hamed Taherdoost

College of Technology and Engineering, Westcliff University, Irvine, CA 92614, USA

ABSTRACT

The rapid advancement of quantum computing poses a significant threat to conventional public-key cryptographic systems, necessitating the development of cryptographic solutions capable of resisting quantum-enabled attacks. This review provides a comprehensive analysis of four major families of post-quantum cryptography: lattice-based, code-based, hash-based, and multivariate approaches. The review synthesizes recent literature to examine their mathematical foundations, security assumptions, computational performance, implementation characteristics, and standardization progress. A structured narrative methodology was adopted to evaluate peer-reviewed studies and official reports, enabling a comparative assessment of the strengths and limitations of each cryptographic family. The analysis indicates that lattice-based cryptography currently demonstrates the highest level of practical maturity, supported by NIST standardization of CRYSTALS-Kyber and CRYSTALS-Dilithium, while code-based cryptography continues to provide exceptional long-term security despite larger key sizes. Hash-based schemes offer highly secure digital signatures, whereas multivariate cryptography remains a promising yet evolving alternative requiring further cryptanalytic evaluation. The review also highlights emerging trends, including hybrid cryptographic architectures, lightweight implementations for resource-constrained devices, hardware acceleration, and secure migration strategies for quantum-safe infrastructures. Overall, this study provides a consolidated perspective on the current state of quantum-resistant cryptography, identifies critical research challenges, and outlines future directions that support the development and global adoption of secure, scalable, and resilient post-quantum communication systems.

Keywords: Post-quantum cryptography, Quantum-resistant cryptography, Lattice-based cryptography, Code-based cryptography, NIST standardization

1. Introduction

The market is rapidly changing with quantum computing altering the course of cybersecurity, and, in particular, the security assumptions of public-key cryptographic systems. Various algorithms are widely used, including the RSA, Diffie–Hellman and Elliptic Curve Cryptography (ECC) algorithms based on integer factorization and discrete logarithm problems that are believed to be secure against classical computers. However, quantum algorithms, especially Shor's algorithm, have been shown to be able to solve these problems efficiently, making digital communications more vulnerable to compromise in terms of their confidentiality, integrity and authenticity (Sharath et al., 2025; Tom et al., 2023). With advances in quantum computing technology, the development of cryptographic techniques that can withstand attacks with quantum computers is becoming increasingly important.

Post-quantum cryptography (PQC) or quantum-resistant cryptography (QR) has become the most promising approach to encrypting digital infrastructures in the quantum era. PQC does not depend on quantum devices or platforms to be deployed in the current communication networks and computing systems. Most current research is directed toward cryptographic designs which are based on problems which are thought to be computationally intractable even on quantum computers. Of these, lattice-based, code-based, hash-based and multivariate cryptographic methods have garnered extensive interest in their robust security underpinnings and potential for practical application (Dam et al., 2023; Sood, 2024). Additionally, the National Institute of Standards and Technology (NIST) has been speeding up the standardization process of some post-quantum algorithms, urging governments and industries to get ready for a mass migration of cryptographic algorithms (Sharath et al., 2025).

While significant progress has been made, the landscape of PQC is still diverse and evolving and evaluating the virtues and drawbacks of the various algorithm families will be difficult. In the past, the existing reviews have focused on cryptographic schemes and been lacking in comparative analysis in terms of security assumption, computational efficiency, implementation complexity, and deployment readiness (Gyasi-Nyarko et al., 2025). Hence, this review critically analyses the four main families of lattice-based, code-based, hash-based and multivariate cryptographic systems. This review summarizes state-of-the-art advances and techniques that have been developed and compares them based on their security and performance, standards status, and application potential, highlighting obstacles and outlining promising avenues for future research in the field of providing secure communication in the post-quantum era.

Objectives

1. To review the fundamental principles and recent advances in quantum-resistant cryptographic systems.
2. To compare lattice-based, code-based, hash-based, and multivariate approaches in terms of security and performance.
3. To identify key challenges, emerging trends, and future research directions in PQC.

2. Review Methodology

This comprehensive review adopted a structured narrative approach to synthesize recent advances in quantum-resistant

cryptographic systems. Relevant literature published between 2016 and 2026 was retrieved from ACM Digital Library, SpringerLink, ScienceDirect, Scopus, Web of Science, and official NIST PQC documentation using predefined keywords related to PQC. Peer-reviewed studies addressing lattice-based, code-based, hash-based, and multivariate cryptographic approaches were included, while irrelevant or duplicate records were excluded. The selected publications were critically analyzed and thematically synthesized based on security foundations, computational performance, implementation characteristics, standardization status, practical applications, and emerging research challenges.

3.1 Fundamentals of Quantum-Resistant Cryptography

Given the fast pace at which quantum computers are developing, Quantum-resistant cryptography, known as PQC, is one of the most pressing areas of research. Traditional public-key cryptographic methods, such as RSA, Diffie–Hellman and Elliptic Curve Cryptography (ECC), use problems like integer factorization and the discrete logarithm problem which are hard to solve on a classical computer. The development of quantum algorithms, however, shows that these problems can be solved efficiently on a sufficiently powerful quantum computer, and this poses a threat to the security of existing digital communication systems (Mohammed, 2018; Mattsson et al., 2021). It is imperative to devise cryptographic protocols that can withstand attacks from classical and quantum adversaries and be compatible with existing communication systems.

To overcome this, PQC has been developed using alternative mathematical principles which are thought to be unbreakable even in the age of quantum computers. Examples are lattice-based problems, decoding of error-correcting codes, cryptographic hash functions, and multivariate polynomial equations for different foundations of secure encryption, digital signatures and key exchange protocols. The strength of these methods relies on solid computational hardness assumptions which have been difficult for several decades to be difficult to be broken by deep cryptanalytical research (Bandeira et al., 2019; Jenefa et al., 2023). Furthermore, the modern PQC algorithms are tested with strict security models, such as adoptive chosen-ciphertext and adaptive chosen-message attacks, which encompass both theoretical and practical security needs in quantum settings.

As quantum-resistant cryptography becomes more significant, there have been several efforts around the world to develop safe and efficient algorithms to be widely adopted, especially under the guidance of the National Institute of Standards and Technology (NIST). Beyond mathematical security, the focus of the current research is on efficiency of implementation, scalability, interoperability and resistance to new attack vectors, such as quantum machine learning and mixed cyber-attacks (Debus et al., 2025). With governments, industries, and other critical infrastructure companies gearing up for the future, quantum-resistant cryptography is now the foundation of ensuring the security of sensitive data in the post-quantum world, where computational power is constantly increasing.

3.2 Lattice-Based Cryptography

A lattice-based cryptography is widely accepted as the paradigm in PQC due to its high computational efficiency, quantum resistance, and its strong mathematical foundations. Conventional public-key cryptosystems are based on integer factorization or discrete logarithms, while lattice-based schemes are based on hard lattice problems like the Shortest Vector Problem (SVP), Closest Vector Problem (CVP), and Learning with Errors (LWE), for which there is no known quantum algorithm that is efficient (Micciancio, 2025; Wang et al., 2023). Such hardness assumptions have been implemented to build practical

encryption, digital signature, and key encapsulation schemes for cloud computing, Internet of Things (IoT), blockchain and secure communication applications.

The security basis for many current post-quantum cryptographic algorithms is a breakthrough in lattice-based cryptography: Learning With Errors (LWE) problem. LWE adds controlled random errors to linear algebraic equations, and even in the quantum computational domain, it is hard to recover the secret keys. Ring-LWE and Module-LWE were then invented for making computation more efficient and reducing the storage space required. Ring-LWE takes advantage of the nature of polynomial rings to speed up the arithmetic calculation and compact key representation, while Module-LWE offers a compromise which avoids too much reliance on highly structured algebraic rings. However, leakage-resilient variants of LWE have been studied recently as alternative variants, which are robust against practical side channel attacks and quantum resistant (Lai et al., 2025; Wang & Wang, 2019).

NTRU is one of the earliest and most efficient lattice-based schemes that are quantum resistant. The great advantage it has is that its polynomial-based lattice construction allows for quicker encryption and decryption, and it also has relatively small key sizes, which makes it ideal for resource-limited environments (Nisha et al., 2024). On this mathematical foundation, the CRYSTALS family is considered as the standard for the latest PQC. CRYSTALS-Kyber is a Module-LWE based key encapsulation mechanism, which is also considered as national standard for post-quantum key establishment and public-key encryption by NIST, which has selected it as the standard (Avanzi et al., 2019). Likewise, CRYSTALS-Dilithium uses Module-LWE and Module-SIS assumptions to create digital signatures that are resistant to known quantum attacks (Ducas et al., 2018), easy to implement and efficient. A more well-known signature scheme based on lattices is Falcon, which is based on NTRU lattices and fast Fourier sampling in order to produce signatures of reduced size and efficient verification which make it very attractive if the amount of communication required when verifying a signature is significant.

However, there are some practical problems with lattice-based cryptography. The public keys, ciphertexts and signatures tend to be larger in conventional cryptographic systems, which requires more communication and storage space. Also, secure implementations should counter side-channel attacks, timing attacks and implementation-specific vulnerabilities via constant-time algorithms and hardware-level protections. Despite this, they have been extensively cryptanalysed and kept proving secure, and their benefits in terms of strong theoretical guarantees, practical efficiency, scalability, and standardization efforts have made them the most developed and widely adopted family of quantum-resistant cryptographic algorithms for next-generation secure communication systems (Micciancio, 2025; Wang et al., 2023). Figure 1 Taxonomy of Major Quantum-Resistant Cryptographic Families.

