International Journal of Advance Innovations, Thoughts and Ideas

Brief Report Open Access

# Post-Quantum Cryptography: Challenges, Solutions, Adoption

**Dr. Victor Hwang***

Department of Information Security, Seoul Institute of Technology, Seoul, South Korea

***Corresponding Author:** Dr. Victor Hwang, Department of Information Security, Seoul Institute of Technology, Seoul, South Korea, E-mail: victor.hwang@sit.ac.uk

**Received:** 02-Sep-2025, Manuscript No. IJAITI-25-173455; **Editor assigned:** 04-Sep-2025, PreQC No. IJAITI-25-173455(PQ); **Reviewed:** 18-Sep-2025, QC No. IJAITI-25-173455; **Revised:** 23-Sep-2025, Manuscript No. IJAITI-25-173455(R); **Published:** 30-Sep-2025, **DOI**: 10.4172/2277-1891.1000354

**Citation:** Hwang DV (2025) Post-Quantum Cryptography: Challenges, Solutions, Adoption. Int J Adv Innovat Thoughts Ideas 14: 354.

## Abstract

This collective body of research explores post-quantum cryptography (PQC), addressing the urgent need to secure digital information against future quantum attacks. It delves into the mathematical foundations and design principles of quantum-resistant schemes, including lattice-based, code-based, and hash-based cryptography. Key topics include NIST's standardization efforts, the evaluation of candidate algorithms, and significant implementation challenges such as computational overhead and integration into existing systems. Special attention is given to PQC's impact on *Internet of Things* (IoT) security and blockchain technology, alongside strategies for optimizing performance and ensuring a smooth transition to quantum-secure digital infrastructures.

## Keywords

Post-quantum cryptography; Quantum attacks; Lattice-based cryptography; Code-based cryptography; NIST standardization; IoT security; Blockchain security; Implementation challenges; Cryptographic schemes; Quantum-resistant algorithms

## Introduction

The field of post-quantum cryptography (PQC) stands as a critical area of research, addressing the imminent threat posed by quantum computers to current cryptographic standards. Extensive surveys offer a comprehensive overview of this domain, delving into the mathematical foundations and design principles behind various quantum-resistant schemes. These include lattice-based, code-based, multivariate polynomial, and hash-based cryptography [1].

The urgent need for a transition to quantum-resistant schemes is consistently emphasized, given the looming threat of quantum computers. Researchers explore the mathematical problems underpinning candidate algorithms like lattice-based, code-based, and multivariate cryptography, providing accessible insights into this complex landscape. There's also a clear focus on the ongoing standardization efforts and the practical challenges associated with deploying these new cryptographic primitives in real-world applications [2].

Implementing post-quantum cryptographic algorithms introduces significant hurdles, particularly concerning computational overhead, memory requirements, and seamless integration into existing systems. Various optimization strategies are explored to enhance efficiency, such as hardware acceleration and software-level improvements. These efforts aim to make schemes like lattice-based and code-based cryptography more feasible for real-world deployment in a post-quantum era [3].

Systematic reviews categorize post-quantum algorithms by their underlying mathematical problems, rigorously evaluating their security proofs against quantum attacks. These analyses also provide insights into the performance metrics of different schemes, highlighting the trade-offs between security, efficiency, and resource consumption. The complexities of transitioning to these new standards within existing communication protocols and infrastructures are a major discussion point [4].

The implications of PQC for securing Internet of Things (IoT) devices are a significant area of investigation. Reviews evaluate the suitability of quantum-resistant schemes, such as lattice-based and hash-based signatures, specifically considering the constrained resources of IoT environments. Key challenges identified include performance overhead and energy consumption, leading to proposals for integrating post-quantum security into future IoT architectures [5]. Similarly, another comprehensive review of post-quantum cryptography specifically for IoT addresses unique security challenges in resource-constrained settings. It systematically categorizes and evaluates quantum-resistant primitives, discussing their suitability for IoT devices based on metrics like computational overhead, memory footprint, and power consumption, and outlines a roadmap for integrating these advanced security solutions into future IoT ecosystems [8].

The National Institute of Standards and Technology (NIST) Post-Quantum Cryptography standardization process is under continuous review. This process details various rounds of evaluation for lattice-based, code-based, and multivariate candidates. Criteria for selection include security against both quantum and classical attacks, performance metrics, and implementation considerations, all while discussing ongoing challenges in establishing robust quantum-resistant standards [6].

