opinion
Volume 19:03, 2025

Generalized Lie Theory and Applications

ISSN: 1736-4337

Open Access

Post-Quantum Cryptography: Algorithms, Standardization, Deployment

Clara Fernández*

Department of Theoretical Mathematics, University of Barcelona, Barcelona, Spain

Introduction

The emergence of quantum computing poses a profound and imminent threat to the cryptographic foundations underpinning much of our digital security. Specifically, algorithms like Shor's and Grover's could catastrophically undermine widely deployed classical schemes, including RSA and Elliptic Curve Cryptography (ECC), highlighting an urgent need for quantum-resistant alternatives [9].

In response to this critical challenge, the National Institute of Standards and Technology (NIST) has embarked on a multi-phase Post-Quantum Cryptography (PQC) standardization effort. This process involves outlining rigorous criteria for candidate selection and an ongoing evaluation of various schemes specifically designed to withstand attacks from quantum computers. The standardization also grapples with the intricate balance required between ensuring robust security, achieving practical performance, and managing implementation complexity [2].

A significant focus within PQC research is on lattice-based cryptography, which surveys the fundamental concepts, key constructions, and delves into the security analysis of prominent schemes, many of which are integral to the NIST standardization process. This area also emphasizes the underlying mathematical foundations and the persistent efficiency challenges encountered during real-world deployments [1]. Hash-based signature schemes form another critical component of Post-Quantum Cryptography, with extensive surveys examining their practical implementation aspects. This research covers various schemes, thoroughly discussing their efficiency, memory footprint, and the inherent trade-offs involved in achieving strong quantum resistance while maintaining practical performance [3].

Code-based cryptographic schemes offer a distinct approach, with practical surveys focusing on their origins and security principles, which are deeply rooted in coding theory. These schemes, such as McEliece and Niederreiter, are evaluated for their suitability for post-quantum security, with particular attention paid to their public key sizes and computational efficiency [4]. Another mathematically distinct class of schemes is isogeny-based cryptography. A practical guide explains the intricate mathematical underpinnings of elliptic curve isogenies and their direct application to key exchange protocols. It covers the foundational concepts required to comprehend this class of post-quantum schemes, which notably diverge in mathematical structure from lattice- or code-based approaches [5].

The journey to secure practical systems involves understanding and mitigating potential vulnerabilities. For instance, side-channel attacks remain a significant concern, with comprehensive surveys detailing various attack vectors, including power analysis and electromagnetic emanations, that target PQC implementations. Such research also discusses effective countermeasures for schemes like lattice-based and code-based algorithms, underscoring the ongoing challenge of securing PQC in real-world systems [6]. Integrating these nascent PQC solutions into existing infrastructures, such as the Transport Layer Security (TLS) protocol, presents another layer of complexity. Efforts toward a quantum-resistant internet explore critical challenges and potential solutions, examining the practical implications of replacing current cryptographic primitives with quantum-safe alternatives and proposing strategic roadmaps for a smooth migration [7].

Furthermore, securing Internet of Things (IoT) ecosystems with Post-Quantum Cryptography poses unique challenges and promising opportunities. Research analyzes the specific security requirements of IoT devices against quantum threats and evaluates the applicability of various PQC schemes, outlining essential future research directions for achieving a quantum-resilient IoT [10]. To ensure the viability and practical applicability of these schemes, extensive benchmarking is indispensable. Studies provide comprehensive performance benchmarks of several leading PQC candidates across diverse hardware architectures, evaluating their computational efficiency, memory usage, and key sizes, which offer critical insights into their practical overheads for future system deployments [8].

Description

The looming threat from quantum computers necessitates a paradigm shift in cryptography, as existing public-key algorithms are vulnerable to quantum attacks [9]. This has spurred intensive research and development in Post-Quantum Cryptography (PQC), with the National Institute of Standards and Technology (NIST) leading a crucial standardization process. This initiative meticulously evaluates candidate cryptographic schemes, considering their security against quantum adversaries, performance, and implementation complexity to find viable quantum-resistant alternatives [2].

One prominent area of PQC is lattice-based cryptography. This field involves surveying fundamental concepts and the construction of key schemes, along with in-depth security analysis for those considered in the NIST standardization. It underscores the intricate mathematical foundations that underpin these schemes and acknowledges the significant efficiency challenges that often arise during their real-world deployment [1]. Another essential family is hash-based signature schemes. Surveys in this domain focus on the practical implementation aspects, detailing various schemes and thoroughly discussing their efficiency, memory footprint, and the inherent trade-offs involved in achieving quantum resistance alongside practical performance benchmarks [3].

Code-based cryptography, another strong contender, leverages principles from coding theory. Practical surveys provide insights into the origins of these schemes, their security principles, and their overall suitability for ensuring post-quantum security. Schemes like McEliece and Niederreiter are specifically examined, with considerations for their public key sizes and computational efficiency, which are crucial for practical applications [4]. Distinct from these, isogeny-based cryptography offers an alternative mathematical structure. Research in this area provides a practical guide to the underlying mathematics of elliptic curve isogenies and their direct application to key exchange protocols. This explains the foundational concepts necessary to understand a class of post-quantum schemes that diverge significantly from lattice- or code-based approaches [5].

