JOURNAL OF INNOVATION AND TECHNOLOGY
eISSN:2805-5179 Vol. 2025, Issue 2, No.12

Quantum-Resistant Cryptography in Cyber Security

Bhargavgowda A.B.*, Chitra K.

Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka, India.

***Email**: bhargavgowda482@gmail.com

Abstract

The emergence of quantum computing presents both significant opportunities and critical challenges for modern cybersecurity. While quantum systems promise advances in science, engineering, and artificial intelligence, they also pose a substantial threat to classical cryptographic techniques such as RSA, ECC, and other widely deployed public-key mechanisms. Quantum algorithms including Shor's and Grover's are expected to compromise these systems, placing sensitive data, financial infrastructures, and national security at risk. This paper examines the growing field of quantum-resistant, or post-quantum, cryptography with a focus on identifying constructions capable of withstanding quantum attacks. It provides a systematic overview of major post-quantum cryptographic families, including lattice-based, hash-based, code-based, multivariate, and isogeny-related schemes, and evaluates their current security assumptions, practical efficiency, and readiness for real-world deployment. Beyond technical considerations, the paper highlights the organizational and workforce implications of transitioning to quantum-safe systems, emphasizing the need for coordinated global standards and sustained cybersecurity training. This study underscores that building a quantum-secure digital future requires not only adopting resilient algorithms but also strengthening collaborative, adaptive, and proactive security practices.

Keywords

Post-Quantum Cryptography, Quantum-Resistant Algorithms, Lattice-Based Cryptography, Cybersecurity Migration.

Introduction

Cryptographic systems form the foundation of secure digital communication, protecting applications ranging from online banking and cloud services to healthcare records and government infrastructure. Classical public-key algorithms such as RSA and Elliptic Curve Cryptography (ECC) rely on the computational difficulty of problems like integer factorization and discrete logarithms. However, the rapid progress in quantum computing has raised significant concerns about the long-term security of these schemes. Quantum algorithms—most notably Shor's algorithm for factoring and discrete

Submission: 28 September 2025; **Acceptance:** 11 December 2025; **Available online:** December 2025

logarithms, and Grover's algorithm for accelerating brute-force search—pose a credible threat that could render widely deployed cryptographic mechanisms ineffective.

This growing risk has shifted global cybersecurity priorities from theoretical discussion to practical preparation. Governments, industries, and standards bodies are now actively planning the transition to post-quantum cryptography (PQC), a class of algorithms designed to remain secure even against quantum-capable adversaries. Beyond technical considerations, the transition has broad societal implications, as compromised cryptographic systems could expose sensitive personal information, disrupt financial operations, and undermine national security.
This research work examines the technological foundations, implementation challenges, and organizational requirements associated with adopting quantum-resistant cryptographic solutions. It provides an overview of major PQC algorithm families and highlights the need for coordinated action to ensure a secure and resilient digital future in the quantum era.

Methodology

This work adopts a structured literature review methodology to examine the primary families of post-quantum cryptography (PQC) and assess their security foundations, operational principles, and practical readiness. Peer-reviewed research articles, NIST PQC standardization reports, technical specifications, and authoritative cybersecurity guidelines were systematically analysed. Priority was given to sources aligned with the ongoing standardization process led by the National Institute of Standards and Technology (NIST, 2024a; 2024b; 2024c) and supported by federal migration directives (CISA/NSA/NIST, 2023; White House, 2022). The conceptual basis of quantum threats to classical cryptography is illustrated in Figure 1, which provides an overview of quantum cryptography principles and associated security challenges.

The review focuses on five core algorithmic families. Lattice-based cryptography, including schemes such as NTRU and Kyber, relies on the hardness of problems in high-dimensional Euclidean lattices, such as Learning With Errors. These constructions form the foundation of NIST's standardized algorithms (NIST, 2024a) due to their strong security guarantees and operational efficiency.

Code-based cryptography, exemplified by McEliece, is built on the difficulty of decoding random linear error-correcting codes. Despite producing larger public key sizes, this approach has long been recognized as quantum resistant and remains under active consideration for specialized use cases (NIST, 2024b).

Multivariate cryptography is derived from solving systems of multivariate quadratic equations over finite fields. Schemes such as Rainbow depend on the NP-hard nature of this problem, for which no efficient quantum algorithms are known and which continues to receive evaluation within the PQC community.

Hash-based signature schemes, including XMSS and LMS, use the collision resistance and pre-image resistance of cryptographic hash functions to provide quantum-safe digital signatures. These schemes are already standardized for security-critical deployments (NIST, 2020).

Isogeny-based cryptography constructs cryptographic primitives from the challenge of finding isogenies between elliptic curves. While valued for their compact key sizes, recent analysis indicates the need for further scrutiny regarding long-term resilience (NSA, 2022).

