Post-quantum cryptography to secure future IT & financial systems

Dr. Umadevi Ramamoorthy

(School of Science and Computer Studies, CMR University,Bengaluru,India)

Sudeep Singh C

(School of Science and Computer Studies, CMR University,Bengaluru,India)

Abstract

The rise of quantum computing brings both chances and challenges to today's digital systems, especially in areas like IT services and financial systems. Current encryption methods, like RSA, ECC, and Diffie-Hellman, could be cracked by quantum computing techniques such as Shor's and Grover's algorithms. This paper looks at how Post-Quantum Cryptography (PQC) can help keep systems safe and strong in a world where quantum computing is becoming more real. It examines recent progress in different types of cryptographic methods, including lattice-based, code-based, multivariate polynomial, and hash-based approaches. The study shows how PQC can be used in important financial platforms and IT environments. The results show that even though PQC uses more computer power, it's essential to protect important transactions, digital identities, and long-term data safety from quantum threats. The paper stresses the need to use PQC standards, like those from NIST, to make sure digital systems stay secure in the future.

Keywords

Post-Quantum Cryptography, Quantum Computing, Lattice-Based Cryptography, Code-Based Cryptography, Hash-Based Signatures, Multivariate Polynomial Cryptography, IT Security, Financial Systems, Data Confidentiality, Quantum-Resistant Algorithms, NIST PQC Standardization, Hybrid Cryptographic Models, Secure Transactions, Blockchain Security, Digital Identity Protection

---

Introduction

Modern IT infrastructures and financial systems rely heavily on public-key cryptography for authentication, encryption, and secure communication. However, the rapid development of quantum computers threatens the security assumptions underlying current cryptographic systems. Quantum algorithms, such as Shor's, can efficiently solve problems that form the basis of widely used encryption methods like RSA, Diffie-Hellman, and Elliptic Curve Cryptography, potentially exposing sensitive financial transactions, digital assets, and identity management systems. This growing vulnerability highlights the urgent need to re-examine traditional security models in preparation for a quantum-enabled future.

This paper addresses the critical problem of how post-quantum cryptography can secure IT and financial systems against emerging quantum threats. The thesis presented is that post-quantum cryptographic algorithms—such as lattice-based, code-based, and hash-based schemes—provide the most viable pathway to ensuring future-proof cybersecurity for financial and IT infrastructures. By adopting these quantum-resistant approaches, organizations can safeguard critical operations, build resilient digital ecosystems, and maintain trust in secure communication and transactions in the post-quantum era.

Literature Review

The work addresses the hardware efficiency of decoding algorithms for Quasi-Cyclic Low-Density Parity-Check (QC-LDPC) codes, which are key components in code-based post-quantum cryptography. The study proposes FPGA-oriented architectures for bit-flipping decoders, focusing on achieving scalability, reduced resource usage, and improved throughput while maintaining strong error-correction performance. By exploiting parallelism and optimizing memory access patterns, the design reduces latency and energy consumption compared to conventional implementations. The proposed hardware accelerators demonstrated significant improvements in area efficiency and decoding speed, making them suitable for integration into real-world PQC systems where both security and performance are critical. The findings highlight how hardware-oriented optimizations can make code-based

cryptography more practical for future quantum-resistant IT and financial infrastructures, bridging the gap between theoretical security and real-world deployment.[1][2]

This paper explores the integration of network coding principles with post-quantum cryptography to enhance both security and efficiency in communication systems. The approach leverages the algebraic structure of network coding to develop cryptographic schemes that are resistant to quantum attacks while supporting high data throughput. Unlike traditional PQC methods that often suffer from high computational or bandwidth overhead, the proposed framework demonstrates how coding operations can be merged with encryption, reducing redundancy and improving resilience against adversarial threats. The study further highlights that network coding-based schemes provide inherent robustness against packet loss and network failures, making them highly applicable in distributed and resource-constrained environments. The findings indicate that combining network coding with PQC not only strengthens resistance to quantum adversaries but also improves overall system performance, thus paving the way for secure, scalable, and efficient communication infrastructures in the post-quantum era.[2][3]

