International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

RACAF-PQC: A Risk-Aware Crypto-Agility Framework for Post-Quantum Secure Communication with Experimental Validation of Security, Performance and Migration Decisions

[1]Seema Agrawal, [2]Rahul Kumar

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

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

ABSTRACT

The emergence of cryptographically relevant quantum computing presents a fundamental challenge to contemporary public-key cryptography because Shor's algorithm can solve the integer-factorization and discrete-logarithm problems on which widely deployed RSA and elliptic-curve cryptographic systems rely. Although standardized post-quantum cryptographic (PQC) algorithms are now available, migration from classical cryptography to quantum-resistant systems is not a simple algorithm-selection problem. Different applications impose different requirements with respect to security strength, computational cost, communication overhead, interoperability, algorithmic diversity, and crypto-agility. This paper proposes RACAF-PQC, a Risk-Aware Crypto-Agility Framework for post-quantum migration decision-making. The framework introduces a Post-Quantum Migration Readiness Index (PMRI) that integrates six normalized criteria: security adequacy, computational performance, communication efficiency, algorithmic diversity, interoperability, and crypto-agility. Six cryptographic configurations are evaluated across five application scenarios: low-risk web communication, enterprise systems, high-confidentiality systems, constrained Internet-of-Things (IoT) environments, and critical infrastructure. The proposed framework is experimentally validated using a reproducible multi-criteria computational experiment and a 10,000-trial sensitivity analysis. Results show that the framework selects ML-KEM-512 for resource-sensitive environments and an ECDHE+ML-KEM-768 hybrid configuration for enterprise, high-confidentiality, and critical-infrastructure scenarios. Relative to a fixed ML-KEM-768 strategy, RACAF-PQC produces scenario-dependent decision improvements ranging from 0.7% to 8.8%, with a mean improvement of approximately 5.0%. Relative to classical-only migration, the corresponding mean improvement is approximately 42.0%. Sensitivity analysis demonstrates that the principal selections remain stable under perturbation of the decision weights, with selection stability reaching 100% for enterprise systems and 99.42% for critical infrastructure. The results demonstrate that post-quantum migration can be improved by treating cryptographic agility and application-specific risk as explicit decision variables rather than adopting a single universal algorithm. The study provides a mathematically transparent and reproducible framework for PQC migration planning while avoiding unsupported claims of hardware-level performance.

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

Keywords: Post-quantum cryptography; ML-KEM; hybrid cryptography; crypto-agility; migration readiness; multi-criteria decision-making; cybersecurity; quantum-resistant cryptography; risk-aware security.

1. INTRODUCTION

1.1 Background and Motivation

Public-key cryptography forms the foundation of secure communication over the Internet and is extensively used in secure web browsing, electronic transactions, digital signatures, cloud services, distributed systems, industrial control systems, and Internet-of-Things (IoT) applications. Classical public-key mechanisms such as RSA and elliptic-curve cryptography derive their security from mathematical problems that are computationally difficult for conventional computers.

The situation changes fundamentally in the presence of sufficiently capable quantum computers. Shor demonstrated that integer factorization and discrete logarithms can be solved in polynomial time on a quantum computer [1]. Consequently, large-scale quantum computers could undermine RSA, Diffie–Hellman, and elliptic-curve cryptographic systems.

This threat has motivated the development of post-quantum cryptography (PQC), which seeks to construct cryptographic mechanisms resistant to both classical and quantum attacks. The standardization effort led by the National Institute of Standards and Technology (NIST) resulted in the publication of three Federal Information Processing Standards in August 2024: FIPS 203 for ML-KEM, FIPS 204 for ML-DSA, and FIPS 205 for SLH-DSA [2–4].

FIPS 203 specifies ML-KEM as a standardized key-encapsulation mechanism based on the hardness of the Module Learning With Errors problem [2]. FIPS 204 specifies ML-DSA, a lattice-based digital signature scheme [3], while FIPS 205 specifies SLH-DSA, a stateless hash-based digital signature scheme [4].

However, the availability of standardized algorithms does not automatically solve the migration problem. A security administrator must determine which algorithm or combination of algorithms is appropriate for a particular application. A configuration optimized for communication efficiency may not be optimal for a critical infrastructure environment. Similarly, the strongest available parameter set may impose unnecessary computational or communication costs on resource-constrained devices.

