Hybrid Post-Quantum and Classical Cryptography Library Analysis

Ishanvi M H[1], R Kshamaa Rajoop[2], Harshada G[3], and Keerthi G S[4]
[1,2,3]*Student, Dept. of CSE (IoT & Cyber Security Including Blockchain Technology), Bangalore Institute of Technology, Bengaluru-560004, India*
[4]*Assistant Professor, Dept. of CSE (IoT & Cyber Security Including Blockchain Technology), Bangalore Institute of Technology, Bengaluru-560004, India*

***Abstract*—The rapid advancement of quantum computing poses a serious threat to existing public-key cryptographic systems, particularly RSA and Elliptic Curve Cryptography (ECC), which form the backbone of secure communications. This survey examines the growing need for quantum-resistant cryptographic solutions by reviewing hybrid cryptographic approaches that combine classical key exchange mechanisms, such as ECDH using X25519, with post-quantum Key Encapsulation Mechanisms, notably ML-KEM (Kyber-768). The survey analyzes dual-secret derivation techniques in which independent secrets from classical and post-quantum primitives are combined using HKDF with strong context binding to ensure security even if one component is compromised. Finally, the survey summarizes reported performance trade-offs, highlighting modest handshake overheads and low key-derivation latency, and positions hybrid cryptography as a practical and defense-in-depth solution during the transition to post-quantum cryptographic standards.**

***Index Terms*—Post-Quantum Cryptography, Hybrid Cryptography, ML-KEM (Kyber), X25519, Quantum-Resistant Security**

I. INTRODUCTION

Cryptographic protocols underpin secure modern communications by relying on hard mathematical problems such as integer factorization and discrete logarithms. While RSA and elliptic-curve schemes have remained secure against classical attacks for decades, the emergence of quantum computing fundamentally threatens them. Shor's algorithm shows that sufficiently powerful quantum computers can efficiently break these systems, leading to "harvest now, decrypt later" risks for sensitive data with long-term confidentiality needs. This threat has created an urgent demand for cryptographic mechanisms that remain secure against both classical and quantum adversaries, motivating the development of post-quantum cryptography.

In response, NIST initiated a global post-quantum cryptography standardization effort, resulting in the selection of lattice-based algorithms such as ML-KEM (CRYSTALS-Kyber) for key encapsulation and ML-DSA (Dilithium) for digital signatures. ML-KEM is based on the Module Learning With Errors problem and is believed to resist both classical and quantum attacks, with ML-KEM-768 offering strong security. However, transitioning entirely to post-quantum cryptography faces challenges, including limited implementation maturity, interoperability with existing infrastructure, regulatory constraints, and the risk of unforeseen cryptanalytic advances.

Hybrid cryptography addresses these challenges by combining classical and post-quantum primitives, ensuring security if either component remains uncompromised while maintaining backward compatibility and operational flexibility.

II. LITERATURE SURVEY

[1] FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard

The National Institute of Standards and Technology (NIST) specifies ML-KEM as a post-quantum key-encapsulation mechanism whose security is based on the computational hardness of the Module Learning With Errors (MLWE) problem [1]. The standard is designed to resist attacks from both classical and

quantum adversaries. FIPS 203 defines three parameter sets—ML-KEM-512, ML-KEM-768, and ML-KEM-1024—offering increasing security at the cost of reduced performance. The specification allows mathematically equivalent implementations provided correctness is preserved and mandates compliance with other NIST-approved cryptographic algorithms for protecting sensitive federal information.

[2] CRYSTALS-Kyber
CRYSTALS-Kyber is a lattice-based key-encapsulation mechanism whose security relies on the MLWE problem [2]. The construction transforms an IND-CPA-secure public-key encryption scheme into an IND-CCA2-secure KEM using a modified Fujisaki–Okamoto transform. Version 3.0 strengthens Kyber512 by increasing the binomial noise parameter, achieving approximately 118-bit Core-SVP hardness under a weak Learning-with-Rounding assumption. Ciphertext compression was reduced to mitigate decryption failures, resulting in a ciphertext size of 768 bytes and a failure probability of 2^{-139}. Kyber employs an "against-all-authority" design by regenerating the public matrix from a fresh random seed for each key pair.

