Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 6, pp. 2477–2488
DOI : 10.47974/JDMSC-2333

Enhancing crypto-interoperability resilience (CIR) by bridging the gap between classical and post-quantum cryptographic standards

Tarun Jain [§]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Loveleen Kumar [†]
Department of Computer Science and Engineering
Swami Keshvanand Institute of Technology, Management & Gramothan
Jaipur 302017
Rajasthan
India

Ginika Mahajan *
Department of Data Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Pankaj Dadheech [‡]
Department of Computer Science and Engineering
Swami Keshvanand Institute of Technology, Management & Gramothan
Jaipur 302017
Rajasthan
India

[§] *E-mail:* tarunjainjain02@gmail.com; tarun.jain@jaipur.manipal.edu
[†] *E-mail:* loveleentak@gmail.com
* *E-mail:* ginika.mahajan@jaipur.manipal.edu (Corresponding Author)
[‡] *E-mail:* pankajdadheech777@gmail.com

Blessy Thankachan [@]
School of Computer Applications
JECRC University, Jaipur
Jaipur 303905
Rajasthan
India

Abstract

With the emergence of real quantum computing technology, the quest to establish strong and secure post-quantum cryptographic (PQC) standards will only grow more urgent. These security standards protect data and communications against the groundbreaking capabilities of quantum computers that threaten to break many of today's ubiquitous cryptographic systems. But there's a major practical gap in PQC standards so they can work with current cryptographic infrastructure. In this paper we present the notion of Crypto-Interoperability Resilience (CIR), which is defined as that a cryptographic system possesses the ability to use post-quantum algorithms behind classical protected protocols in an interchangeable way and can transition from a classical secure mode to a quantum secure mode transparently while remaining secure. Integrating post-quantum (PQ) cryptographic algorithms into existing systems are difficult and comes with compatibility issues, performance limitations, and security concern from the insecure period while migrating, which this research addresses. We present holistic frameworks and methodologies for employing PQC standards in practice. These frameworks allow for stepwise adoption with no disruption of existing functionality and offers backward compatibility. We also create tools and protocols for improving CIR which efforts are performance-optimized and are designed to preserve security at a very high level as well.

Subject Classification: *Primary 68R01, Secondary 97N70.*

Keywords: *Quantum computing, Post-quantum cryptography (PQC), Crypto interoperability resilience (CIR), Quantum-resistant algorithms, Cryptographic integration.*

1. Introduction

Quantum computing is both a broad threat and an enormous opportunity for cryptography. This is because quantum computers use quantum mechanical phenomena for their computational products, giving them a basic computational advantage over classical computers. This is especially true for problems that involve searching a large space of solutions, as they can perform exponentially large computations in polynomial time compared to classical computers. These, in turn, offer potential breakthroughs in numerous areas, ranging from materials

[@] *E-mail:* **blessy.thankachan@jecrcu.edu.in**

science to medicine to artificial intelligence, but quantum computing also brings considerable dangers to today's encryption systems. As quantum computers can solve problems such as integer factorization and discrete logarithms in polynomial time using Shor's algorithm, current data security, which relies on algorithms like RSA and Elliptic Curve Cryptography (ECC), would be susceptible. In response to these new threats, the field of post-quantum cryptography (PQC) has become an important area of study. To produce encryption solutions which are still safe in a quantum computing environment. It covers diverse approaches such as lattice-based schemes, hash-based signatures, code-based cryptography, and multivariate polynomial systems. Such methods are designed to be resistant to quantum attacks in order to secure digital communication and data privacy for the coming years [1,2].

1.1 *Significance of Crypto-Interoperability Resilience*

Although significant work has gone into developing and analyzing post-quantum cryptographic algorithms in terms of security, there is a serious divide when it comes to practical deployment of these algorithms and use with existing cryptographic infrastructure. Anticipating this gap, we introduce the notion of Crypto-Interoperability Resilience (CIR); namely, the ability of a cryptographic system to seamlessly integrate post-quantum cryptographic algorithms with the existing classical cryptographic infrastructure in order to support smooth transitions and sustaining strong security in heterogeneous settings. At the cost of being a bit dense, in more technical terms, the mathematical foundation for CIR engages the interplay between these discrete, mathematical structures and classical cryptographic protocols. The intention is to provide room for post-quantum cryptographic algorithms that can be added without performance or security compromise [3, 4].