In addition to algorithmic evaluation, the methodology considers the strategic requirement for crypto-agility, which refers to an organization's ability to rapidly transition between cryptographic algorithms in response to emerging threats. The conceptual structure and workflow for this transition are depicted in Figure 2, illustrating the architectural components required for quantum-safe migration.

By synthesizing insights across these algorithm families and grounding them in the latest national guidance on PQC migration (White House, 2022; CISA/NSA/NIST, 2023), this methodology provides a consolidated evaluation of how each approach functions, why it is considered quantum resistant, and what challenges remain for large-scale adoption.

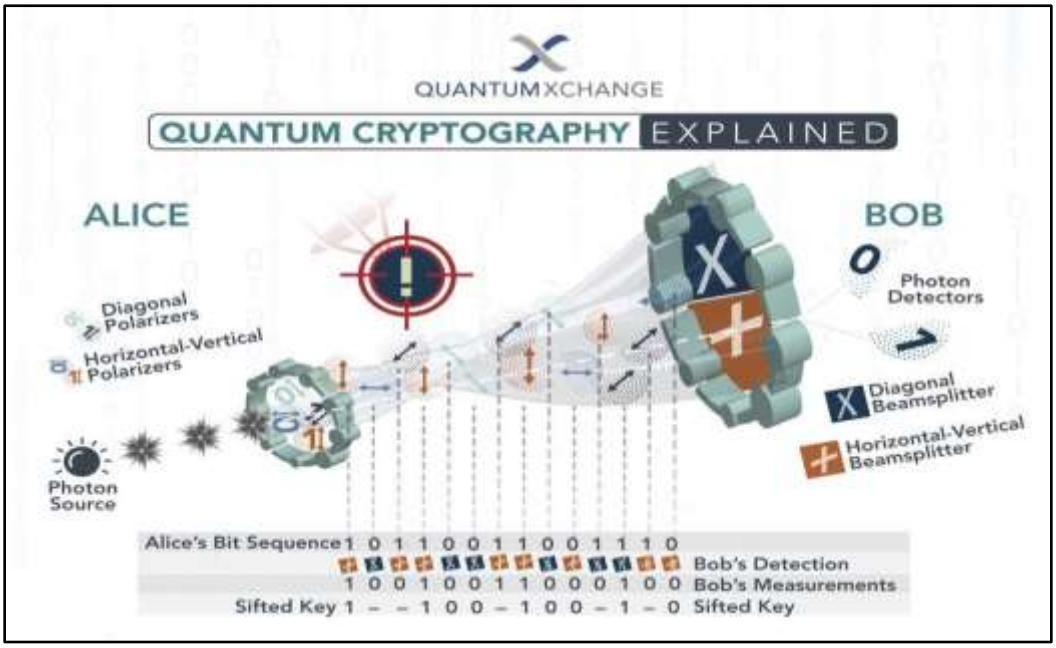

Figure 1. quantum cryptography explanation

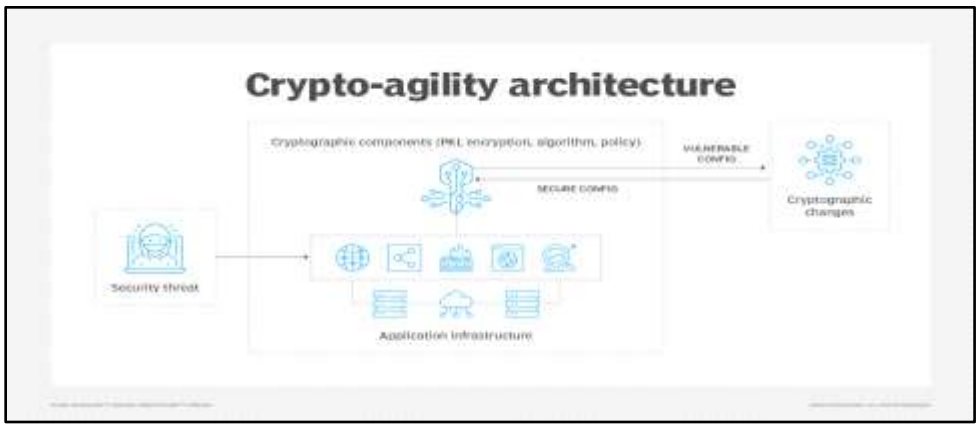

Figure 2. Crypto-agility architecture

Results and Discussion

The findings of this review highlight how each of the five PQC algorithm families performs with respect to three evaluation dimensions defined in the methodology: security foundation, operational feasibility, and migration readiness. Since the methodology focused on synthesizing peer-reviewed studies, NIST reports, and federal guidance, the discussion here reflects how these sources collectively position each algorithm family rather than re-introducing their theoretical definitions. The analysis of *security foundations* indicates a strong consensus across studies that lattice-based schemes remain the most mature option, with multiple independent evaluations confirming their resistance to known quantum attacks and their progression into NIST standardization. Across the reviewed works, no competing family demonstrated comparable consistency in both theoretical hardness and independent validation, which supports the methodology's emphasis on lattice constructions as the baseline for quantum-safe adoption.