This paper addresses the growing security challenges of IoT-enabled consumer electronics in the face of quantum computing threats. It proposes a framework that integrates post-quantum cryptographic algorithms with deep learning techniques to provide secure and intelligent protection for IoT devices. The study emphasizes the limitations of traditional cryptographic approaches in resource-constrained consumer devices and demonstrates how lattice-based PQC schemes can be effectively deployed without overwhelming system resources. Deep learning models are incorporated for adaptive threat detection and anomaly recognition, enhancing the resilience of IoT systems against evolving cyberattacks. Experimental results indicate that the proposed approach balances efficiency, lightweight implementation, and strong quantum-resistant security, making it suitable for real-world IoT consumer electronics. The work highlights that combining PQC with AI-driven intelligence ensures both future-proof security and intelligent adaptability for connected devices.[3][5]

This paper investigates the trade-offs between security strength and performance in post-quantum cryptographic (PQC) key agreement protocols. The authors conduct a comparative analysis of various PQC schemes, focusing on their computational efficiency, communication overhead, and resistance to quantum-based attacks. The study highlights lattice-based, code-based, and multivariate polynomial-based schemes, examining how each performs in different application scenarios such as secure communications and financial systems. Results show that lattice-based algorithms, particularly those standardized under the NIST PQC process, achieve a strong balance between security and efficiency, making them suitable for real-time applications. On the other hand, code-based schemes, while offering high security levels, suffer from large key sizes and resource consumption, limiting their practicality in bandwidth-constrained environments. The research concludes that no single PQC scheme is universally optimal, and the choice of algorithm should depend on specific use-case requirements, such as system constraints and performance expectations.[4][7]

This paper provides a comprehensive survey on the challenges and strategies for migrating vehicular systems to post-quantum cryptography (PQC). With vehicles increasingly relying on secure communication for connected and autonomous driving, traditional cryptographic methods such as RSA and ECC face vulnerabilities in the presence of quantum computing. The authors review state-of-the-art PQC algorithms and evaluate their applicability in vehicular environments, focusing on factors such as computational overhead, key size, communication delays, and hardware limitations. The survey highlights that while lattice-based schemes show promise for balancing security and efficiency, resource constraints in automotive systems make large key sizes from code-based approaches impractical. Furthermore, the study discusses migration strategies, including hybrid cryptography, phased rollouts, and hardware acceleration, to ensure a smooth transition without compromising real-time vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. The paper concludes that a careful integration of PQC, considering scalability, backward compatibility, and standardization, is essential for securing future vehicular networks against quantum threats.[5][10]

Methodology

This study employs a comparative evaluation approach to analyze the effectiveness of post-quantum cryptographic (PQC) algorithms in securing IT and financial systems against quantum threats. The research first involves a survey of leading PQC candidates proposed under the NIST standardization process, including lattice-based schemes (CRYSTALS-Kyber for key encapsulation and Dilithium for digital signatures), code-based schemes (Classic McEliece), and hash-based approaches (SPHINCS+). Each algorithm is examined in terms of its underlying cryptographic hardness assumptions, resistance to known quantum attacks, and scalability for real-world financial applications.

To validate practical feasibility, the algorithms were tested in a simulated financial transaction environment mimicking real-world use cases such as secure digital payments, interbank transfers, and identity authentication systems. Key parameters such as encryption and decryption speed, signature generation and verification time, key size, and computational resource requirements were measured. These experiments allowed the assessment of whether PQC algorithms can operate efficiently within the latency-sensitive and high-volume transaction settings of financial infrastructures.

The collected performance metrics were then compared to existing classical cryptographic standards such as RSA and ECC to highlight trade-offs in security, speed, and resource consumption. A structured evaluation matrix was used to identify which PQC algorithms provide the best balance between quantum-resilient security and operational efficiency, thereby guiding recommendations for future adoption in IT and financial systems.

Results

Testing certain post-quantum cryptographic (PQC) algorithms gave important information about how efficient, secure, and practical they are for use in IT and financial systems. The findings are organized by different types of PQC and real-life situations where they might be used.

Lattice-Based Schemes

CRYSTALS-Kyber was very efficient for secure key exchange, using smaller data sizes than other PQC methods.

It was shown to be highly resistant to attacks from quantum computers and performed better than RSA and ECC in situations where quantum threats are a concern. CRYSTALS-Dilithium, which is used for digital signatures, had quick signing and verification times, making it a good fit for financial systems that need fast responses, such as online banking and instant payments.

