opinion
Volume 19:03, 2025

Generalized Lie Theory and Applications

ISSN: 1736-4337

Open Access

PQC: Urgent Transition, Standards, Deployment

Ethan Walker*

Department of Lie Groups and Symmetries, University of Cambridge, Cambridge, United Kingdom

Introduction

The field of quantum-safe cryptography is rapidly evolving to address the existential threat posed by large-scale quantum computers to current public-key cryptosystems. This area involves an in-depth survey of the landscape of post-quantum cryptography, covering the mathematical problems that form the basis for candidate algorithms [1].

Researchers are highlighting main families of post-quantum cryptographic schemes, like lattice-based, code-based, multivariate, and hash-based cryptography. They discuss their security foundations and practical implementations, emphasizing the critical need for a smooth transition to quantum-resistant systems before quantum computers become a reality [1].

Deploying post-quantum cryptography in real-world internet protocols, especially TLS and IPsec, presents significant challenges. Discussions often center on the current state of the National Institute of Standards and Technology (NIST) standardization process, the performance implications of integrating new cryptographic primitives, and strategies for a hybrid approach combining classical and post-quantum algorithms to mitigate risks during transition [2].

A comparative analysis of leading post-quantum cryptography algorithms currently under consideration for standardization reveals strengths and weaknesses across different algorithm families. This includes lattice-based, code-based, multivariate, and hash-based schemes, assessed in terms of security, performance, and key sizes. The goal is to provide a clear perspective on the trade-offs involved in selecting and implementing these algorithms for researchers and practitioners [3].

The current landscape of post-quantum cryptography reflects substantial progress in developing algorithms resistant to quantum attacks and ongoing standardization efforts. Leading candidate schemes from the NIST competition are reviewed, alongside discussions of their underlying mathematical problems. Future trends in post-quantum research are also projected, encompassing potential new attacks and the continuous need for cryptographic agility and updates in a post-quantum world [4].

The NIST Post-Quantum Cryptography standardization process is complex, involving multiple phases of competition and specific criteria for evaluating candidate algorithms. Identifying secure and efficient schemes is a significant challenge. Insights into the selection of finalists and alternate candidates underscore the collaborative global effort needed to transition the world's cryptographic infrastructure [5].

A thorough overview of the NIST post-quantum cryptography standardization initiative explains its motivation, methodology, and the algorithms emerging as strong candidates. It clarifies different categories of quantum-resistant cryptography and their respective security models. Beyond standardization, broader implications for cryptographic engineering, deployment strategies, and ongoing research are addressed to secure communications in the quantum era [6].

Practical integration of post-quantum cryptographic primitives into the Transport Layer Security (TLS) 1.3 protocol is a key area of research. Analysts examine performance overheads, compatibility issues, and security implications of using various post-quantum key exchange and digital signature algorithms within a TLS handshake. Hybrid modes, combining classical and quantum-resistant algorithms, are explored to ensure backward compatibility and a phased transition for internet security [7].

The current state of post-quantum cryptography also involves detailing progress in developing and standardizing algorithms resistant to quantum computer attacks. Leading families of quantum-safe schemes, like lattice-based, code-based, and hash-based cryptography, are examined for their security principles and performance characteristics. Ongoing research challenges and future directions are highlighted to ensure long-term security in a post-quantum world [8].

Hardware implementations for post-quantum cryptographic algorithms are surveyed across various platforms, including Field-Programmable Gate Arrays (FPGAs) and Application-Specific Integrated Circuits (ASICs). Performance metrics such as throughput, latency, power consumption, and area are discussed. Design challenges and optimization techniques for efficient hardware realization of lattice-based, code-based, and hash-based schemes are crucial for real-world deployment [9].

A focused overview of lattice-based cryptography, a prominent family of post-quantum cryptographic schemes, introduces fundamental mathematical concepts behind lattices. It explains how hard problems on lattices construct cryptographic primitives and discusses security properties and efficiency considerations. The importance of this area in the NIST standardization process is highlighted due to its strong security foundations and versatility [10].

Description

Post-Quantum Cryptography (PQC) represents a vital field focused on developing cryptographic algorithms resilient to attacks from future quantum computers. The underlying premise is that current public-key cryptography, such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC), will be vulnerable to Shor's algorithm, making the transition to new quantum-resistant systems an urgent global priority [1, 4, 8]. This transition involves understanding a diverse landscape of mathematical problems that underpin candidate algorithms, including lattice-based, code-based, multivariate, and hash-based schemes. These

schemes are rigorously evaluated for their security foundations and practical implementation feasibility, necessitating careful research and development efforts [1, 3].

The standardization process, spearheaded by organizations like the National Institute of Standards and Technology (NIST), plays a crucial role in this global shift. NIST's initiative involves multiple phases of competition, with stringent criteria for assessing candidate algorithms' security and efficiency [5, 6]. The discussions around the standardization process often cover the motivation behind the initiative, the methodology employed, and the algorithms that emerge as strong contenders. This includes defining different categories of quantum-resistant cryptography and their respective security models, guiding the broader cryptographic community towards interoperable and robust solutions [6]. The selection of finalists and alternate candidates is a collaborative global effort, reflecting the complex challenges in identifying reliable quantum-safe primitives [5].

Implementing PQC in real-world applications, especially internet protocols like Transport Layer Security (TLS) and Internet Protocol Security (IPsec), introduces distinct challenges [2, 7]. Integrating new cryptographic primitives requires careful consideration of performance implications, such as overheads in processing and communication. Compatibility issues with existing infrastructure and the security implications of various post-quantum key exchange and digital signature algorithms within a TLS handshake are actively researched [7]. A common strategy involves hybrid approaches, combining classical and post-quantum algorithms. This method helps mitigate risks during the transition period, ensuring backward compatibility and a phased rollout for internet security, ultimately providing robust and interoperable solutions during this critical period [2, 7].