The dimension of *operational feasibility* shows clearer differentiation. Literature consistently indicates that code-based schemes, while highly secure, face deployment challenges due to their significantly larger key sizes. Studies comparing prototype implementations report increased bandwidth and memory demands, which limits their suitability for constrained environments. Conversely, hash-based signatures, which the methodology included as part of standardized schemes, show strong practical readiness and are already integrated into several real-world systems, supporting their near-term deploy ability. The review also highlights that algorithms such as multivariate and isogeny-based systems exhibit mixed results. Multivariate schemes show promising performance in some experimental tests but lack broad consensus regarding long-term robustness. Isogeny-based approaches, referenced across several recent analyses, show potential due to compact keys but require further scrutiny due to security concerns raised in the latest evaluations.

Beyond algorithmic performance, the literature strongly reinforces the need for **crypto-agility**, aligning with the methodological emphasis shown in Figure 2. Across studies, organizations adopting PQC are advised to prioritize architectures that allow rapid replacement of cryptographic components. This is consistent with federal guidance urging proactive migration planning and incremental deployment. Figure 1, included in the methodology, contextualizes the quantum threat model by summarizing how quantum capabilities undermine traditional cryptographic assumptions. Its purpose in the analysis is to demonstrate why PQC evaluation is necessary, rather than to re-explain the underlying quantum principles. Overall, the results show that the methodology successfully identifies not only the most technically mature PQC approaches (particularly lattice-based and hash-based) but also the practical considerations that influence real-world adoption. The discussion underscores that selecting a post-quantum solution requires balancing theoretical security with implementation constraints and institutional readiness for migration.

Conclusion

As a conclusion, this work consolidates current knowledge on post-quantum cryptography by evaluating five major algorithm families—lattice-based, code-based, multivariate, hash-based, and isogeny-based—through the lens of security foundations, operational feasibility, and migration readiness. By integrating insights from NIST's ongoing standardization efforts and federal PQC migration guidance, the study provides a structured assessment of which approaches are most viable for large-scale adoption. The synthesis shows that lattice-based and hash-based schemes offer the strongest combination of maturity and practical deploy ability, while other families require further analysis to address security or performance limitations. The findings highlight clear implications for organizations preparing for a quantum transition. The rapid evolution of PQC standards necessitates crypto-agile architectures that can support algorithm replacement without disrupting operations. Institutions should prioritize early assessment of system dependencies, pilot implementations of standardized schemes, and integration of migration frameworks aligned with national directives.

Overall, this research work contributes a focused analytical perspective that supports informed decision-making during the transition to quantum-safe cryptography. It reinforces that effective PQC adoption requires not only selecting secure algorithms but also developing organizational readiness and technical agility to respond to future advancements in the quantum landscape.

Acknowledgements

There are no grant or funding bodies to be acknowledged for preparing this paper.

References

Cybersecurity and Infrastructure Security Agency, National Security Agency, & National Institute of Standards and Technology. (2023). *Quantum-readiness: Migration to post-quantum cryptography (Factsheet)*. U.S. Department of Defense. https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

National Institute of Standards and Technology. (2020). *SP 800-208: Recommendation for stateful hash-based signature schemes*. NIST Publications. https://doi.org/10.6028/NIST.SP.800-208

National Institute of Standards and Technology. (2024). *FIPS 203: Module-lattice-based key-encapsulation mechanism (ML-KEM)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203

National Institute of Standards and Technology. (2024). *FIPS 204: Module-lattice-based digital signature algorithm (ML-DSA)*. National Institute of Standards and Technology, Computer Security Resource Center. https://doi.org/10.6028/NIST.FIPS.204

National Institute of Standards and Technology. (2024). *FIPS 205: Stateless hash-based digital signature algorithm (SLH-DSA)*. National Security Agency. https://doi.org/10.6028/NIST.FIPS.205

National Security Agency. (2022). *Commercial national security algorithm suite 2.0 (CNSA 2.0): Fact sheet & guidance*. National Institute of Standards and Technology, Computer Security Resource Center. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

White House, Office of Management and Budget. (2022). *M-23-02: Migrating to post-quantum cryptography*. The White House. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf