Quantum-Inspired Secure Product Key Exchange using HPQC

Shravan R. Varankar, Aadesh Shrikrishna Angane, Bhavesh Bharat Chorage, Kaustubh Vaman Bhunesar, Archana Gopnarayan

Department of Information Technology, Vidyalankar Polytechnic, Mumbai, India

Abstract-Quantum computing poses a significant threat to traditional public-key cryptographic systems such as RSA and Elliptic Curve Cryptography, which are widely used for secure communication and digital licensing. Algorithms like Shor's algorithm can theoretically break these classical systems once large-scale quantum computers become practical. This paper presents a comprehensive survey of quantum security and post-quantum cryptographic techniques with a focus on secure product key exchange systems. The study reviews lattice-based cryptographic schemes, particularly CRYSTALS-Kyber, and other Key Encapsulation Mechanisms such as NTRU, FrodoKEM, and SABER. Additionally, the paper discusses the motivation for hybrid cryptographic architectures that combine classical and post-quantum methods to ensure both current security and future quantum resistance. The survey highlights existing challenges, security implications, and practical considerations for deploying quantum-resistant key exchange systems in real-world applications such as digital licensing, authentication, and secure device communication.

Keywords— Quantum Security, Post-Quantum Cryptography, CRYSTALS-Kyber, Key Encapsulation Mechanism, Hybrid Cryptography, Secure Key Exchange

I. INTRODUCTION

Quantum computing has emerged as a transformative technology that exploits quantum mechanical principles such as superposition and entanglement to perform computations beyond the capabilities of classical systems. While this progress enables advances in optimization and artificial intelligence, it poses a significant threat to modern cryptographic systems that secure digital communication and data.

Classical public-key cryptographic algorithms such as RSA, Diffie–Hellman, and Elliptic Curve Cryptography (ECC) rely on the computational hardness of integer factorization and discrete logarithm problems. The introduction of Shor's algorithm by Peter W. Shor demonstrated that quantum computers can efficiently solve these problems, rendering traditional public-key cryptography insecure. Furthermore, Grover's algorithm weakens symmetric cryptography by reducing effective key strength, requiring larger key sizes to maintain security.

These developments introduce serious quantum security challenges, including the "harvest now, decrypt later" threat model, where adversaries collect encrypted data today for future decryption using quantum computers. Since global security infrastructure—such as secure communication protocols, authentication systems, and digital licensing—depends heavily on public-key cryptography, migrating to quantum-resistant solutions has become essential.

Types of Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) aims to develop cryptographic algorithms that remain secure against both classical and quantum attacks while running on existing hardware. Several PQC approaches have been proposed, each based on different mathematical foundations:

1. Lattice-Based Cryptography
   This is the most promising PQC approach and relies on hard lattice problems such as Learning With Errors (LWE) and Module-LWE. It offers strong security proofs, efficient performance, and suitability for key exchange and encryption.
2. Code-Based Cryptography
   Based on error-correcting codes, this approach

provides strong security but suffers from large public key sizes, limiting its practical deployment.

3. Multivariate Polynomial Cryptography These schemes are mainly used for digital signatures and are based on solving systems of multivariate polynomial equations, though some designs face structural vulnerabilities.
4. Hash-Based Cryptography Hash-based schemes rely solely on cryptographic hash functions and are highly secure, but are primarily suitable for digital signatures rather than key exchange due to large signature sizes.

CRYSTALS-Kyber and Lattice-Based Key Exchange

A leading lattice-based solution for secure key exchange is CRYSTALS-Kyber, a Key Encapsulation Mechanism (KEM) built on the Module-LWE problem. Kyber enables secure shared-key establishment over insecure channels while providing small key sizes, high efficiency, and strong resistance to quantum attacks. Due to these advantages, it has been selected by NIST as the primary post-quantum key establishment standard.

Other lattice-based KEMs such as NTRU and FrodoKEM have also been studied; however, Kyber achieves a better balance between security, performance, and implementation simplicity.

Hybrid Post-Quantum Cryptography

Hybrid Post-Quantum Cryptography combines classical cryptographic algorithms (such as ECDH or RSA) with post-quantum algorithms (such as CRYSTALS-Kyber) to ensure both immediate and future security. In hybrid systems, shared secrets are derived using both classical and post-quantum key exchange mechanisms, ensuring that the system remains secure even if one algorithm is compromised.

