International Journal for Rapid Research in Engineering Technology & Applied Science (IJRRETAS)

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume 11 issue 07 July 2025 OPEN ACCESS E-ISSN: 2455-4723 Impact Factor 7.95

Resource-Aware Post-Quantum Hybrid Key Establishment with Forward-Secure Session Management

Seema Agrawal[1], Rahul Kumar[2]

[1,2]Department of Mathematics, S.S.V. (P.G.) College, Hapur, Chaudhary Charan Singh University, Meerut, Uttar Pradesh, India

[1,2] seemagrwl7@gmail.com, ujjwalrahul@gmail.com

Abstract

The transition to post-quantum cryptography (PQC) has become an immediate systems-engineering requirement because classical public-key mechanisms based on integer factorization and elliptic-curve discrete logarithms are vulnerable to sufficiently capable quantum computers. The harvest-now-decrypt-later threat further increases the urgency for long-lived confidential information. At the same time, post-quantum mechanisms introduce larger communication objects and different computational and memory requirements, making direct replacement difficult in heterogeneous and resource-constrained environments. This paper proposes a resource-aware hybrid key-establishment and session-management framework based entirely on established cryptographic primitives. The framework combines ephemeral X25519 with ML-KEM-768, binds the resulting secrets to the protocol transcript through a domain-separated HKDF-based key-combination procedure, and introduces a policy layer that selects rekey intervals according to measured resource conditions and application sensitivity. The work deliberately does not claim novelty for the X25519/ML-KEM combination itself; hybrid ECDHE-MLKEM key agreement was already being standardized in the IETF in 2024–early 2025. The research contribution is instead the experimentally testable resource-aware session-management layer. A precise threat model, protocol description, security rationale, overhead model, and reproducible evaluation methodology are provided. The manuscript does not fabricate experimental measurements; numerical results are to be obtained from the proposed implementation before submission as an empirical article.

Keywords: post-quantum cryptography; ML-KEM; X25519; hybrid key establishment; forward secrecy; TLS 1.3; cryptographic agility; IoT; resource-aware security.

1. Introduction

Public-key cryptography is a core component of secure Internet communication, cloud services, healthcare systems, industrial networks, financial applications, and the Internet of Things (IoT). Classical systems such as RSA and elliptic-curve cryptography rely on mathematical problems that are believed to be difficult for classical computers. Shor's algorithm demonstrates that sufficiently capable quantum computers would solve integer factorization and discrete logarithm problems in polynomial time, threatening widely deployed public-key mechanisms.

The risk is not limited to the time at which a cryptographically relevant quantum computer becomes available. Adversaries can collect encrypted traffic today and attempt decryption later,

making long-lived information particularly exposed. This motivates migration toward post-quantum mechanisms whose security is based on problems for which efficient quantum attacks are not currently known.

NIST finalized ML-KEM, ML-DSA, and SLH-DSA as FIPS 203, FIPS 204, and FIPS 205 in August 2024. The same year, the IETF published successive Internet-Draft versions defining hybrid TLS 1.3 key-agreement groups including X25519MLKEM768, SecP256r1MLKEM768, and later SecP384r1MLKEM1024. The March 2025 draft explicitly described these groups as combinations of ML-KEM and ECDH for TLS 1.3. Thus, by April 2025, hybrid classical/PQC key establishment was already an active standardization direction rather than an unexplored concept.

Research on PQC in IoT similarly identifies resource constraints as a major deployment issue. Surveys published before May 2025 report that computational cost, memory, communication overhead, and lack of coordinated optimization remain important barriers. Recent work on IoT communication protocols has also begun evaluating PQC integration beyond TLS, including CoAP and MQTT-SN. These observations motivate a research problem focused not on inventing another KEM, but on managing standardized hybrid cryptography efficiently across heterogeneous devices.

2. Research Gap and Contribution

Existing literature has established the feasibility and security rationale of post-quantum and hybrid key establishment, but practical deployment still requires policies for heterogeneous devices and long-lived sessions. A fixed cryptographic configuration and fixed rekey interval can be unnecessarily expensive for constrained devices or unnecessarily conservative for high-resource devices. The gap addressed in this work is therefore resource-aware session management around a standardized hybrid key-establishment mechanism.

The proposed contribution has three elements. First, the framework uses X25519 and ML-KEM-768 as independently generated key-establishment components. Second, their outputs are combined through an explicit transcript-bound, domain-separated KDF interface rather than being used directly as application traffic keys. Third, a resource-aware policy selects a rekey interval from a predefined safe set using device resources, communication conditions, application sensitivity, and session lifetime. The cryptographic algorithms themselves are not modified.