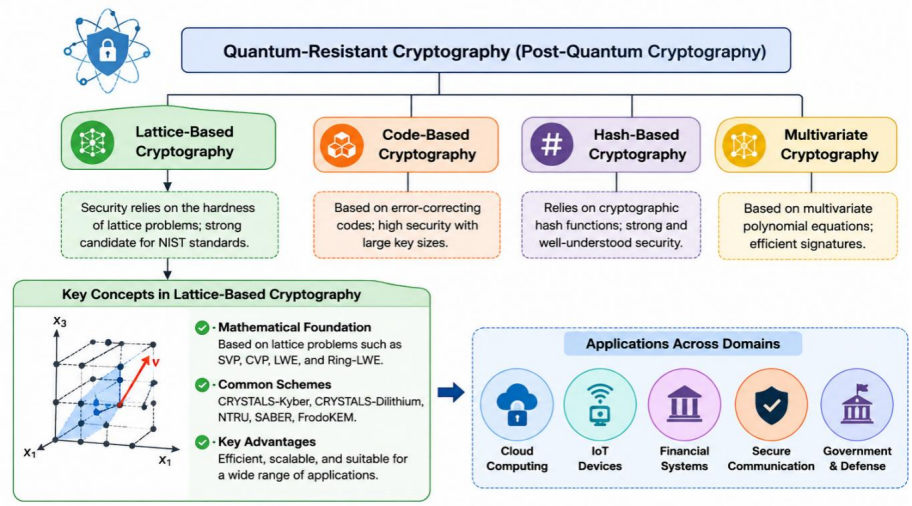

Figure 1. Overview of Quantum-Resistant Cryptographic Families with Emphasis on Lattice-Based Cryptography

3.3 Code-Based Cryptography

One of the earliest and most widely studied methods in PQC, code-based cryptography provides robust security guarantees and is based on the hardness of decoding random linear error-correcting codes. Code-based cryptographic systems were introduced by Robert McEliece in 1978 and have been secure against classical and quantum cryptanalysis for decades and are one of the most promising candidates to be quantum secure. Their security is based on the syndrome decoding problem that is known to be NP-hard and is still not efficiently solvable even with the aid of quantum computers (Gaborit & Deneuville, 2021; Singh, 2019). However, due to their well-founded theory and demonstrated robustness, code-based schemes have emerged as leading contenders for the National Institute of Standards and Technology (NIST) PQC standardization process.

The problem of decoding the syndrome is the mathematical cornerstone of code-based cryptography, in which the reconstruction of an original error vector from a known syndrome arising from a linear error-correcting code is the focus. It can be easily solved if the code is specially structured with a secret algorithm for decoding but is difficult if the code is a random sequence of numbers, such as the code used in a public key cryptographic system. This problem has been demonstrated to be a very strong one for centuries, since it has resisted both classical and quantum attacks, and is believed to remain secure for the foreseeable future (Feneuil et al., 2023; Gaborit & Deneuville, 2021). Hence the assumption that the syndrome can be decoded remains the major hardness assumption for most of the modern constructions in code-based cryptography.

In the code-based cryptography arena, Classic McEliece is the most well-developed and analyzed encryption scheme. It uses the binary Goppa code to provide a very high level of security, while also being efficient in the encryption and decryption process. The major drawback is its large public key size, which can significantly increase storage and communication costs as compared to the lattice-based alternatives. However, the algorithm has shown an incredible cryptanalytic strength for more than 40 years and is one of the most trusted post quantum cryptographic algorithms (Singh, 2019). Other modern developments are BIKE (Bit Flipping Key Encapsulation) and HQC (Hamming Quasi-Cyclic), which are based on quasi-

cyclic code constructions to achieve very small public keys used in this context with still high security. The goal of these schemes is to enhance the efficiency of communication and the computation required without sacrificing the resistance to quantum attacks and such schemes are appealing for their practical applications in the modern communication schemes (Avanzi et al., 2019).

As for performance, code-based cryptographic systems offer quick encryption and decryption processes, strong security assurance, and superior resistance to quantum attackers. The main issue that still stands in their way is the relatively large size of public key, but research is still going on to develop small constructions of codes and optimized implementations for cloud computing, Internet of Things (IoT) and distributed network (Dickinson et al., 2018). In summary, code-based cryptography is one of the most trusted and practical families of quantum resistant cryptographic systems for securing future digital infrastructures, thanks to its long-standing record of security, rigorous mathematical bases and continuous algorithmic improvements (Gaborit & Deneuville, 2021; Singh, 2019).