Beyond general applications, the intersection of blockchain technology and post-quantum cryptography is critical. Current blockchain security, heavily reliant on Public Key Infrastructure (PKI), is vulnerable to quantum computers. Research explores quantum-resistant algorithms suitable for integration into blockchain frameworks, such as lattice-based and hash-based signatures, addressing challenges and potential solutions for developing quantum-secure blockchain systems capable of withstanding future quantum threats [7].

A specialized focus reveals lattice-based cryptography as a prominent family of PQC schemes. Surveys detail their mathematical foundations, security properties rooted in hard lattice problems, and various construction methods. They analyze the efficiency and security of key algorithms like Kyber and Dilithium, highlighting their advantages in resistance to quantum attacks, and practical considerations for implementation and deployment in a post-quantum world [9].

Finally, the adoption of post-quantum cryptography into existing software systems presents significant challenges and opportunities. This includes the complexities of integrating new cryptographic primitives into legacy codebases, managing performance overhead, and ensuring backward compatibility. Research directions aim at developing tools and methodologies to facilitate a smooth and secure transition to quantum-resistant software, which is crucial for future-proofing digital infrastructure [10].

## Description

The landscape of post-quantum cryptography (PQC) is crucial for securing digital information against future quantum threats. Comprehensive overviews delve into the foundational mathematical principles and design methodologies for various schemes, including lattice-based, code-based, multivariate polynomial, and hash-based cryptography. These surveys explore NIST's standardization efforts, critically assessing the strengths, weaknesses, and remaining security challenges for candidates [1]. Understanding these underlying mathematical problems is essential, with discussions highlighting the urgent need for quantum-resistant solutions. The standardization process is a key theme, alongside challenges of deploying these new cryptographic primitives in real-world applications [2].

A major hurdle in PQC adoption lies in its practical implementation. This involves managing substantial computational overhead, considerable memory requirements, and the complex integration into existing systems. To overcome these, researchers explore optimization strategies like hardware acceleration and software-level improvements. These efforts aim to boost the efficiency and performance of schemes such as lattice-based and code-based cryptography, making them more viable for deployment [3]. Furthermore, systematic reviews analyze algorithms, categorizing them by mathematical underpinnings and rigorously evaluating their security against quantum attacks. Such reviews offer insights into performance metrics, clarifying trade-offs in security, efficiency, and resource consumption. Difficulties in migrating existing communication protocols and infrastructures to new standards are frequently highlighted [4].

The specific application of PQC in specialized domains like the Internet of Things (IoT) presents unique considerations. Reviews dedicated to IoT security analyze quantum-resistant schemes, such as lattice-based and hash-based signatures, assessing their suitability for resource-constrained IoT devices. Critical challenges identified include performance overhead and increased energy consumption. This research often proposes concrete directions for integrating post-quantum security into future IoT architectures [5]. Another comprehensive review for IoT further emphasizes these unique security challenges in constrained environments, systematically categorizing and evaluating quantum-resistant cryptographic primitives. It assesses their fitness for IoT devices based on metrics like computational overhead, memory footprint, and power consumption, outlining a roadmap for integrating advanced security solutions into upcoming IoT ecosystems [8].

Standardization efforts, particularly by NIST, are central to PQC's future. Surveys meticulously review this process, detailing multiple rounds of evaluation for candidates including lattice-based, code-based, and multivariate schemes. Selection criteria are multifaceted, encompassing security against quantum and classical attacks, performance benchmarks, and critical implementation considerations. Ongoing challenges and future directions for establishing robust, quantum-resistant cryptographic standards are consistently discussed [6]. This systematic approach ensures chosen algorithms are theoretically sound, practically implementable, and efficient.

Beyond general infrastructure, blockchain technology faces unique vulnerabilities from quantum computing. Current blockchain security relies heavily on Public Key Infrastructure (PKI), susceptible to quantum attacks. Research investigates various quantum-resistant algorithms, such as lattice-based and hash-based signatures, for potential integration into blockchain frameworks. The goal is to address challenges and develop viable solutions for creating quantum-secure blockchain systems capable of defending against future quantum threats [7]. This highlights a crucial area where existing digital trust mechanisms need urgent quantum-proofing.