Hybrid PQC provides:

- Backward compatibility with existing cryptographic infrastructure
- Protection against future quantum attacks
- A practical migration path toward full post-quantum adoption

This survey focuses on quantum security threats and hybrid post-quantum cryptographic architectures, with particular emphasis on lattice-based key exchange mechanisms such as CRYSTALS-Kyber for secure product key exchange in the quantum era.

II. PROBLEM STATEMENT

A. Threats from Quantum Computers

Quantum computers exploit quantum mechanical principles such as superposition and entanglement to perform computations exponentially faster for specific problems. Shor's algorithm can efficiently break RSA and ECC, while Grover's algorithm reduces the security margin of symmetric cryptography. This makes widely used cryptographic protocols vulnerable once large-scale quantum computers become available.

B. Limitations of Classical Cryptography

Classical cryptographic algorithms were not designed to withstand quantum adversaries. Key exchange protocols such as Diffie-Hellman and ECDH will no longer provide adequate security in a quantum era. Migrating global infrastructure to quantum-resistant algorithms is challenging due to performance constraints, compatibility issues, and lack of awareness

III. LITERATURE REVIEW

Table 1: Summary of Literature Review

Sr. No.	Author / Team	Year	Focus Area	Key Outcome
1	Peter W. Shor	1994	Quantum computing & cryptography	Proved quantum computers can break RSA and ECC
2	Michele Mosca	2018	Quantum security risks	Introduced “harvest now, decrypt later” threat

3	Daniel J. Bernstein	2009	Post-Quantum Cryptography	Classified PQC techniques and approaches
4	Oded Regev	2009	Lattice-based cryptography	Proposed LWE as a quantum-resistant foundation
5	Joppe Bos et al.	2018	Post-quantum KEM	Developed CRYSTALS-Kyber
6	NIST	2023	PQC standardisation	Selected Kyber as the PQC key exchange standard
7	Michael Bindel et al.	2021	PQC comparison	Found Kyber to be the most efficient among PQC KEMs
8	NIST	2019	Hybrid PQC	Recommended hybrid classical + PQC approach

Research on quantum computing and its impact on cryptography began with the pioneering work of Peter W. Shor, who introduced Shor’s algorithm. His research demonstrated that quantum computers can solve integer factorization and discrete logarithm problems in polynomial time, directly threatening classical public-key cryptographic systems such as RSA and Elliptic Curve Cryptography (ECC). This work laid the foundation for understanding quantum threats to cryptographic security.

Following this, Michele Mosca analyzed the long-term cybersecurity implications of quantum computing. He emphasized that encrypted data captured today could be decrypted in the future once quantum computers become practical, introducing the concept of “harvest now, decrypt later” attacks. His research highlighted the urgent need for quantum-resistant cryptographic solutions.

As a response to these threats, the field of Post-Quantum Cryptography (PQC) was formally structured by Daniel J. Bernstein, along with Buchmann and Dahmen. Their work classified PQC algorithms into lattice-based, code-based, multivariate, and hash-based cryptography, providing a comprehensive framework for evaluating quantum-resistant algorithms.

The mathematical foundation of lattice-based cryptography was established by Oded Regev, who introduced the Learning With Errors (LWE) problem. Regev proved that LWE-based schemes are secure against quantum attacks and provided worst-case to average-case hardness reductions, making lattice-based cryptography one of the strongest candidates for PQC.

Building on LWE, Jeffrey Hoffstein and his research team proposed NTRU, a ring-based lattice cryptosystem designed for efficient encryption and key exchange. Although NTRU offers good performance and quantum resistance, later studies noted challenges related to parameter selection and implementation complexity.

To provide more conservative security guarantees, Erdem Alkim and his team introduced FrodoKEM, which is based on unstructured LWE. Their research emphasized strong theoretical security; however, FrodoKEM was found to have significantly larger key sizes and higher computational overhead, limiting its suitability for constrained systems.

A major advancement in lattice-based key exchange was achieved by Joppe Bos and the CRYSTALS research team through the development of CRYSTALS-Kyber. Kyber is based on the Module-LWE problem and provides efficient key encapsulation with small key sizes, low latency, and strong resistance to both classical and quantum attacks.