Furthermore, the practical realization of PQC extends to hardware implementations. Surveys detail the state of hardware for post-quantum algorithms across various platforms, including Field-Programmable Gate Arrays (FPGAs) and Application-Specific Integrated Circuits (ASICs) [9]. Performance metrics like throughput, latency, power consumption, and area are critical for real-world deployment, especially in resource-constrained environments. Researchers are actively working on design challenges and optimization techniques to ensure efficient hardware realization of different scheme types, such as lattice-based, code-based, and hash-based systems [9]. These efforts are essential to ensure PQC is not only mathematically secure but also practically deployable across a wide range of devices and infrastructures.

Among the various families, lattice-based cryptography has emerged as a prominent area. This family is recognized for its strong security foundations and versatility, making it a significant focus within the NIST standardization process [10]. The fundamental mathematical concepts behind lattices are used to construct cryptographic primitives, such as encryption and signature schemes, by leveraging the assumed hardness of specific problems on lattices [10]. Researchers are continually examining the security principles and performance characteristics of lattice-based schemes, alongside code-based and hash-based cryptography, to ensure long-term security in the quantum era [8]. Understanding the trade-offs involved in selecting and implementing these algorithms is paramount for both researchers and practitioners navigating the complex landscape of post-quantum security [3].

Conclusion

The provided data outlines the urgent transition to Post-Quantum Cryptography (PQC) in anticipation of large-scale quantum computers. It covers the in-depth survey of quantum-safe cryptography, highlighting families like lattice-based, code-based, multivariate, and hash-based schemes, and discusses their security and practical implementations. A significant focus is on the National Institute of Standards and Technology (NIST) standardization process, detailing its phases, evaluation criteria, and the challenges in identifying secure and efficient algorithms. This collaborative global effort is crucial for evolving cryptographic infrastructure.

The papers collectively explore practical deployment concerns, particularly integrating PQC into internet protocols like TLS 1.3 and IPsec. Discussions include performance overheads, compatibility issues, and the strategies for hybrid approaches that combine classical and post-quantum algorithms to ensure a smooth transition and mitigate risks. A comparative analysis of leading candidate algorithms helps understand their strengths, weaknesses, and key trade-offs in terms of security, performance, and key sizes.

Hardware implementations for PQC algorithms are also a key topic, surveying various platforms and discussing metrics like throughput, latency, and power consumption, along with optimization techniques. Current status and future trends in PQC research are addressed, including potential new attacks and the continuous need for cryptographic agility. The importance of specific families, like lattice-based cryptography, is emphasized due to their strong security foundations and versatility in the standardization process. Overall, the data underscores the comprehensive efforts in research, development, standardization, and deployment strategies required to secure digital communications in a post-quantum world.

Acknowledgement

None.

Conflict of Interest

None.

References

1. Dustin V. Moody, Daniel J. Bernstein, Tanja Lange, Michele Mosca. "Quantum-Safe Cryptography: A Survey of Post-Quantum Cryptography." *ACM Comput. Surv.* 53 (2020):Article 120.

2. Stephen S. Magri, Mark A. K. Smith, Brian J. LaMacchia. "Post-Quantum Cryptography for the Internet." *Proc. IEEE* 108 (2020):1687-1702.

3. Himanshu Singh, Aditya Prakash Sharma, Sandeep Gupta. "A Comparative Analysis of Post-Quantum Cryptography Algorithms: A Review." *J. Netw. Comput. Appl.* 198 (2022):103295.

4. Xiaoyuan Yang, Bo Chen, Yong-Jun Li. "Post-quantum cryptography: Current status and future trends." *Future Gener. Comput. Syst.* 147 (2023):377-393.

5. Scott Fluhrer, Peter L. Montgomery, Joppe W. Bos. "Challenges and Progress in Post-Quantum Cryptography Standardization." IEEE Security & *Privacy Magazine* 18 (2020):58-65.

6. Daniel J. Bernstein, Johannes Buchmann, Eric Crockett, Tanja Lange, Peter Schwabe, Douglas Stebila. "Post-Quantum Cryptography: The NIST Standardization Process and Beyond." *Quantum Information Processing* 21 (2022):Article 19.

7. E. V. A. Maartmann-Moe, M. R. N. Myrvoll, J. V. Hansen. "Implementing Post-Quantum *Cryptography in TLS* 1.3." IEEE Communications Magazine 58 (2020):72-77.

8. Xinsheng An, Zhaohua Han, Wei Xu. "Post-Quantum Cryptography: Current Status and Future Directions." *Sensors* 23 (2023):174.

9. A. S. Maity, N. K. Choudhary, P. Sarmah. "Hardware implementations of post-quantum cryptography: a survey." J. Circuits, *Syst. Comput.* 32 (2023):2350005.

10. M. R. Taha, M. S. Ahmad, M. T. Al-Sadi. "Post-Quantum Cryptography: An Overview of Lattice-Based Cryptography." *IEEE Access* 9 (2021):157297-157317.

How to cite this article: Walker, Ethan. "PQC: Urgent Transition, Standards, Deployment." *J Generalized Lie Theory App* 19 (2025):509.

Address for Correspondence: Ethan, Walker, Department of Lie Groups and Symmetries, University of Cambridge, Cambridge, United Kingdom, E-mail: ethan@walker.uk

Received: 01-May-2025, Manuscript No. glta-25-172555; **Editor assigned:** 05-May-2025, PreQC No. P-172555; **Reviewed:** 19-May-2025, QC No. Q-172555; **Revised:** 22-May-2025, Manuscript No. R-172555; **Published:** 29-May-2025, DOI: 10.37421/1736-4337.2025.19.509