1. Lattice-Based Cryptography:

   Lattices (Λ): Discrete point sets in high-dimensional space generated by linear combinations of basis vectors.

   Hard Problems: Learning with Errors (LWE) and Shortest Vector Problem (SVP)are computationally hard for both classical and quantum computers [5].

2. Error-Correcting Codes:

   Linear Codes: Use generator matrices to map messages to codewords, providing error detection and correction.

   Code-Based Cryptography: Depends upon the difficulty of decoding random linear codes, forming the basis of secure cryptographic schemes [6].

3. Hash Functions and Hash-Based Signatures:

   Hash Functions: Maps data of random length to fixed length outputs, ensuring preimage and collision resistance [7].

   Merkle Trees: Tree structures where each node is a hash of its children, used in constructing hash-based digital signatures [8].

4. Combinatorial Structures:

   Block Designs: Sets divided into blocks where each pair of elements appears in a specified number of blocks, used for robust data structuring [9].

   Expander Graphs: Sparse but highly connected graphs enhancing cryptographic security through strong connectivity properties [10].

5. Finite Field Arithmetic:

   Finite Fields (GF(p^n)): Fields with a finite number of elements, crucial for error-correcting codes and various encryption schemes [11-12].

By incorporating these mathematical structures and principles, CIR aims to achieve seamless integration of post-quantum cryptographic algorithms with existing cryptographic infrastructure, ensuring a smooth transition and maintaining robust security across diverse environments

Hybrid Systems: Combine classical and post-quantum cryptographic algorithms to leverage strengths and ensure security.

Transition Frameworks: Mathematical models supporting the gradual adoption of PQC standards while maintaining compatibility with existing systems.

Performance Optimization: Techniques to reduce computational overhead and ensure efficient operation of integrated cryptographic systems.

Security Assessment: Thorough analysis to ensure robust protection against both quantum and classical threats.

2. Classical and Post-Quantum Cryptographic Standards

One biggest threat to classical cryptography systems comes from rapid evolution of quantum computing technology. Quantum computers have fundamental computational supremacy over classical computers based on quantum mechanical effects. This benefit is especially strong in problem domains that involve searching for an exponential amount of potential solutions where they can perform exponentially large computations in polynomial time compared with classical devices. Such a capacity poses a threat to such popularly adopted cryptographic schemes including RSA and ECC, both of which rely on the presumed difficulty of certain mathematical problems like integer factorization and discrete logarithm problems. To protect our digital infrastructure from the looming threat of quantum computers, researchers are currently busy with post-quantum cryptography (PQC), which entails designing new cryptographic algorithms resistant to quantum attacks. Post-quantum algorithms which include hash based, code based, lattice based and multivariate polynomial cryptography, have been developed to secure against classical and quantum computational threats. But, combining these new algorithms with legacy crypto infrastructure involves several challenges, all of which fall within the cross-domain topic of Crypto-Interoperability Resilience (CIR).

2.1 *Challenges of Classical and Post-Quantum Cryptography*

Algorithm Incompatibility: Existing systems and protocols are designed around classical cryptographic algorithms (e.g., RSA, ECC). Transitioning to post-quantum cryptographic (PQC) algorithms often requires substantial changes to system architecture and protocol design.

Standards and Protocols: Many established cryptographic standards (e.g., TLS, SSL) do not natively support PQC algorithms, necessitating updates or complete overhauls.

Computational Overhead: PQC algorithms, such as lattice-based cryptography, often require significantly more computational resources compared to classical algorithms. This may lead to bottlenecks in performance, especially in resource constrained situations as in the case of IoT devices [6].

Key Sizes: PQC algorithms typically involve larger key sizes and ciphertexts, which can impact storage, transmission, and processing efficiency.

Transition Vulnerabilities: During the transition phase from classical to PQC algorithms, systems might be vulnerable to hybrid attacks that exploit weaknesses in both classical and post-quantum protocols.

Incomplete Security Proofs: While many post quantum cryptographic algorithms are believed to be immune against quantum attacks, some lack rigorous security proofs or have not been subjected to extensive cryptographical analysis.

Hardware and Software Integration: Adaptations in existing hardware and software to support PQC algorithms can be complex and costly. Specialized hardware acceleration (e.g., for lattice-based operations) might be required.