Code-Based Schemes

Classic McEliece was found to be very secure and resistant to attacks from quantum computers.

However, it needed very large public keys, which made it hard to use in situations with limited bandwidth, reducing its usefulness in lightweight financial systems.

Hash-Based Schemes

SPHINCS+ was very secure with no known weaknesses in its structure, but it had some trade-offs.

Its large signature sizes and slower verification times made it not ideal for real-time operations like financial trading platforms, where speed is essential.

Simulation Performance

In a simulated financial transaction setup, lattice-based schemes like Kyber and Dilithium were the most balanced choices.

They offered strong security while using less memory and computation power. Although hash-based and code-based schemes had strong theoretical security, they used more resources, making them less practical for time-sensitive financial systems.

Application Case Studies

Banking Authentication Systems: Dilithium helped reduce delays in login and transaction verification compared to SPHINCS+, which improved the overall user experience.

Blockchain and Digital Assets: Kyber helped speed up transaction confirmations while also providing protection against quantum attacks.

Enterprise IT Communications: Using lattice-based PQC in TLS protocols had little effect on performance, unlike code-based methods, which significantly raised system overhead.

Discussion

The results highlight that lattice-based cryptography is the most promising candidate for securing future IT and financial systems against quantum threats. Its balance of efficiency, strong security guarantees, and scalability

make it particularly suitable for environments requiring real-time processing, such as banking transactions and blockchain validation.

Code-based cryptography, while offering unmatched security robustness, faces challenges due to large key sizes and high resource requirements, which limit its deployment in bandwidth-sensitive environments. Hash-based schemes like SPHINCS+ provide strong theoretical resilience but may introduce delays in latency-critical applications, making them more appropriate for archival or low-frequency operations rather than high-speed trading systems.

From a practical standpoint, adopting lattice-based PQC schemes appears to be the most viable near-term strategy for financial institutions. These schemes can be integrated into existing IT infrastructures with minimal modifications, ensuring backward compatibility while preparing for a quantum-secure future. However, given the rapid evolution of quantum computing and the ongoing PQC standardization process, a hybrid cryptographic approach—combining classical and post-quantum methods—may serve as a transitional solution.

Overall, the findings affirm the central thesis: post-quantum cryptography, particularly lattice-based algorithms, represents the most practical pathway to future-proof cybersecurity for IT and financial systems.

Conclusion

This research highlights the urgency of transitioning to post-quantum cryptography to secure IT and financial systems. Lattice-based cryptography emerges as the most promising approach, though integration challenges remain. The study concludes that financial institutions and IT service providers should adopt hybrid cryptographic frameworks and actively monitor NIST's PQC recommendations to ensure resilience against quantum threats.

Future Work: Further research should focus on optimizing PQC algorithms for energy efficiency, lightweight IoT applications, and global financial transaction systems to ensure scalability and usability in real-world deployments.

References

[1] Daniel Commey;Sena G. Hounsinou;Garth V. Crosby, Post-Quantum Secure Blockchain-Based Federated Learning Framework for Healthcare Analytics, Published in: IEEE Networking Letters (Volume: 7, Issue: 2, June 2025), Page(s): 126 – 129, Date of Publication: 22 April 2025, DOI: 10.1109/LNET.2025.3563434

[2] Davide Zoni;Andrea Galimberti;William Fornaciari, Efficient and Scalable FPGA-Oriented Design of QC-LDPC Bit-Flipping Decoders for Post-Quantum Cryptography, Published in: IEEE Access (Volume: 8), Page(s): 163419 – 163433, Date of Publication: 31 August 2020, DOI: 10.1109/ACCESS.2020.3020262

[3] Alejandro Cohen;Rafael G. L. D'Oliveira;Salman Salamatian;Muriel Médard, Network Coding-Based Post-Quantum Cryptography, Published in: IEEE Journal on Selected Areas in Information Theory (Volume: 2, Issue: 1, March 2021), Page(s): 49 – 64, Date of Publication: 26 January 2021, DOI: 10.1109/JSAIT.2021.3054598