The migration problem is therefore inherently multi-dimensional. A practical migration framework should simultaneously consider security against classical and quantum threats; computational requirements; communication overhead; interoperability with existing systems; availability of alternative cryptographic mechanisms; and the ability to replace or combine algorithms as the threat landscape evolves. These requirements motivate the development of RACAF-PQC.

1.2 Research Gap and Contributions

Existing PQC studies have primarily concentrated on algorithm design, cryptanalysis, implementation optimization, benchmarking, and standardization. These studies are essential for establishing the security and practical feasibility of individual algorithms. However,

comparatively less attention has been devoted to the decision problem of selecting an appropriate cryptographic configuration for different operational environments.

The principal contribution of this study is not a new cryptographic primitive. Instead, RACAF-PQC provides a mathematically explicit decision framework for selecting and migrating cryptographic configurations.

The principal contributions are: (1) a risk-aware crypto-agility framework for PQC migration; (2) a Post-Quantum Migration Readiness Index integrating six decision criteria; (3) application-specific weighting for five representative deployment scenarios; (4) a reproducible computational experiment comparing six cryptographic configurations; (5) a 10,000-trial sensitivity analysis; (6) quantitative comparison with fixed ML-KEM-768 and classical-only strategies; and (7) explicit separation of model-based decision validation from hardware-level benchmarking.

2. RELATED WORK AND RESEARCH CONTEXT

2.1 Post-Quantum Cryptography

The fundamental motivation for PQC arises from the vulnerability of public-key systems to quantum algorithms. Shor's algorithm demonstrated that factorization and discrete logarithms become tractable on sufficiently powerful quantum computers [1].

Before NIST standardization, several candidate families were investigated, including lattice-based, code-based, hash-based, multivariate, and isogeny-based constructions. New Hope introduced a lattice-based key-exchange approach based on Ring-LWE assumptions [5]. The CRYSTALS-Kyber family subsequently became one of the most important lattice-based KEM candidates [6]. Kyber's security, efficiency, and practical implementation characteristics contributed to its selection as the basis of ML-KEM. Similarly, CRYSTALS-Dilithium became a major lattice-based signature candidate [7], eventually forming the basis of ML-DSA.

NIST finalized ML-KEM, ML-DSA, and SLH-DSA in 2024 [2–4]. The standardization represents a major transition from experimental PQC research toward practical deployment.

2.2 Standardization and Hybrid Cryptography

The publication of FIPS 203–205 provides organizations with standardized cryptographic mechanisms for post-quantum migration [2–4]. However, migration does not necessarily require immediate abandonment of all classical mechanisms.

Hybrid cryptography combines a classical mechanism with a PQC mechanism. A hybrid construction can provide protection against the failure of either component, subject to the security properties and composition method of the particular protocol. Hybrid key establishment has consequently become an important migration strategy. Research and engineering work around TLS 1.3 has investigated combinations such as X25519 with ML-KEM-768 and elliptic-curve Diffie–Hellman mechanisms combined with ML-KEM [8].

NIST's work on KEM recommendations also emphasizes appropriate key-establishment mechanisms and secure integration into applications and protocols [9]. In March 2025, NIST announced the selection of HQC as an additional algorithm for the fourth round of the PQC

process [10]. HQC is based on error-correcting codes and therefore offers algorithmic diversity relative to lattice-based ML-KEM.

2.3 Research Gap

The literature establishes that quantum computing threatens classical public-key cryptography; PQC algorithms provide quantum-resistant alternatives; hybrid cryptography can support migration; different algorithms have different computational and communication characteristics; and algorithmic diversity can contribute to resilience. However, these properties are often studied independently. RACAF-PQC integrates them into a single decision model and determines which configuration provides the best overall score under a specified operational risk profile.

3. PROPOSED RACAF-PQC FRAMEWORK

3.1 Framework Architecture

RACAF-PQC consists of four logical stages: Input Layer → Security and Performance Assessment → PMRI Computation → Migration Decision. The input layer defines candidate cryptographic configurations and the application scenario. The assessment layer evaluates each candidate according to six normalized criteria: S (Security adequacy), P (Computational performance), B (Communication efficiency), D (Algorithmic diversity), I (Interoperability), and A (Crypto-agility). The normalized values lie between 0 and 1, where larger values represent more desirable properties.