3.4 Hash-Based Cryptography

One of the most well-established and theoretically strong approaches to quantum-resistant cryptography is based on the security of cryptographic hash functions, which are simpler in structure than the algebraic ones. These schemes rely on the preimage, second preimage and collision resistance properties of hash functions, which makes them very secure both to classical and quantum attacks, with Grover's algorithm reducing security only quadratically which can be overcome by increasing the length of the hash function. Therefore, hash-based cryptographic schemes are a promising option to achieve the long-term security and cryptographic strength for the digital signature application (Asif & Agal, 2025; Li et al., 2022). They have some relatively simple mathematical underpinning, which also makes it easy to conduct formal security analysis and implementation in different computing environments.

The first hash-based signature schemes were one-time signature (OTS) schemes, such as the Lamport and the Winternitz signatures, which are secure but can only be used once per key pair. This was solved by hierarchical tree-based structures which can generate multiple signatures from a single public key securely. There are two noteworthy stateful schemes: the eXtended Merkle Signature Scheme (XMSS) and the Leighton–Micali Signature (LMS), which both contain many one-time keys in Merkle hash trees to provide secure and efficient authentication. These schemes are provably secure and have been standardized for schemes that need high assurance but do need careful state management to avoid unplanned reuse of keys that would break the security (Li et al., 2022).

To remove the state management issues of the operational system, researchers designed SPHINCS+ (Stateless hash-based signature scheme), a stateless hash-based signature system which is a combination of hypertrees, few-time signatures, and randomized hash constructions that provides good security without having to store signing state. SPHINCS+ is highly resistant to quantum attack, and is easy to deploy in distributed systems, cloud systems, and large-scale systems where reliable state synchronization is challenging. It is generally larger than stateful alternatives in terms of size of its signatures and its computational requirements, but its flexibility and simplicity of implementation have made it one of the most prominent digital signature schemes which are not based on a quantum computer (Bernstein et al., 2019).

Choosing between stateful and stateless hash-based signatures is a trade-off between security effectiveness and complexity of

operation. Stateful schemes like XMSS and LMS can be computed cheaper and produce shorter signatures but necessitate secure tracking of the state throughout scheme operations. Stateless schemes, however, like SPHINCS+ do not have the disadvantage of the state-management risks and come with the tradeoffs of larger signatures and greater computational cost (Cohen et al., 2021). Overall, hash-based cryptography offers a very high level of security and has strong theoretical guarantees and will be quantum resistant in the long haul. While some applications might be restricted by their size and the time to sign, their size and signing time are still being optimized for their applicability in resource constrained environments, Internet of Things (IoT) devices and critical digital infrastructures that demand durable post-quantum authentication (Kane et al., 2020; Asif & Agal, 2025).

3.5 Multivariate Cryptography

Multivariate cryptography is one of the most popular post-quantum cryptographic systems whose security depends on the computational hardness of solving a system of multivariate quadratic (MQ) equations over finite fields. The MQ problem is an NP-hard problem and is unfeasible by classical and quantum computing. Therefore, it has been proposed as a basis for quantum-resistant digital signature schemes. Unlike lattice-based and code-based cryptography, multivariate cryptography is mostly used for authentication due to its efficiency in generating and verifying signatures and has small size signatures and high computing speed. These qualities have made them the focus of much research for use in applications that demand fast authentication, embedded systems and resource-constrained environments (Ding et al., 2020; Joux & Mora, 2025).

Infeasibility of solving large systems of nonlinear quadratic equations without knowledge of a secret trapdoor transformation is the foundation of the security of multivariate cryptographic schemes. This mathematical basis can be used to build digital signature algorithms that have efficient signing and verification processes. One of the more prominent schemes is Unbalanced Oil and Vinegar (UOV) which uses layered quadratic polynomial structures to create secure signatures and Rainbow. UOV proposes an asymmetric configuration of oil and vinegar variables that provides better resistance to direct algebraic attacks and remains efficient in computation. Rainbow enhances this idea by adding several layers of variables to flexibly and effectively improve the signature performance, which is one of the most thoroughly studied multivariate signature schemes (Ding et al., 2020).

Over the last few years, multivariate cryptographic algorithms have proven to be very effective but have also been the subject of numerous cryptanalytic attacks. In the last few years, the algebraic approach in cryptanalysis has shed light on the structural flaws of several multivariate schemes, such as the well-known Rainbow scheme.In recent years, several multivariate schemes, especially Rainbow, were broken to a significant extent by the advances of algebraic cryptanalysis. With the use of new analysis methods, it has been shown that some secret algebraic methods can be used to extract private keys more efficiently than was thought, and this is why Rainbow no longer participates in the NIST PQC standardization process. Likewise, ongoing tests of UOV will explore its resistance to increasingly powerful cryptanalytic attacks and suggest modifications to make UOV more secure in the long run (Beullens, 2021).