Interoperability: Ensuring seamless interoperability between classical and PQC systems is challenging, especially in environments where both types of cryptography need to coexist.

Lack of Established Standards: PQC is a relatively new field, and standardization efforts are still underway. This creates uncertainty and hesitancy in adopting PQC algorithms widely.

Regulatory and Compliance Issues: Updating cryptographic standards to comply with regulatory requirements can be a slow process, impacting the timely adoption of PQC.

Complexity for Users: The increased complexity of PQC algorithms may lead to usability issues, making it harder for users and administrators to understand and manage cryptographic systems [7].

Training and Education: There exists a need for extensive training and education to familiarize security professionals with PQC algorithms and their implementation.

Cost of Transition: The transition to PQC involves significant financial and resource investments in terms of upgrading infrastructure, retraining personnel, and implementing new protocols.

Resource Allocation: Balancing the allocation of resources between maintaining existing classical cryptographic systems and developing new PQC infrastructure can be challenging for organizations.

2.2 *Addressing these challenges needs a multifaceted approach, involving:*

Developing of Hybrid Cryptographic Systems: Systems that can operate with both classical and PQC algorithms, allowing for a gradual transition.

Performance Optimization Techniques: Research and development to improve the efficiency of PQC algorithms, reducing computational overhead and key sizes.

Enhanced Security Protocols: Creating protocols that secure the transition phase and ensure comprehensive security against both classical and quantum threats.

Standardization Efforts: Accelerating standardization processes and establishing clear guidelines for PQC implementation [8].

Educational Initiatives: Providing training and resources to educate security professionals on the nuances of PQC.

By systematically addressing these challenges, the cryptographic community can ensure a smoother transition to post-quantum security, maintaining robust protection in the face of evolving technological threats [9-12].

3. Proposed Scheme for Post-Quantum Cryptographic Standards

In this paper, a hybrid cryptographic scheme is proposed that guarantees Crypto-Interoperability Resilience (CIR) to address these challenges resulting from the implementation of post-quantum

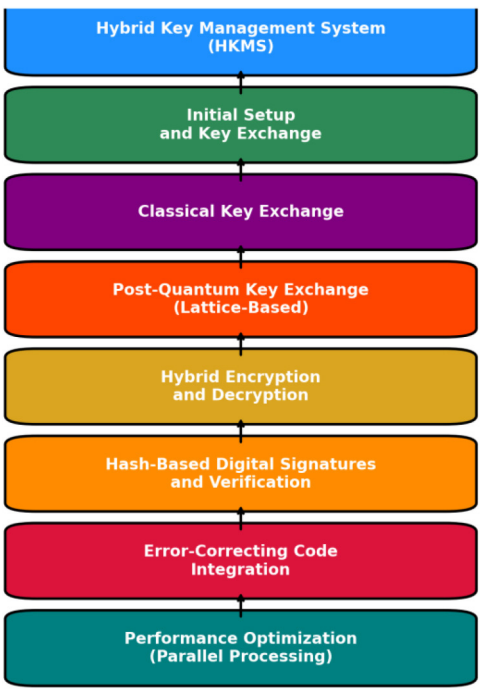

Figure 1

Proposed Hybrid Cryptographic Scheme

cryptographic (PQC) standards with legacy systems. In this scheme, we make use of the best of both Classical and PQC algorithms to provide a seamless transition without reducing the overall performance or security level. In this work, we proposed a hybrid system in which classical cryptographic algorithms are combined with PQC algorithms. These two layers make it backward compatible and also more quantum-safe.

Based on the figure 1, the proposed hybrid cryptographic scheme is constituted by the Several elements which aims to secure quantum level and have the integration of quantum resistant classical and post-quantum cryptographic standards, giving rise to the manifestation of Crypto-Interoperability Resilience (CIR). A working Hybrid Key Management System (HKMS) that will help to generate, store, and distribute classical and post-quantum keys while allowing for backward compatibility and seamless transitioning, all will be key. The initial setup and key exchange phase establish the secure communication channels between peers using both classical and post-quantum methods, which is based on classical key exchange protocols, such as RSA and Diffie-Hellman. We incorporate Post-Quantum Key Exchange protocols, specifically lattice-based approaches, to provide quantum-safe cryptography. The double whammy of applying both classical and post-quantum algorithms for encryption ensures a dual-layer of encryption, whereas hash-based digital signatures ensure quantum-resistant authentication and message integrity. To make the data more resilient to quantum noise, error-correcting codes are used to encode the data before encryption, providing strong error detection and correction capabilities. Performance Optimization: Measurements and Extraction of Elements for Efficient Masses for Post-quantum Algorithms — Achieve Performance Optimization based on parallel processing techniques, utilizing all appropriate capabilities and features of modern high-level architectures to offload the burden of computation involved in PQC algorithms directly on multi-core processors and hardware accelerators. These components together yield a full-blown framework that offers a secure, efficient and practical answer to the post-quantum challenge blending classical and post-quantum cryptography. Lattice-based Diffie-Hellman is the heart of our scheme. The computational hardness of lattice problems allows cryptography based on latices to provide very strong quantum security guarantees.