3.2 Post-Quantum Migration Readiness Index

For candidate configuration i, the PMRI is defined as:

$PMRI_i = w_sS_i + w_pP_i + w_\beta B_i + w_D D_i + w_iI_i + w_aA_i$

subject to $w_s + w_p + w_\beta + w_D + w_i + w_a = 1$ and $0 \le S_i, P_i, B_i, D_i, I_i, A_i \le 1$. The selected configuration is $C^* = \arg\max_i PMRI_i$.

3.3 Candidate Configurations

ID	Configuration
C1	Classical ECDHE
C2	ML-KEM-512
C3	ML-KEM-768
C4	ML-KEM-1024
C5	ECDHE + ML-KEM-768 Hybrid
C6	ML-KEM-768 + HQC diversified configuration

Configuration	S	P	B	D	I	A
Classical ECDHE	.20	1.00	1.00	.10	1.00	.35
ML-KEM-512	.75	.92	.80	.55	.70	.80
ML-KEM-768	.90	.82	.65	.55	.78	.85
ML-KEM-1024	1.00	.70	.45	.55	.70	.85
ECDHE + ML-	.97	.72	.45	.75	.92	.90

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

KEM-768						
ML-KEM-768 + HQC	1.00	.55	.35	1.00	.55	.88

These numerical values are experimental decision-model inputs rather than official NIST security scores.

3.4 RACAF Decision Algorithm

The computational process is: define candidate configurations; normalize the six criteria; define application-specific weights; calculate PMRI for every candidate; rank the candidates; select the configuration with maximum PMRI; perturb the weights repeatedly to determine decision stability; and report the selected configuration and sensitivity statistics. This makes the decision process reproducible and transparent.

4. EXPERIMENTAL METHODOLOGY AND RESULTS

4.1 Experimental Design

Five representative application scenarios were defined: low-risk web communication, enterprise systems, high-confidentiality systems, constrained IoT environments, and critical infrastructure. Each scenario uses a different set of weights.

Scenario	S	P	B	D	I	A
Low-risk Web	.15	.25	.25	.05	.20	.10
Enterprise	.25	.15	.15	.15	.25	.05
High Confidentiality	.35	.05	.10	.20	.15	.15
Constrained IoT	.25	.20	.25	.10	.15	.05
Critical Infrastructure	.35	.10	.10	.20	.15	.10

4.2 PMRI Results

Scenario	ECDHE	ML-KEM-512	ML-KEM-768	ML-KEM-1024	Hybrid	ML-KEM-768 + HQC
Low-risk Web	.770	0.790	0.771	.690	.750	.623
Enterprise	.632	.743	.766	.722	0.806	.716
High Confidentiality	.442	.724	.776	.772	0.844	.827
Constrained IoT	.678	.772	.766	.705	.757	.674
Critical Infrastructure	.475	.730	.774	.765	.834	.810

The results demonstrate that no single configuration is optimal across all scenarios. ML-KEM-512 produces the highest PMRI for low-risk web and constrained-IoT environments.

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

The hybrid configuration produces the highest PMRI for enterprise, high-confidentiality, and critical-infrastructure scenarios.

4.3 Comparative Analysis

Relative to fixed ML-KEM-768, the improvement is calculated as $G_{768} = (PMRI_R ACAF - PMRI_{768})/PMRI_{768} \times 100$.

Scenario	RACAF Selection	Improvement over ML-KEM-768
Low-risk Web	ML-KEM-512	2.5%
Enterprise	Hybrid	5.2%
High Confidentiality	Hybrid	8.8%
Constrained IoT	ML-KEM-512	0.7%
Critical Infrastructure	Hybrid	7.8%

The mean improvement is approximately 5.0%.

Relative to classical-only ECDHE, the improvement is $G_classical = (PMRI_R ACAF - PMRI_E CDHE)/PMRI_E CDHE \times 100$.

Scenario	Improvement over Classical ECDHE
Low-risk Web	2.6%
Enterprise	27.4%
High Confidentiality	90.6%
Constrained IoT	13.9%
Critical Infrastructure	75.7%

The mean improvement is approximately 42.0%.

4.4 Communication Overhead and Sensitivity

Parameter set	Public key	Ciphertext	Combined size
ML-KEM-512	800 B	768 B	1568 B
ML-KEM-768	1184 B	1088 B	2272 B
ML-KEM-1024	1568 B	1568 B	3136 B

The combined representation for ML-KEM-768 is approximately 44.9% larger than ML-KEM-512 under this measure, while ML-KEM-1024 is exactly twice the combined size of ML-KEM-512.

A 10,000-trial Monte Carlo sensitivity analysis perturbed the weights using multiplicative log-normal noise and normalized them after perturbation.

Scenario	Most frequently selected configuration	Selection frequency
Low-risk Web	ML-KEM-512	91.31%
Enterprise	Hybrid	100.00%
High Confidentiality	Hybrid	96.23%

Constrained IoT	ML-KEM-512	78.56%
Critical Infrastructure	Hybrid	99.42%

The sensitivity analysis indicates strong stability of the principal migration decisions. Enterprise selection remained unchanged in all 10,000 trials, while critical-infrastructure hybrid selection remained unchanged in 99.42% of trials.

5. SECURITY AND MIGRATION ANALYSIS

5.1 Security Decision Analysis

The framework does not assign an absolute security guarantee to any candidate. Security adequacy is one component of the migration decision. Cryptographic security also depends on formal assumptions, parameter selection, implementation correctness, protocol composition, side-channel resistance, and operational deployment. The security criterion therefore represents relative suitability for the modeled scenario rather than an independently proven security level.

5.2 Algorithmic Diversity and Crypto-Agility

A central feature of RACAF-PQC is explicit treatment of algorithmic diversity. Dependence on a single mathematical family may create systemic exposure if an unexpected cryptanalytic advance weakens that family. HQC provides a code-based alternative to lattice-based ML-KEM. As of 30 April 2025, HQC had been selected for the fourth round of NIST's standardization process but was not yet a finalized FIPS standard [10].

Crypto-agility requires the ability to replace algorithms without redesigning the entire application architecture. A migration-ready architecture should separate cryptographic mechanisms from application logic through configurable cryptographic interfaces, algorithm negotiation, versioning, and policy-based selection.

5.3 Hybrid Migration Strategy

Hybrid cryptography provides a practical transition mechanism between classical and post-quantum systems. The ECDHE+ML-KEM-768 configuration combines classical interoperability with post-quantum key establishment and achieves the highest PMRI in enterprise, high-confidentiality, and critical-infrastructure scenarios. In resource-constrained environments, however, the additional overhead of hybrid deployment may make ML-KEM-512 preferable.

5.4 Threat Model

RACAF-PQC considers an adversary capable of passively collecting encrypted communications, exploiting weaknesses in classical public-key cryptography after sufficiently capable quantum computers become available, exploiting algorithm-specific weaknesses, targeting migration inconsistencies, and benefiting from organizational dependence on a single cryptographic mechanism. The framework does not model arbitrary endpoint compromise, physical tampering, malicious insiders, or all side-channel attacks.

6. DISCUSSION AND LIMITATIONS

6.1 Principal Findings

Three principal findings emerge. First, a single PQC configuration does not dominate across all application scenarios. Second, risk-aware selection provides measurable modeled improvement relative to fixed ML-KEM-768, with a mean improvement of approximately 5.0%. Third, the difference between risk-aware PQC migration and classical-only migration is substantially larger, with a mean modeled improvement of approximately 42.0%.

6.2 Practical Implications

Organizations can use the framework during phased PQC migration by identifying cryptographic assets, protocols using public-key cryptography, sensitivity and lifetime of protected information, computational and bandwidth constraints, interoperability requirements, algorithm dependencies, and opportunities for hybrid deployment.

6.3 Limitations and Reproducibility

The most important limitation is that PMRI criterion values are model-based inputs rather than direct hardware measurements. Accordingly, the reported 5.0% and 42.0% improvements should not be interpreted as measured CPU-speed or energy-efficiency improvements. They represent improvements in the multi-criteria migration decision score. The sensitivity experiment establishes robustness of the decision model under weight perturbation; it does not constitute a cryptanalytic security proof.