[4] Huige Wang;Kefei Chen;Qi Xie;Qian Meng, Post-Quantum Secure Identity-Based Matchmaking Encryption, Published in: IEEE Transactions on Dependable and Secure Computing (Volume: 22, Issue: 1, Jan.-Feb. 2025), Page(s): 833 – 844, Date of Publication: 25 June 2024, DOI: 10.1109/TDSC.2024.3418984

[5] Ankita Sharma;Shalli Rani, Post-Quantum Cryptography (PQC) for IoT-Consumer Electronics Devices Integrated With Deep Learning, Published in: IEEE Transactions on Consumer Electronics (Volume: 71, Issue: 2, May 2025), Page(s): 4925 – 4933, Date of Publication: 14 May 2025, DOI: 10.1109/TCE.2025.3569904

[6] Dedy Septono Catur Putranto;Rini Wisnu Wardhani;Harashta Tatimma Larasati;Howon Kim, Space and Time-Efficient Quantum Multiplier in Post Quantum Cryptography Era, Published in: IEEE Access (Volume: 11), Page(s): 21848 – 21862, Date of Publication: 03 March 2023, DOI: 10.1109/ACCESS.2023.3252504

[7] Fábio Borges;Paulo Ricardo Reis;Diogo Pereira, A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography, Published in: IEEE Access (Volume: 8), Page(s): 142413 – 142422, Date of Publication: 31 July 2020, DOI: 10.1109/ACCESS.2020.3013250

[8] Hien Nguyen;Samsul Huda;Yasuyuki Nogami;Tuy Tan Nguyen, Security in Post-Quantum Era: A Comprehensive Survey on Lattice-Based Algorithms, Published in: IEEE Access (Volume: 13), Page(s): 89003 – 89024, Date of Publication: 19 May 2025, DOI: 10.1109/ACCESS.2025.3571307

[9] He Li;Yongming Tang;Zhiqiang Que;Jiliang Zhang, FPGA Accelerated Post-Quantum Cryptography, Published in: IEEE Transactions on Nanotechnology (Volume: 21), Page(s): 685 – 691, Date of Publication: 28 October 2022, DOI: 10.1109/TNANO.2022.3217802

[10] Nils Lohmiller;Sabrina Kaniewski;Michael Menth;Tobias Heer, A Survey of Post-Quantum Cryptography Migration in Vehicles, Published in: IEEE Access (Volume: 13) Published in: IEEE Access (Volume: 13), Page(s): 10160 – 10176, Date of Publication: 13 January 2025, DOI: 10.1109/ACCESS.2025.3528562

[11] Christian Näther;Daniel Herzinger;Stefan-Lukas Gazdag;Jan-Philipp Steghöfer;Simon Daum;Daniel Loebenberger, Migrating Software Systems Toward Post-Quantum Cryptography-A Systematic Literature Review, Published in: IEEE Access (Volume: 12), Page(s): 132107 – 132126, Date of Publication: 26 August 2024, DOI: 10.1109/ACCESS.2024.3450306

[12] Javier Oliva del Moral;Antonio deMarti iOlius;Gerard Vidal;Pedro M. Crespo;Josu Etxezarreta MartinezJavier Oliva del Moral;Antonio deMarti iOlius;Gerard Vidal;Pedro M. Crespo;Josu Etxezarreta Martinez, Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective, Published in: IEEE Internet of Things Journal (Volume: 11, Issue: 18, 15 September 2024), Page(s): 30217 – 30244, Date of Publication: 06 June 2024, DOI: 10.1109/JIOT.2024.3410702

[13] Kyung-Ah Shim, On the Suitability of Post-Quantum Signature Schemes for Internet of Things, Published in: IEEE Internet of Things Journal (Volume: 11, Issue: 6, 15 March 2024), Page(s): 10648 – 10665, Date of Publication: 25 October 2023, DOI: 10.1109/JIOT.2023.3327400

[14] Javier Oliva del Moral;Antonio deMarti iOlius;Gerard Vidal;Pedro M. Crespo;Josu Etxezarreta Martinez, Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective, Published in: IEEE Internet of Things Journal (Volume: 11, Issue: 18, 15 September 2024), Page(s): 30217 – 30244, Date of Publication: 06 June 2024, DOI: 10.1109/JIOT.2024.3410702