Finally, adopting PQC into existing software systems introduces substantial challenges and novel opportunities. This involves navigating the complexities of integrating new cryptographic primitives into legacy codebases, effectively managing performance overhead, and ensuring backward compatibility. Research actively points towards developing new tools and methodologies designed to facilitate a smooth and secure transition to quantum-resistant software, a vital step for future-proofing critical digital infrastructure [10]. Additionally, a focused survey on lattice-based cryptography, a prominent PQC family, provides detailed insights into its mathematical foundations, security properties from hard lattice problems, and various construction methods. It analyzes the efficiency and security of algorithms like Kyber and Dilithium, highlighting their quantum resistance and practical implementation considerations [9].

# Conclusion

The current digital landscape faces an impending threat from quantum computers, necessitating a global shift to post-quantum cryptography (PQC). This area of study comprehensively surveys mathematical foundations, design principles, and standardization efforts for quantum-resistant schemes like lattice-based, code-based, multivariate polynomial, and hash-based cryptography. Research highlights the critical need for this transition, evaluating the strengths, weaknesses, and security challenges of various candidate algorithms, especially those undergoing NIST's standardization process.

Implementing PQC algorithms introduces significant practical challenges, including managing computational overhead, memory requirements, and integration complexities. Optimization strategies, such as hardware acceleration and software improvements, are crucial for enhancing efficiency, particularly for lattice-based and code-based schemes. Beyond general applications, PQC has vital implications for securing specific domains. For instance, in the Internet of Things (IoT), researchers analyze the suitability of quantum-resistant solutions for resource-constrained devices, addressing performance and energy consumption issues. Similarly, the integration of PQC into blockchain technology is explored to fortify its security against quantum attacks, given its reliance on vulnerable public-key infrastructure.

The adoption of PQC into existing software systems also presents challenges related to legacy codebases, performance management, and backward compatibility. Specialized surveys delve into specific PQC families, such as lattice-based cryptography, detailing their mathematical underpinnings and analyzing the efficiency and quantum resistance of algorithms like Kyber and Dilithium. The overarching goal across all these efforts is to develop robust, efficient, and deployable quantum-resistant solutions to future-proof digital infrastructure against evolving quantum threats.

# References

1. Chen R, Hou Z, Luo T, Zhang P, Li F et al. (2021) Post-quantum cryptography: a comprehensive survey. J. Inf. Sec. Appl. 61:102919

2. Ecker E, Krenn R, Seidl D, Trummer J, Pichler L et al. (2023) The Future of Cryptography: An Overview of Post-Quantum Cryptography. Sensors 23:6813

3. Banaszak M, Michalak A, Zięba A, Szmaj K, Krawiec P et al. (2023) Post-Quantum Cryptography Implementation Challenges and Optimization Strategies. Sensors 23:7578

4. Ali T, Qamar Z, Hussain S, Nawaz A, Ahmad N et al. (2022) Post-Quantum Cryptography: A Systematic Review. KSII Trans. Internet Inf. Syst. 16:1308-1327

5. Shah J, Hussain A, Khan L, Naeem H, Asghar N et al. (2021) A review of post-quantum cryptographic algorithms and their impact on IoT security. J. Ambient Intell. Humaniz. Comput. 12:4577-4596

6. Pan J, Jiang S, Ma J, Wang J, Zhang S et al. (2021) A Survey of NIST Post-Quantum Cryptography Standardization Process. EURASIP J. Wirel. Commun. Netw. 2021:161

7. Khan N, Ullah N, Ali I, Iqbal M, Muhammad K et al. (2023) Blockchain and Post-Quantum Cryptography: Challenges and Solutions. Sensors 23:7800

8. Abbas W, Khan M, Asif A, Khan N, Shah J et al. (2022) A Comprehensive Review of Post-Quantum Cryptography for the Internet of Things. Electronics 11:3887

9. Li Y, Wu X, Wei Z, Zhang Z, Gao F et al. (2022) A Survey on Post-Quantum Cryptography: Lattice-based Cryptography. China Commun. 19:36-53

10. Hämmerle C, Heider S, Heider G, Sprengelmeyer L, Schütz M et al. (2023) Challenges and Opportunities of Post-Quantum Cryptography Adoption in Software Systems. SN Comput. Sci. 4:412