Research efforts are concentrated on strengthening the robustness of multivariate cryptography by designing new constructions of polynomials, new security proofs and defense against the new attack models. Machine learning has created new possibilities in cryptanalysis, enabling the detection of hidden structure and optimization of algebraic attacks, thus

necessitating constant security evaluation of multivariate schemes (Singh et al., 2024). Although the use of multivariate cryptography is not as widespread as lattice-based cryptography yet, it still offers insights into other approaches to quantum-resistant security. With continuous algorithmic advancements and its efficient signature generation and outputs, it continues to be a significant field of research in the wider realm of post-quantum cryptographic solutions, especially in sectors where lightweight and high-speed digital authentication is paramount.

3.6 Comparative Analysis of Quantum-Resistant Cryptographic Families

The four major lattices based, code based, hash based and multivariate families of PQC have different properties in terms of security, computational complexity, implementation efficiency and deployability. They all withstand quantum attacks, but they differ significantly in the size of their key, the size of their signature, the amount of overhead for communication, how much memory they need, and their practical scalability. Comparative assessment of these attributes is of paramount importance to identify suitable cryptographic schemes for various application areas such as the Internet of Things (IoT), financial systems, critical infrastructure, etc. In addition, the continuous work being done in standardisation by the National Institute of Standards and Technology (NIST) offers useful reference points to evaluate the maturity and viability of those cryptographic families (Bansod & Ragha, 2022; Yesina et al., 2022).

Lattice-based and code-based cryptographic systems offer the highest level of security in the face of quantum attackers due to the security that can be provided by the mathematics of the problems they are designed to solve. Furthermore, hash-based cryptography is extremely secure, using well known cryptographic hash functions, whereas multivariate cryptography has been secure after the success of attacks on several proposed schemes. Computationally, lattice-based algorithms offer a nice balance between security and complexity of computation, and code-based schemes tend to have longer public keys, with efficient encryption and decryption. Generally, hash-based signatures are more costly in terms of computation to generate while multivariate schemes are faster in the signature operation but need continuous reassessment of security (Mohammed, 2018; Pronika & Tyagi, 2021).

Another factor that makes a difference is the size of the key and the size of the signature. Lattice based algorithms are moderately sized keys with relatively small-sized ciphertexts and signatures that are practical for deployment. Contrastively, although code-based cryptography is usually efficient to execute, it typically has much longer public keys. The signatures produced by hash-based cryptography are comparatively large, especially in stateless constructions like SPHINCS+, while the multivariate cryptography may require a larger public key, but has a much smaller signature. These features directly affect the overhead in communication and storage efficiency in bandwidth-constrained environments (Siu et al., 2018; Bansod & Ragha, 2022).

For implementation performance, lattice-based cryptography offers great scalability and is efficient in encryption, decryption and key encapsulation operations, which is ideal for cloud services, blockchain and IoT applications. The code-based schemes make an efficient job of providing high reliability, however there are deployment challenges due to their key storage requirements. Hash-based algorithms are well suited for long-term digital signatures, where security is paramount and faster execution is not so critical, while multivariate cryptography is appealing for light-weight authentication due to its quick

signature generation. Today's NIST standardization results also reiterate the practical maturity of lattice-based cryptography, as the lattice-based digital signature algorithms (DSA) CRYSTALS-Kyber and CRYSTALS-Dilithium are selected, and the hash-based DSA SPHINCS+ is approved as a standardized lattice-based DSA. The developments show that lattice-based cryptography is the most well-rounded option in terms of security, efficiency, scalability and implementability, with code-based, hash-based and multivariate approaches still catering for specific applications and continuing to inspire current research for future quantum-safe security solutions (Yesina et al., 2022; Mohammed, 2018). Table 1 contains a summary of the mathematical underpinnings, advantages, disadvantages, and typical schemes for the four main post-quantum cryptographic families.

Table 1. Comparative Characteristics of Major Post-Quantum Cryptographic Families

Cryptographic family	Security foundation	Main strengths	Main limitations	Representative schemes	References
Lattice-based	LWE, Ring-LWE, Module-LWE, SVP	Efficient, scalable, strong standardization progress	Moderate key, ciphertext, and signature sizes	CRYSTALS-Kyber, Dilithium, Falcon, NTRU	(Micciancio, 2025; Wang et al., 2023)
Code-based	Syndrome decoding and error-correcting codes	Long-standing security, efficient encryption and decryption	Very large public keys	Classic McEliece, BIKE, HQC	(Gaborit & Deneuville, 2021; Singh, 2019)
Hash-based	Preimage, second preimage, and collision resistance	Strong security assumptions and simple construction	Large signatures and state-management requirements	XMSS, LMS, SPHINCS+	(Bernstein et al., 2019; Li et al., 2022)
Multivariate	Multivariate quadratic equation problem	Fast signing and compact signatures	Vulnerability to algebraic and structural attacks	UOV, Rainbow	(Beullens, 2021; Ding et al., 2020)

3.7 Practical Applications of Post-Quantum Cryptography

With the rapid advancement of quantum computing, the rollout of PQC has been gaining momentum in various industries where the security of sensitive data is paramount. PQC offers a solution that withstands quantum attacks without disrupting the current digital infrastructure, making it a viable alternative for secure communication and data protection.PQC is a practical approach to ensuring secure communication and data protection, as it remains compatible with the existing digital infrastructure and provides resistance to quantum attacks. With the advent of quantum threats near the horizon, enterprises are incorporating quantum-resistant algorithms into their critical applications to guarantee confidentiality, integrity, authentication, and secure key exchange in the quantum era.

PQC is also making its way into secured Internet communication, including Transport Layer Security (TLS), Virtual Private Networks (VPN), secure email protocols, and web authentication protocols, for data sent over public networks. This ensures secure communication even if there is a future threat to this, reducing the threat of “harvest now, decrypt later” attacks.

Specifically, in the cloud computing environment, PQC makes data transport, storage and user identity more secure by replacing the current public-key infrastructure with quantum resistant ways of performing cryptography and key encapsulation. These algorithms can be used to ensure secure cloud migration, compatibility with services and computational cost reduction.

The Internet of Things (IoT) applications are also provided with lightweight quantum resistant cryptographic schemes as an important aid. With attention to billions of connected devices sharing sensitive information, efficient post-quantum authentication and key management protocols help keep homes smart, industrial automation, healthcare monitoring and intelligent transportation systems safe without imposing undue energy or computational demands.

PQC is utilized in blockchain and distributed ledger technologies to prevent future quantum attacks on digital signatures, wallet authentication and consensus mechanisms. The adoption of signature algorithms that are resistant to quantum computers will help safeguard the security and immutability of decentralized financial systems, smart contracts, and digital asset transactions in the long run.

The use of PQC is particularly important in the healthcare industry, where secure and private access to EHRs, medical imaging, genomic databases, and telemedicine solutions is essential for long-term storage. Similarly, quantum-resistant encryption is applied to safeguard digital identities in online banking and payment systems, as well as interbank transactions, against new quantum-type attacks from financial institutions. Post-quantum migration is also a topic of active research by government and defense organisations to protect national security networks, military communications and critical infrastructure, among other things, that contain classified information. The diverse applications cited highlight the potential of PQC to become a key component in the quest for secure and robust digital environments in the era of quantum computing.

3.8 Emerging Trends and Future Research Directions

PQC is an emerging technology that is developing rapidly, and the research community is working on creating new and more secure, efficient and deployable cryptographic solutions. Although many success stories have been realized due to lattice-based, code-based, hash-based, and multivariate methods, ongoing research now focuses on solving the real deployment challenges, computational efficiency and making the systems more resistant to novel attack models. A possible solution is development of hybrid systems, which are systems that are compatible with both classical and post-quantum algorithms, to ensure better security during the transition to quantum safe infrastructures and provide backward compatibility. These hybrid solutions allow companies to make a gradual transition without having to overhaul their communication systems or risk security breaches.

A further noted trend is the combination of Quantum Key Distribution (QKD) with post-quantum cryptographic algorithms. PQC gives resistance to software while QKD gives information-theoretic security to key exchange using quantum communication channels. These complementary technologies are expected to create very secure communication networks, which will be able to withstand both computational and physical attacks. At the same time, however, light weight post quantum cryptography is becoming more of a focus, with optimized algorithms developed for resource-limited scenarios like the Internet of Things (IoT), wireless sensor networks, embedded systems, and edge computing platforms. The aim of these solutions is to achieve a small footprint for the computation, memory, communication and energy used, while maintaining

strong quantum-resistant security.

Further research directions include the use of dedicated cryptographic accelerators, dedicated GPUs, Field-Programmable Gate Arrays (FPGAs), and specialized processors to boost the speed of execution of post-quantum cryptographic algorithms that require significant computational power. At the same time, the advent of artificial intelligence-enabled cryptanalysis has created further possibilities for revealing algorithmic weaknesses, the intelligent selection of parameters, and enhanced security analysis using sophisticated machine learning methods. Moreover, ongoing international development and adoption as well as especially after NIST post-quantum standardization, will be important in shaping interoperable security frameworks across governments, industries and critical infrastructures. However, there are still some open research issues to be addressed, such as reducing the size of the keys and signatures, increasing the efficiency of the implementation, improving resistance to side channel attacks, secure migration strategies and cryptographic agility in the long term. These challenges must be overcome to make scalable, efficient, and resilient quantum-resistant cryptographic systems a reality that will keep future digital systems secure. The main challenges faced during the implementation of PQC and their related future research directions are summarized in Table 2.

Table 2. Research Challenges and Future Directions in PQC

Research challenge	Current limitation	Future direction	References
Large keys and signatures	Increased storage and communication overhead	Develop compact parameters and compression methods	(Bansod & Ragha, 2022; Yesina et al., 2022)
Computational overhead	Higher processing and energy requirements	Optimize algorithms and use hardware acceleration	(Pronika & Tyagi, 2021; Kane et al., 2020)
Side-channel attacks	Leakage through timing, power, and memory behavior	Design constant time and leakage-resistant implementations	(Lai et al., 2025; Mattsson et al., 2021)
Migration complexity	Limited interoperability with classical systems	Adopt hybrid cryptography and cryptographic agility	(Jenefa et al., 2023; Dam et al., 2023)
Cryptanalytic uncertainty	Emerging attacks may weaken candidate schemes	Continuing security evaluation and parameter refinement	(Beullens, 2021; Singh et al., 2024)

4. Conclusion

As quantum computing enters the scene, the current public-key cryptographic systems are facing a paradigm shift and need to be equipped and implemented with quantum resistant security solutions. This review described in detail the four major families of PQC: lattice-based, code-based, hash-based and multivariate Cryptography, which includes their mathematical background, security assumptions, characteristics and practical applications. Lattice-based cryptography appears to have the best balance of high security, computational efficiency, scalability and standardization preparedness, while code-based cryptography has high security, but the keys are large. While hash-based schemes still have many proven security properties associated with them, they are excellent schemes for digital signatures, multivariate cryptography is still a good scheme with good lightweight authentication properties, although it continues to be a challenge to cryptanalyse. The review also highlights the increasing significance and need for hybrid cryptographic architecture, lightweight implementations, hardware acceleration,

and international standardization efforts for the transition to quantum-safe communication systems. While much progress has been made, efficiency of implementation, side channel resistant communication, overhead, and secure migration strategies are areas that need further research. Moving forward, algorithm performance optimization, enhancing security against new quantum attack models and creating interoperable deployment mechanisms in various application areas of interest should be addressed in future research. Together, these advances will help to create resilient and sustainable cryptographic infrastructures for the post-quantum era that will safeguard digital information.

References

1. Asif, M., & Agal, S. (2025, May). A comprehensive study on lattice, code, and hash-based cryptographic algorithms in post-quantum security with practical applications. In Parul University International Conference on Engineering and Technology 2025 (PiCET 2025) (Vol. 2025, pp. 1176-1183). IET.
2. Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., ... & Stehlé, D. (2019). CRYSTALS-Kyber algorithm specifications and supporting documentation. NIST PQC Round, 2(4), 1-43.
3. Bandeira, A. S., Kunisky, D., & Wein, A. S. (2019). Computational hardness of certifying bounds on constrained PCA problems. arXiv preprint arXiv:1902.07324.
4. Bansod, S., & Ragha, L. (2022, February). Secured and Quantum Resistant Key Exchange Cryptography Methods–A Comparison. In 2022 Interdisciplinary Research in Technology and Management (IRTM) (pp. 1-5). IEEE.
5. Bernstein, D. J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., & Schwabe, P. (2019, November). The SPHINCS+ signature framework. In Proceedings of the 2019 ACM SIGSAC conference on computer and communications security (pp. 2129-2146).
6. Beullens, W. (2021, June). Improved cryptanalysis of UOV and rainbow. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 348-373). Cham: Springer International Publishing. Cryptanalysis and Security Challenges
7. Cohen, R., Kadosh, M., Lo, A., & Sayah, Q. (2021). Lb scalability: Achieving the right balance between being stateful and stateless. IEEE/ACM Transactions on Networking, 30(1), 382-393.
8. Dam, D. T., Tran, T. H., Hoang, V. P., Pham, C. K., & Hoang, T. T. (2023). A survey of post-quantum cryptography: Start of a new race. Cryptography, 7(3), 40.
9. Debus, P., Wendlinger, M., Tscharke, K., Herr, D., Brügmann, C., De Mello, D. O., ... & Petsch, F. (2025, August). Entangled Threats: A Unified Kill Chain Model for Quantum Machine Learning Security. In 2025 IEEE International Conference on Quantum Computing and Engineering (QCE) (Vol. 1, pp. 1653-1664). IEEE.
10. Dickinson, M., Debroy, S., Calyam, P., Valluripally, S., Zhang, Y., Antequera, R. B., ... & Xu, D. (2018). Multi-cloud performance and security driven federated workflow management. IEEE Transactions on Cloud Computing, 9(1), 240-257.