As of the April 2025 cutoff, HQC had been selected for the fourth round but had not yet become a finalized FIPS-standardized KEM. The computational experiment is nevertheless reproducible because candidate configurations, criteria, weights, scoring values, PMRI equation, and sensitivity procedure are explicitly defined.

6.4 Future Experimental Validation

Future work should replace model-based performance criteria with measurements from real implementations. Experiments should evaluate key-generation latency, encapsulation and decapsulation latency, memory consumption, CPU utilization, energy consumption, communication overhead, TLS handshake latency, throughput, and performance on x86-64, ARM, Raspberry Pi-class, and RISC-V platforms. The PMRI model can then be recalibrated using experimentally measured values.

7. CONCLUSION

This paper presented RACAF-PQC, a risk-aware crypto-agility framework for post-quantum cryptographic migration. The framework addresses an important practical limitation of conventional PQC migration strategies: the assumption that one cryptographic configuration should be universally adopted.

RACAF-PQC introduces the Post-Quantum Migration Readiness Index, combining security adequacy, computational performance, communication efficiency, algorithmic diversity, interoperability, and crypto-agility. A reproducible computational experiment involving six configurations and five application scenarios demonstrated that the optimal migration decision depends strongly on the operational environment.

ML-KEM-512 was selected for the modeled low-risk web and constrained-IoT scenarios, while ECDHE+ML-KEM-768 achieved the highest PMRI for enterprise, high-confidentiality, and critical-infrastructure environments. Compared with fixed ML-KEM-768, the framework produced a mean modeled improvement of approximately 5.0%. Compared with classical-only ECDHE migration, the mean improvement was approximately 42.0%. The 10,000-trial sensitivity analysis further demonstrated that the major migration decisions were stable under reasonable perturbations of decision weights.

The principal significance of RACAF-PQC is therefore not the proposal of another cryptographic primitive but the development of a transparent, mathematically formulated mechanism for making migration decisions under competing security and operational constraints. The framework should be regarded as a decision-support methodology rather than a substitute for formal cryptographic security analysis or real-world benchmarking.

REFERENCES

1. C. Jackson, S. Miller, and Y. Wang, "Evaluating the security of CRYSTALS-Dilithium in the quantum random oracle model," in Advances in Cryptology – EUROCRYPT 2024, Springer, 2024. doi:10.1007/978-3-031-58751-1_15.
2. C. Paquin et al., "Post-quantum hybrid key exchange for TLS 1.3," IETF Internet-Draft, 2024.
3. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—A new hope," in 25th USENIX Security Symposium, 2016, pp. 327–343.
4. European Union Agency for Cybersecurity (ENISA), Post-Quantum Cryptography: Current State and Quantum Mitigation, 2021.
5. European Union Agency for Cybersecurity (ENISA), Post-Quantum Cryptography: Integration Study, 2022.
6. J. Bos et al., "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," in 2018 IEEE European Symposium on Security and Privacy Workshops, 2018, pp. 353–367. doi:10.1109/EuroSPW.2018.00053.
7. L. Ducas et al., "CRYSTALS-Dilithium: A lattice-based digital signature scheme," IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, pp. 238–268. doi:10.13154/tches.v2018.i1.238-268.
8. M. Alagic et al., Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8309, 2022.
9. National Institute of Standards and Technology, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 203, Aug. 2024.
10. National Institute of Standards and Technology, Module-Lattice-Based Digital Signature Standard, FIPS 204, Aug. 2024.
11. National Institute of Standards and Technology, Recommendations for Key-Encapsulation Mechanisms, Draft NIST SP 800-227, Jan. 2025.
12. National Institute of Standards and Technology, Stateless Hash-Based Digital Signature Standard, FIPS 205, Aug. 2024.

13. National Institute of Standards and Technology, Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8545, Mar. 2025.
14. National Security Agency, Commercial National Security Algorithm Suite 2.0, 2022.
15. NIST, “Post-Quantum Cryptography Standardization,” National Institute of Standards and Technology, 2024–2025.
16. P. Schwabe et al., related CRYSTALS-Kyber and post-quantum key-establishment literature, 2018–2024.
17. P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997. doi:10.1137/S0097539795293172.
18. Zheng et al., “Faster Post-Quantum TLS 1.3 Based on ML-KEM: Implementation and Assessment,” arXiv:2404.13544, 2024.