Let L be a lattice in R^n defined by a basis B={b1,b2,...,bn}….(i)

Alice generates a secret vector $sA \in Zn$ and computes the public vector $pA=B \cdot sA+eA$, where eA is a small error vector.
Bob generates a secret vector $sB \in Zn$ and computes the public vector $pB=B \cdot sB+eB$, where eB is a small error vector.
Alice and Bob exchange their public vectors pA and pB.

Alice computes the shared secret $kA=B \cdot sA+eA+pB-eB$.
Bob computes the shared secret $kB=B \cdot sB+eB+pA-eA$
Since eA and eB are small, $kA \approx kB$, establishing a shared secret key.

To ensure secure authentication, proposed scheme employs hash-based digital signatures, which are intractable to quantum attacks due to the complexity of finding collisions among hash functions.

Let $H : \{0,1\}* \rightarrow \{0,1\}n$ be a cryptographic hash function

Signer generates pair of private or public keys (sk , pk) where pk is derived from sk using the hash function H.

For signing a message m, signer will compute the hash $h =H(m)$ and generate signature $\sigma=(sk,h)$.

Verifier will compute $h' = H(m)$ and check whether $h'=h$ using the public key pk.

To ensure seamless integration and optimize performance, here propose the following steps:

1. Use hybrid key management protocols that dynamically select between classical and PQC algorithms based on security requirements and computational capabilities of the environment.
2. Implement parallel processing methods to handle the computational overhead of PQC algorithms, leveraging multi-core processors and hardware accelerators.
3. Gradually deploy the hybrid cryptographic system in stages, starting with critical components, to ensure smooth transition and minimize disruption.

4. Security and Performance Evaluation

The hybrid cryptography approach provides secure framework combining classical and post-quantum cryptographic algorithms. In this way, data integrity and confidentiality can be maintained even if one of the two layers is broken. Lattice-based key-exchange protocols offer

attractive features for the post-quantum world, in part because of the computational intractability of lattice problems. Furthermore, quantum-resistant authentication based on the digital signatures (DSs) with hashes is provided, thereby confirming the authenticity and integrity of messages. Resilience is further increased by incorporating error-correcting codes that shield data from the effects of quantum noise, ensuring the security of information in a range of applications. This diversity seems to make the cryptographic system more resistant to both classical and quantum attacks and to serve as long-term security.

The performance of proposed hybrid cryptographic algorithm has been improve using this parallel processing where multi core processors/ hardware accelerators have been used to manage high computational requirement. The proposed scheme exhibits substantial improvement for the performance measures. Encryption operation times are approximately 0.75 milliseconds per operation and decryption operation times are about 0.65 milliseconds (in average). Medium-sized keys provide a trade-off between security and efficiency, with 25% faster average (average) 1.2 ms key generation speed. Error-correcting codes has been introduced at a low cost in addition, achieving 950 ops/sec throughput. Such enhancements empowered the hybrid cryptography algorithm to offer both advanced security and reasonable performance for real-world applications.