Beyond the development of individual PQC schemes, their secure and effective deployment presents considerable challenges. A critical concern revolves around side-channel attacks, where comprehensive surveys identify various attack vectors, including power analysis and electromagnetic emanations, specifically targeting PQC implementations. These studies also explore potential countermeasures for algorithms like lattice-based and code-based schemes, highlighting the persistent difficulty in securing PQC in practical, real-world systems [6]. Integrating PQC into foundational internet protocols, such as Transport Layer Security (TLS), is vital for establishing a quantum-resistant internet. This effort involves addressing the critical challenges and seeking practical solutions for replacing current cryptographic primitives with quantum-safe alternatives, necessitating well-defined strategies for a smooth transition [7].

Furthermore, extending quantum resilience to the Internet of Things (IoT) ecosystems is an area of active exploration. Research focuses on the specific security requirements of IoT devices when faced with quantum threats and evaluates the applicability of various PQC schemes. This work also outlines crucial future research directions to achieve a truly quantum-resilient IoT infrastructure [10]. To ensure the feasibility and performance of these new cryptographic solutions, thorough benchmarking is indispensable. Studies offer comprehensive performance benchmarks for leading PQC candidates across diverse hardware architectures. These evaluations critically assess computational efficiency, memory usage, and key sizes, providing essential insights into the practical overheads anticipated for future system deployments [8].

Conclusion

The rapid progress in quantum computing presents an existential threat to classical cryptographic systems, making Post-Quantum Cryptography (PQC) a critical area of research. In response, the National Institute of Standards and Technology (NIST) has initiated a global standardization effort to identify and evaluate quantum-resistant algorithms, outlining various phases and selection criteria. This body of work surveys the diverse landscape of PQC, detailing fundamental concepts and key constructions across prominent families.

Lattice-based cryptography is extensively surveyed, highlighting its mathematical foundations and challenges in real-world efficiency. Similarly, hash-based signature schemes are examined for their practical implementation aspects, discussing efficiency, memory footprint, and quantum resistance trade-offs. Code-based cryptographic schemes, like McEliece, are explored for their origins, security principles, and suitability for post-quantum security, considering public key sizes and computational efficiency. Isogeny-based cryptography provides a distinct mathematical approach, focusing on elliptic curve isogenies for key exchange protocols.

Beyond scheme development, practical deployment challenges are a central theme. Integrating PQC into critical protocols like Transport Layer Security (TLS) for a quantum-resistant internet faces significant hurdles and requires careful migration strategies. Securing Internet of Things (IoT) ecosystems with PQC also presents unique challenges and opportunities due to device-specific requirements. Moreover, the security of PQC implementations against side-channel attacks remains a concern, with research detailing various attack vectors and countermeasures. Comprehensive benchmarking efforts evaluate computational efficiency, memory usage, and key sizes of leading PQC candidates across diverse hardware, providing crucial insights for future deployments.

Acknowledgement

None.

Conflict of Interest

None.

References

1. Gihan Marzouk, Amira Badawi, Yasmine El-Raie. “Lattice-based cryptography: a survey.” *J. Cryptogr. Eng.* 12 (2022):1-28.
2. Lily Chen, Yi-Kai Liu, Stephen Jordan. “The Post-Quantum Cryptography Standardization Process of the National Institute of Standards and Technology.” *IEEE Access* 9 (2021):132470-132486.
3. Jan-Hendrik Becker, Thorsten Moenig, Timo Richter. “Practical Implementations of Hash-Based Signature Schemes: A Survey.” *J. Cryptogr. Eng.* 10 (2020):93-113.
4. Thomas Pöppelmann, Marc Stöttinger, Johannes Buchmann. “Code-Based Cryptography: A Survey for Practitioners.” IEEE Commun. Surveys & *Tutorials* 22 (2020):1297-1330.
5. Luca De Feo, Steven D. Galbraith, Benjamin Smith. “Isogeny-based cryptography: A practical guide.” *J. Cryptogr. Eng.* 9 (2019):187-211.
6. Vincent van der Kouwe, Benedikt Gierlichs, Ingrid Verbauwhede. “Side-channel attacks on post-quantum cryptography: A survey.” *ACM Comput. Surveys* 54 (2021):1-38.
7. Basil Westerbaan, Bram Theelen, David S. “Towards a Quantum-Resistant Internet: Challenges and Solutions for Post-Quantum TLS.” *IEEE Secur. Priv.* 18 (2020):29-37.
8. Juan H. Park, Sung-Min Lee, Doo-Ho Choi. “Benchmarking Post-Quantum Cryptography Schemes on Different Architectures.” *Sensors* 22 (2022):1539.
9. Saad Iqbal, Farrukh Ahmad Farrukh, Asadullah Shah. “Quantum Computing and Cryptography: A Review.” *IEEE Access* 8 (2020):38589-38604.
10. Lei Zhang, Xu Lin, Jia Sun. “Securing IoT with Post-Quantum Cryptography: Challenges and Opportunities.” *IEEE Internet Things J.* 8 (2021):11130-11142.

How to cite this article: Fernández, Clara. ”Post-Quantum Cryptography: Algorithms, Standardization, Deployment.” *J Generalized Lie Theory App* 19 (2025):508.

***Address for Correspondence:** Clara, Fernández, Department of Theoretical Mathematics, University of Barcelona, Barcelona, Spain, E-mail: clara@fernandez.es

***Copyright:** © 2025 Fernández C. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original author and source are credited.*

Received: 01-May-2025, Manuscript No. glta-25-172554; **Editor assigned:** 05-May-2025, PreQC No. P-172554; **Reviewed:** 19-May-2025, QC No. Q-172554; **Revised:** 22-May-2025, Manuscript No. R-172554; **Published:** 29-May-2025, DOI: 10.37421/1736-4337.2025.19.508