[3] CRYSTALS-Dilithium
CRYSTALS-Dilithium is a post-quantum digital signature scheme based on the hardness of the MLWE and MSIS problems [3]. The scheme follows the Fiat–Shamir with Aborts paradigm and uses uniform sampling to avoid side-channel vulnerabilities associated with discrete Gaussian sampling. Although this work focuses on key exchange, Dilithium is relevant for future integration of post-quantum authentication mechanisms in hybrid handshake protocols.

[4] Post-Quantum Key Exchange and Open Quantum Safe
Stebila and Mosca analyze the threat posed by quantum computing to RSA and elliptic curve cryptography due to Shor's algorithm [4]. They identify lattice-based key exchange schemes based on LWE and Ring-LWE as promising alternatives and discuss practical deployments using hybrid TLS ciphersuites. The Open Quantum Safe paper is introduced to facilitate experimentation and adoption of post-quantum algorithms in real-world protocols.

[5] Hybrid Post-Quantum Key Exchange for TLS
Campagna *et al.* propose hybrid key encapsulation mechanisms for TLS 1.2 that combine classical ECDHE with post-quantum KEMs such as Kyber, BIKE, or SIKE [5]. The resulting premaster secret is derived from both exchanges, ensuring security against classical and quantum adversaries. The draft introduces new hybrid cipher suites and handshake extensions and is intended for experimental deployment.

[6] KEM Combiners
Giacon *et al.* introduce KEM combiners that produce a CCA-secure KEM as long as at least one component KEM remains secure [6]. These black-box constructions provide strong resilience guarantees and are particularly relevant for hybrid classical–post-quantum deployments.

[7] Hybrid Signatures and PKI Transition
Bindel *et al.* examine hybrid digital signature schemes as a method for transitioning existing public key infrastructures to post-quantum security [7]. The work analyzes security models, integration into standards such as X.509 and TLS, and highlights implementation challenges arising from increased certificate sizes.

[8] Side-Channel Attacks on Lattice-Based Schemes
Catinca *et al.* demonstrate correlation power analysis attacks against lattice-based post-quantum KEMs, including Kyber, Saber, and NTRU-KEM [8]. Their results show that naive implementations are vulnerable and emphasize the necessity of constant-time implementations. This work highlights that implementation security is as critical as mathematical hardness when deploying post-quantum cryptography in real-world systems.

[9] Hybrid Key Exchange in IKE
RFC 9370 specifies mechanisms for hybrid classical and post-quantum key exchange in IKEv2, introducing the IKE_ INTERMEDIATE exchange to support multiple key exchanges and large payloads [9]. The final shared secret incorporates all exchanged secrets, ensuring post-quantum security.

[10] Performance of Post-Quantum KEMs
Gustafsson and Stensson evaluate the performance of post-quantum KEMs across consumer, cloud, and mainframe platforms [10]. Their results show significant overhead compared to classical algorithms, while highlighting the benefits of hardware acceleration such as AVX, FPGAs, and cryptographic coprocessors.

[11] Advances in Lattice Algorithms
Ducas and van Woerden present efficient algorithms for solving the closest vector problem in lattices relevant to post-quantum cryptography [11]. These results support parameter optimization and validate security margins of lattice-based schemes.

[12] State of the Art in Post-Quantum Cryptography
Johannes *et al.* provide a comprehensive survey of post-quantum cryptography, categorizing hash-based, lattice-based, and code-based approaches and discussing their security foundations in the presence of quantum adversaries [12].

The literature highlights the growing urgency of post-quantum cryptography as a response to quantum threats against RSA and elliptic-curve systems. NIST's standardization of lattice-based schemes such as ML-KEM (CRYSTALS-Kyber) and ML-DSA (Dilithium) establishes a strong foundation for quantum-resistant key exchange and digital signatures, with security rooted in the hardness of lattice problems like MLWE and MSIS. Prior research emphasizes hybrid approaches that combine classical and post-quantum key exchanges in protocols such as TLS and IKE, ensuring security as long as at least one component remains secure. Studies on KEM combiners further formalize this "at-least-one-secure" guarantee, while work on hybrid signatures addresses challenges in transitioning public key infrastructures. At the same time, side-channel analyses reveal that secure implementation practices, such as constant-time execution, are critical for real-world deployment. Performance evaluations demonstrate notable overheads for post-quantum schemes, motivating optimization and hardware acceleration. Overall, existing surveys and experimental deployments collectively position hybrid post-quantum cryptography as a practical and resilient path toward quantum-safe communication systems.