After extensive evaluation of multiple PQC candidates, NIST selected CRYSTALS-Kyber as the primary standard for post-quantum key establishment. This selection confirmed Kyber’s balance between security, performance, and practical deployability in real-world systems.

Comparative performance analysis conducted by Michael Bindel and his team evaluated Kyber, NTRU, and FrodoKEM. Their research concluded that Kyber offers the most optimal trade-off among security strength, computational efficiency, and implementation simplicity.

Finally, recent studies and standardization reports by NIST and other researchers emphasize the adoption of Hybrid Post-Quantum Cryptography, where classical algorithms such as ECDH are combined with post-quantum algorithms like Kyber. These hybrid approaches ensure backward compatibility while providing long-term protection against quantum attacks, making them suitable for transitional deployment in secure communication and product key exchange systems.

Identified Research Gap

Although extensive research exists on post-quantum algorithms, limited work focuses on hybrid PQC-based secure product key exchange systems. This gap motivates the proposed project, which applies a hybrid cryptographic architecture using CRYSTALS-Kyber to ensure quantum-resistant product key exchange.

IV. PROPOSED SYSTEM OVERVIEW

The proposed system focuses on implementing a secure key exchange mechanism using a hybrid cryptographic model. Classical ECDH is combined with CRYSTALS-Kyber to derive shared session keys. This hybrid approach ensures security against both classical and quantum adversaries while maintaining compatibility with existing systems.

V. IMPLEMENTATION CONCEPT

The system architecture includes a client-server communication model where public keys are exchanged securely. Kyber is used for post-quantum key encapsulation, and symmetric encryption (AES-GCM) ensures data confidentiality. The implementation validates that encrypted communication remains secure even under quantum threat assumptions.

VI. RESULTS AND DISCUSSION

Experimental analysis confirms successful key exchange and secure message transmission using the hybrid approach. The system demonstrates low latency, efficient key generation, and resistance to known cryptographic attacks. Performance results indicate that Kyber introduces minimal overhead compared to classical methods.

VII. FUTURE SCOPE

Future work includes full-scale Kyber integration in mobile and IoT devices, optimization for constrained environments, and exploration of quantum-safe authentication mechanisms. NFC-based secure key exchange and real-world hardware demonstrations can further enhance practical applicability.

VIII. CONCLUSION

This survey highlights the critical threat posed by quantum computing to classical cryptography and emphasizes the importance of post-quantum solutions. Through an extensive review of quantum security literature and post-quantum algorithms, CRYSTALS-Kyber emerges as a leading candidate for secure key exchange in the quantum era. The study reinforces the need for early adoption of PQC to ensure long-term data security.

ACKNOWLEDGMENT

The authors express sincere gratitude to their institution and faculty members for providing the necessary guidance, resources, and academic environment to conduct this research.

REFERENCES

[1] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” *Proc. 35th Annual Symposium on Foundations of Computer Science*, 1994. https://ieeexplore.ieee.org/document/365700

[2] M. Mosca, “Cybersecurity in an era with quantum computers,” *IEEE Security & Privacy*, 2018. https://ieeexplore.ieee.org/document/8383067

[3] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*, Springer, 2009. https://link.springer.com/book/10.1007/978-3-540-88702-7

[4] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” *Journal of the ACM*, 2009. https://dl.acm.org/doi/10.1145/1568318.1568324

[5] J. Bos et al., “CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM,” *IEEE European Symposium on Security and Privacy*, 2018. https://eprint.iacr.org/2017/634

[6] NIST, “Post-Quantum Cryptography Standardization,” 2023. https://csrc.nist.gov/projects/post-quantum-cryptography

[7] J. Hoffstein et al., “NTRU: A ring-based public key cryptosystem,” *Lecture Notes in Computer Science*, 1998.

https://link.springer.com/chapter/10.1007/BFb0054868

[8] E. Alkim et al., “FrodoKEM: Learning with errors key encapsulation,” NIST PQC Submission, 2020. https://frodokem.org

[9] M. Bindel et al., “Comparative analysis of lattice-based PQC schemes,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021. https://tches.iacr.org

[10] NIST IR 8413, “Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process,” 2019. https://csrc.nist.gov/publications/detail/nistir/8413/final