3. Proposed Framework

Let the client and server generate ephemeral X25519 key pairs. Their classical shared secret is denoted by Z_E. In parallel, an ML-KEM-768 exchange generates the post-quantum shared secretZ_Q and the associated ciphertext. Let T denote the authenticated transcript, including negotiated parameters, public shares, ML-KEM ciphertext, identities or authenticated context, and protocol nonces.

$$PRK = HKDF - Extract(salt, Encode(Z_E)||Encode(Z_Q))$$

$$K_0 = HKDF - Expand(PRK, "PQ - HYBRID - SESSION"||H(T), L)$$

International Journal for Rapid Research in Engineering Technology & Applied Science (IJRRETAS)

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume 11 issue 07 July 2025 OPEN ACCESS E-ISSN: 2455-4723 Impact Factor 7.95

The equations define the research abstraction. When instantiated inside TLS 1.3, the implementation must follow the applicable TLS key schedule and the IETF hybrid-group specification rather than replacing the standardized schedule with an ad hoc construction. The important property for the proposed framework is that both component secrets are cryptographically bound to the same session context and that a protocol-specific domain-separation label prevents cross-protocol key reuse.

For session management, let R=(C,M,E,B) denote normalized computational capacity, memory availability, energy budget, and effective bandwidth. Let S represent application sensitivity and L the expected session lifetime. The policy engine selects a rekey interval r from a predefined set R_k subject to security and resource constraints. The selection is made only among approved cryptographic configurations and does not alter the underlying security parameters of ML-KEM.

Table 1. Example resource-aware policy classes.

Class	Security context	Resource condition	Rekey policy
C1	Constrained but standard-risk data	Low/medium resources	Short interval only when affordable
C2	General secure communication	Moderate resources	Moderate interval
C3	Long-lived sensitive information	Higher resources	Shorter interval and stricter monitoring

4. Security Analysis

The adversary is assumed to control the communication network and may observe, record, modify, replay, delay, and inject traffic. A future quantum-capable adversary is also considered. The framework assumes correctly implemented X25519 and ML-KEM, secure random generation, authenticated algorithm negotiation, correct transcript binding, and secure erasure of obsolete traffic secrets.

The hybrid construction is intended to preserve security when at least one component retains the required security property, under the assumptions of the applicable hybrid-combiner and TLS framework. If a future quantum adversary compromises X25519, the ML-KEM contribution remains available under the assumed post-quantum security of ML-KEM. Conversely, compromise of the PQC component alone does not directly reveal the classical contribution. This argument is conditional on correct composition and implementation; it is not a claim that arbitrary concatenation of secrets is automatically secure.

Forward secrecy is obtained from ephemeral key establishment and controlled rekeying with secure deletion. Replay protection is delegated to the authenticated protocol and epoch-specific state. The proposed resource policy does not weaken the underlying primitive; it changes only the timing of session-key refresh within predefined limits.

5. Experimental Methodology

The framework should be evaluated against three baselines: X25519-only; ML-KEM-768-only in a compatible test protocol; and the standardized hybrid X25519MLKEM768. The fourth

configuration is the same hybrid mechanism combined with the proposed resource-aware rekeying policy. Experiments should be conducted on at least one x86-64 system and one ARM-based platform representative of constrained deployment.

For each configuration, measure key-generation time, encapsulation and decapsulation time, handshake completion time, peak memory, bytes transmitted, rekeying overhead, energy per handshake or protected data volume, and sustained throughput. Report median, dispersion, and confidence intervals. Hardware, compiler, library version, operating-system version, CPU frequency policy, and network conditions must be recorded.

The primary hypothesis is that resource-aware rekeying can reduce computational, energy, or communication cost relative to a fixed conservative rekey interval while maintaining a predefined exposure bound. The null hypothesis is that the adaptive policy provides no statistically significant reduction under equivalent security constraints. Statistical analysis should report effect sizes and confidence intervals in addition to significance tests.

6. Discussion and Conclusion

The proposed research direction is intentionally conservative in its cryptographic claims. X25519/ML-KEM hybrid exchange was already described in IETF drafts by 2024 and early 2025, so it should not be presented as a new cryptographic primitive. The research novelty is the resource-aware management layer and its experimentally testable effect on long-lived secure sessions. This distinction is important for an authentic journal submission and avoids overstating novelty.