III. CONCLUSION

This survey has examined the growing impact of quantum computing on modern cryptographic systems and highlighted the necessity of transitioning toward quantum-resistant security mechanisms. While post-quantum algorithms such as ML-KEM and ML-DSA provide strong theoretical resistance to quantum attacks, practical deployment challenges related to performance, interoperability, implementation maturity, and regulatory constraints remain significant. Hybrid cryptographic approaches emerge as a pragmatic and robust solution by combining classical and post-quantum primitives to provide defense-in-depth and cryptographic agility during the transition period. The reviewed literature demonstrates that hybrid key exchange mechanisms, supported by secure KEM combiners and careful implementation practices, can maintain security even if one component is compromised. Overall, hybrid post-quantum cryptography represents a viable and resilient pathway for securing communications in the pre- and post-quantum era while allowing gradual adoption of emerging standards.

REFERENCES

[1] National Institute of Standards and Technology, FIPS 203: "Module-Lattice-Based Key Encapsulation Mechanism Standard", U.S. Department of Commerce, 2024. https://nvlpubs. nist.gov/nistpubs /fips/nist.fips.203.pdf
[2] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, Damien Stehlé, CRYSTALS-Kyber: "Algorithm Specifications and Supporting Documentation, Version 3.0", NIST PQC Paper, 2023. https://pq-crystals.org/kyber/data/kyber-specification-round3.pdf
[3] Shi Bai, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé, CRYSTALS-Dilithium: "Algorithm Specifications and Supporting Documentation", Version 3.01, NIST PQC Paper, 2023. https://pq-crystals.org /dilithium/data /dilithium -specification-round3.pdf
[4] Douglas Stebila and Michele Mosca, "Post-Quantum Key Exchange for the Internet and the

Open Quantum Safe Project", in Selected Areas in Cryptography (SAC), 2016. https://eprint.iacr. org/ 2016/1017

[5] M. Campagna, E. Crockett, "Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS)", IETF Internet-Draft, 2024. https://www. ietf.org /archive/id/draft-campagna-tls-bike-sike-hybrid-07.html

[6] Federico Giacon, Felix Heuer, and Bertram Poettering, "KEM Combiners", Journal of Cryptology, vol. 36, no. 4, 2023. https://eprint. iacr. org/2018/024

[7] Nina Bindel, Udyani Herath, Matthew McKague, and Douglas Stebila, "Transitioning to a Quantum-Resistant Public Key Infrastructure", in PQCrypto, 2017. https://eprint.iacr.org /2017/460

[8] Catinca Mujdei, Arthur Beckers, Jose Maria Bermudo Mera, Angshuman Karmakar, Lennert Wouters, and Ingrid Verbauwhede, "Side-Channel Analysis of Lattice-Based Post-Quantum Cryptography: Exploiting Polynomial Multiplication", IEEE Transactions on Computers, vol. 72, no. 5, 2023. https://eprint. iacr.org/2022/474

[9] CJ. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van Geest, O. Garcia-Morchon, V. Smyslov, Internet Engineering Task Force, RFC 9370: "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)", 2024. https://www.rfc-editor.org/rfc/rfc9370.html

[10] Alex Gustafsson and Carl Stensson, "The Performance of Post-Quantum Key Encapsulation Mechanisms: A Study on Consumer, Cloud and Mainframe Hardware", Master's Thesis, Blekinge Institute of Technology, 2021. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1574260

[11] Léo Ducas and Wessel P. J. van Woerden, "The closest vector problem in tensored root lattices of type A and in their duals", IACR ePrint Report 2016/910. https://eprint.iacr.org/2016/910

[12] Johannes A. Buchmann, Denis Butin, Florian Göpfert, Albrecht Petzoldt, "Post-Quantum Cryptography: State of the Art" https://amphawa. eu/ data/Post-Quantum_ Cryptography_ State_ of_theArt. pdf