11. Ding, J., Petzoldt, A., & Schmidt, D. S. (2020). Multivariate cryptography. In Multivariate public key cryptosystems (pp. 7-23). New York, NY: Springer US.
12. Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). Crystals–dilithium: Digital signatures from module lattices.
13. Feneuil, T., Joux, A., & Rivain, M. (2023). Shared permutation for syndrome decoding: new zero-knowledge protocol and code-based signature.
14. Gaborit, P., & Deneuville, J. C. (2021). Code-based cryptography. In Concise encyclopedia of coding theory (pp. 799-822). Chapman and Hall/CRC.
15. Gyasi-Nyarko, D., Freeman, E., Ujakpa, M. M., Amponsah, W., & Amoako, S. O. (2025, May). A Systematic Review of Public Key Cryptography: Implementation, Challenges and Future Opportunities. In 2025 IST-Africa Conference (IST-Africa) (pp. 1-15). IEEE.
16. Jenefa, A., Josh, F. T., Taurshia, A., Kumar, K. R., Kowsega, S., & Naveen, E. (2023, December). PQC Secure: Strategies for defending against quantum threats. In 2023 2nd international conference on automation, computing and renewable systems (ICACRS) (pp. 1799-1804). IEEE.
17. Joux, A., & Mora, R. (2025). The regular multivariate quadratic problem: A. Joux, R. Mora. Designs, Codes and Cryptography, 93(12), 5179-5229.
18. Kane, L. E., Chen, J. J., Thomas, R., Liu, V., & Mckague, M. (2020). Security and performance in IoT: A balancing act. IEEE access, 8, 121969-121986.
19. Lai, R., Swarnakar, M., & Woo, I. (2025). Leaky LWE: learning with errors with semi-adaptive secret-and error-leakage. IACR Communications in Cryptology, 1-23.
20. Li, L., Lu, X., & Wang, K. (2022). Hash-based signature revisited. Cybersecurity, 5(1), 13.
21. Mattsson, J. P., Smeets, B., & Thormarker, E. (2021). Quantum-resistant cryptography. arXiv preprint arXiv:2112.00399.
22. Micciancio, D. (2025). Lattice-based cryptography. In Encyclopedia of Cryptography, Security and Privacy (pp. 1400-1403). Cham: Springer Nature Switzerland. Micciancio, D. (2025). Lattice-based cryptography. In Encyclopedia of Cryptography, Security and Privacy (pp. 1400-1403). Cham: Springer Nature Switzerland.
23. Mohammed, A. (2018). Quantum-Resistant Cryptography: Developing Encryption Against Quantum Attacks. Journal of Innovative Technologies, 1(1), 1-14.
24. Nisha, F., Lenin, J., Saravanan, S. K., Rohit, V. R., Selvam, P. D., & Rajmohan, M. (2024, February). Lattice-based cryptography and NTRU: quantum-resistant encryption algorithms. In 2024 international conference on emerging systems and intelligent computing (ESIC) (pp. 509-514). IEEE.
25. Pronika, S., & Tyagi, S. (2021). Performance analysis of encryption and decryption algorithm. Indonesian Journal of Electrical Engineering and Computer Science, 23(2), 1030-1038.

26. Sharath, H. A., Vrindavanam, J., Dana, S., & Prasad, S. N. (2025). Quantum-resilient cryptography: A survey on classical and quantum algorithms. IEEE Access.
27. Singh, A., Sivangi, K. B., & Tentu, A. N. (2024). Machine learning and cryptanalysis: An in-depth exploration of current practices and future potential. Journal of Computing Theories and Applications, 1(3), 257-272.
28. Singh, H. (2019). Code based cryptography: Classic mceliece. arXiv preprint arXiv:1907.12754.
29. Siu, K., Stuart, D. M., Mahmoud, M., & Moshovos, A. (2018, September). Memory requirements for convolutional neural network hardware accelerators. In 2018 IEEE International Symposium on Workload Characterization (IISWC) (pp. 111-121). IEEE.
30. Sood, N. (2024). Cryptography in post quantum computing era. Available at SSRN 4705470.
31. Tom, J. J., Anebo, N. P., Onyekwelu, B. A., Wilfred, A., & Eyo, R. E. (2023). Quantum computers and algorithms: a threat to classical cryptographic systems. Int. J. Eng. Adv. Technol, 12(5), 25-38.
32. Wang, X., Xu, G., & Yu, Y. (2023). Lattice-based cryptography: A survey. Chinese Annals of Mathematics, Series B, 44(6), 945-960.
33. Wang, Y., & Wang, M. (2019). Module-lwe versus ring-lwe, revisited. Cryptology ePrint Archive.
34. Yesina, M. V., Ostrianska, Y. V., & Gorbenko, I. D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process. Radiotekhnika, (210), 75-86.