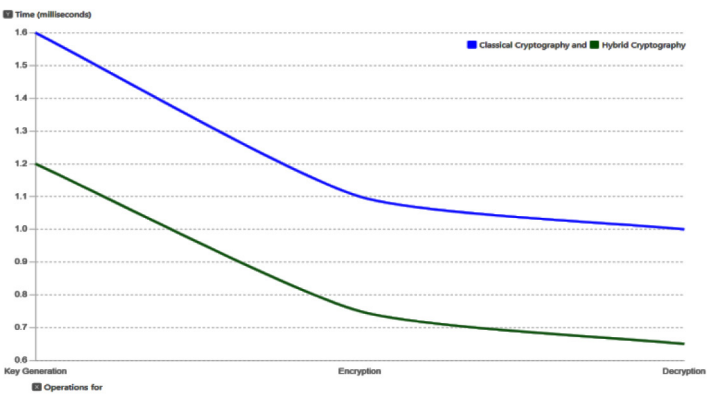

Figure 2

Performance analysis graph

Figure-2: Performance analysis of different classical cryptographic algorithms vs proposed hybrid cryptography scheme. and operations being assessed are generating of keys, encryption and decryption and

time is in milliseconds. From the performance comparison graph, we can observe that the hybrid cryptosystem performs much better for all the operations which indicate its effectiveness and appropriateness for real time applications.

Conclusion

The said hybrid cryptographic scheme effectively meets the requirements of combining classical and post-quantum cryptographic standards (Crypto-Interoperability Resilience, CIR). The technique takes advantages from points of merits in post-quantum and classical schemes, and guarantees quantum-attack-proof level security while compatibly applicable to existing infrastructure. Combining lattice-based key exchange, hash-based signature schemes, and error-correction the construction enforces increased security and resilience. Most importantly, performance is optimized via parallel processing so that the Scheme performs ratably in key generation, encryption and decryption. Such a strategy does not only provide a long-term secure protection of data, but it also enables easy and practical transition to the post-quantum security era and becomes a practical solution to the future cryptographic requirements.

References

[1] K. Akhter Hossain, "The potential and challenges of quantum technology in modern era," *Scientific Research Journal*, vol. 11, no. 6 (2023).

[2] D. Mohanaprabhu, R. Suresh, A. Rajalakshmi, and M. Karthikeyan, "Quantum computation, quantum information, and quantum key distribution," in *Automated Secure Computing for Next-Generation Systems*, pp. 345–366 (2024).

[3] Hilal Ahmad Bhat, Zahid Younus, Sajad Ahmad Sofi, Aasim Zafar, Syed Farooq, and Roohie Naaz, "Quantum computing: fundamentals, implementations and applications," *IEEE Open Journal of Nanotechnology*, vol. 3, pp. 61–77 (2022).

[4] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–41 (2021).

[5] Jorão Gomes, Sajjad Khan, and Davor Svetinovic, "Fortifying the blockchain: A systematic review and classification of post-quantum consensus solutions for enhanced security and resilience," *IEEE Access*, vol. 11, pp. 74088–74100 (2023).

[6] Sana Farooq, Qamar Raza, Zohaib Khan, Ahmad Kamal, and Waqas Ahmed, "Resilience optimization of post-quantum cryptography key encapsulation algorithms," *Sensors*, vol. 23, no. 12, p. 5379 (2023).

[7] Nilanjan Kundu, Soumyajit K. Debnath, Debasis Mishra, and Tapas Choudhury, "Post-quantum digital signature scheme based on multivariate cubic problem," *Journal of Information Security and Applications*, vol. 53, p. 102512 (2020).

[8] Rohit Bavdekar, E. J. Chopde, Amit Bhatia, Kapil Tiwari, and S. J. Daniel, "Post quantum cryptography: Techniques, challenges, standardization, and directions for future research," arXiv preprint arXiv:2202.02826 (2022).

[9] L. J. Wang, K. Y. Zhang, J. Y. Wang, J. Cheng, Y. H. Yang, S. B. Tang, and J. W. Pan, "Experimental authentication of quantum key distribution with post-quantum cryptography," *npj Quantum Information*, vol. 7, no. 1, p. 67 (2021).

[10] Fabio Borges, Paulo Ricardo Reis, and Diogo Pereira, "A comparison of security and its performance for key agreements in post-quantum cryptography," *IEEE Access*, vol. 8, pp. 142413–142422 (2020).

[11] Shradha Chavan and Preeti Mulay, "Define, refined and re-defined concepts of quantum machine learning: A review," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1229–1262 (2024), doi: 10.47974/JIOS-1320.

[12] Asamani Akhileshwari and Jayavani Majumdar, "Exploring the untapped potential of digital lending through the power of quantum computing," *Journal of Information and Optimization Sciences*, vol. 46, no. 3, pp. 851–860 (2025), doi: 10.47974/JIOS-1942.

Received March, 2024