The framework is particularly relevant to IoT, industrial IoT, healthcare sensors, wireless sensor networks, and other environments in which cryptographic overhead varies substantially across devices. Its principal limitation is that the adaptive policy must be implemented and benchmarked before claims of performance improvement can be made. No experimental values are fabricated in this manuscript. The completed article should report reproducible measurements, statistical analysis, implementation details, and a formal security argument for the exact protocol instantiation.

In conclusion, this paper presents a resource-aware framework for deploying standardized post-quantum hybrid key establishment with controlled forward-secure session management. By treating cryptographic migration as a systems optimization problem rather than merely an algorithm-selection problem, the proposed approach provides a defensible research direction for practical PQC deployment while remaining aligned with the standards and literature available before May 2025.

References

1. National Institute of Standards and Technology, “Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM),” FIPS 203, Aug. 2024, doi: 10.6028/NIST.FIPS.203.
2. National Institute of Standards and Technology, “Module-Lattice-Based Digital Signature Standard (ML-DSA),” FIPS 204, Aug. 2024, doi: 10.6028/NIST.FIPS.204.
3. National Institute of Standards and Technology, “Stateless Hash-Based Digital Signature Standard (SLH-DSA),” FIPS 205, Aug. 2024, doi: 10.6028/NIST.FIPS.205.

4. D. Moody, R. Perlner, A. Regenscheid, A. Robinson, and D. Cooper, "Transition to Post-Quantum Cryptography Standards," NIST IR 8547, 2024.
5. G. Alagic et al., "Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process," NIST IR 8545, 2024.
6. K. Kwiatkowski, P. Kampanakis, B. E. Westerbaan, and D. Stebila, "Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3," Internet-Draft, draft-kwiatkowski-tls-ecdhe-mlkem-01, Aug. 2024.
7. K. Kwiatkowski, P. Kampanakis, B. E. Westerbaan, and D. Stebila, "Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3," Internet-Draft, draft-kwiatkowski-tls-ecdhe-mlkem-02, Sept. 2024.
8. K. Kwiatkowski, P. Kampanakis, B. E. Westerbaan, and D. Stebila, "Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3," Internet-Draft, draft-kwiatkowski-tls-ecdhe-mlkem-03, Dec. 2024.
9. K. Kwiatkowski, P. Kampanakis, B. E. Westerbaan, and D. Stebila, "Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3," Internet-Draft, draft-ietf-tls-ecdhe-mlkem-00, Mar. 2025.
10. E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, IETF, Aug. 2018.
11. A. Langley, M. Hamburg, and S. Turner, "Elliptic Curves for Security," RFC 7748, IETF, Jan. 2016.
12. H. Krawczyk and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)," RFC 5869, IETF, May 2010.
13. E. Barker, L. Chen, and R. Davis, "Recommendation for Key-Derivation Methods in Key-Establishment Schemes," NIST SP 800-56C Rev. 2, Aug. 2020.
14. T. Liu, G. S. Ramachandran, and R. Jurdak, "Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization," arXiv:2401.17538, 2024.
15. S. Kumari, M. Singh, R. Singh, and H. Tewari, "Post-quantum cryptography techniques for secure communication in resource-constrained Internet of Things devices: A comprehensive survey," Software: Practice and Experience, vol. 52, no. 10, pp. 2047–2076, 2022, doi: 10.1002/spe.3121.
16. N. Mishra, S. K. Hafizul Islam, and S. Zeadally, "A survey on security and cryptographic perspective of Industrial-Internet-of-Things," Internet of Things, vol. 25, 101037, 2024, doi: 10.1016/j.iot.2023.101037.
17. P. R. Babu, S. A. P. Kumar, A. G. Reddy, and A. K. Das, "Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges," Computer Science Review, vol. 54, 100676, 2024, doi: 10.1016/j.cosrev.2024.100676.
18. J. R. Jency, B. L. R., E. E. Nithila, C. S. Shibi, and A. Rosi, "A Survey about Post Quantum Cryptography Methods," EAI Endorsed Transactions on Internet of Things, vol. 10, no. 1, 2024, doi: 10.4108/eetiot.5099.
19. "Integrating Post-Quantum Cryptography into CoAP and MQTT-SN Protocols," Proc. IEEE Symposium on Computers and Communications (ISCC), 2024, doi: 10.1109/ISCC61673.2024.10733716.
20. Meta Engineering, "Post-quantum readiness for TLS at Meta," May 2024.
21. Amazon Web Services, "How to tune TLS for hybrid post-quantum cryptography with Kyber," 2022.