iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XII **Month of publication:** December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76503

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

Comparative Analysis of Classical Public-Key Cryptography and NIST-Standardized Post-Quantum Algorithms with a Focus on Migration Strategies

Sreerasmi V M[1], Jisna C K [2]
Assistant Professor, Department of Computer science Chinmaya Institute of Technology, Kerala, India

Abstract: ***The rapid developments in quantum computing pose a critical threat to classical public-key cryptography, particularly RSA and Elliptic Curve Cryptography (ECC), which rely on mathematical problems solvable by Shor's algorithm. In response, the National Institute of Standards and Technology (NIST) has standardized quantum-resistant algorithms, including ML-KEM, ML-DSA, FALCON, and SPHINCS+, to prepare global infrastructure for a post-quantum future. This paper provides a unified comparative analysis of classical cryptography and NIST-standardized PQC algorithms, evaluating their security assumptions, efficiency, architectural characteristics, and resilience against quantum adversaries. A comprehensive literature review identifies gaps in existing studies, particularly concerning unified migration frameworks that combine theory, implementation requirements, certificate ecosystem changes, and organizational readiness. To address these gaps, the paper proposes a structured comparative framework and outlines practical migration strategies, including hybrid cryptographic deployment, protocol upgrades, and phased transition roadmaps. The findings highlight that while PQC introduces larger key and signature sizes, its quantum resistance and standardization maturity make it essential for long-term security. The study concludes that strategic migration planning, driven by hybrid adoption and ecosystem adjustments, is crucial for ensuring a secure and seamless transition to post-quantum cryptography.***

Keywords: ***Post-Quantum Cryptography, RSA, ECC, ML-KEM, ML-DSA, Migration Strategies, Quantum Security, Classical Cryptography***

I. INTRODUCTION

Public-key cryptography has been the cornerstone of secure digital communications for over four decades. Technologies such as RSA and Elliptic Curve Cryptography (ECC) secure billions of internet connections every day, protect electronic payments, ensure integrity through digital signatures, and maintain authentication in critical infrastructures. Their security depends on mathematical problems that classical computers cannot solve in reasonable time.

However, the emergence of large-scale quantum computing has disrupted this security landscape. Shor's algorithm [1] theoretically breaks RSA and ECC in polynomial time, meaning all systems relying on classical public-key cryptography will become vulnerable the moment quantum computers become operational at required scale.

Governments, financial institutions, healthcare systems, IoT ecosystems, defence communications, and cloud providers are at risk. Encryption and digital signatures used today may be recorded and decrypted later—a threat known as "harvest-now, decrypt-later." [7] Therefore, transitioning to quantum-resistant algorithms is a global cybersecurity priority [2],[8].

NIST, after a multi-year international effort, standardized the first generation of post-quantum cryptographic (PQC) algorithms: ML-KEM for encryption/key exchange, ML-DSA and FALCON for signatures, and SPHINCS+ [2] as an alternative hash-based signature.

This paper presents:

1) A comprehensive comparison between classical and PQC algorithms.
2) A deep analysis of migration strategies required to transition global systems to PQC.
3) Tables and figures comparing security levels, key sizes, computation overhead, and migration phases.

©IJRASET: All Rights are Reserved

II. RELATED WORK/LITERATURE REVIEW

Several studies discuss the conceptual differences between RSA/ECC and PQC algorithms. These works compare underlying mathematics, expected security, and computational characteristics [3],[4],[5],[6]. However, most are narrowly focused on the algorithms themselves rather than the system-wide migration impact. Academic studies rarely combine comparative cryptographic analysis + migration strategies, leaving a notable gap. Government bodies (NIST, NSA, ETSI, IETF) provide migration guidance, but mostly at a high level [2],[7],[8],[9]. IETF drafts propose hybrid mechanisms for TLS and IKEv2, yet do not address organizational readiness, certificate lifecycle changes, or architecture modifications.

Industry whitepapers discuss PQC adoption challenges in cloud, telecom, and IoT environments, but lack theoretical comparison frameworks.

This paper contributes by integrating:

1) Cryptographic comparison
2) System-level migration analysis
3) Infrastructure readiness
4) Hybrid adoption models
5) Practical roadmap phases

This unified view is currently limited in literature, meeting the novelty requirement.

III. BACKGROUND

A. Classical Cryptography (RSA, ECC)

RSA is based on integer factorization, requiring large keys for security. ECC is based on elliptic curve discrete logs, offering smaller keys with equivalent strength. However, both are vulnerable to quantum attacks.

B. Post-Quantum Cryptography (NIST Standardized)

NIST's chosen PQC algorithms include:

1) ML-KEM → Replaces RSA/ECDH key exchange [3]
2) ML-DSA → Replaces RSA/ECDSA signatures [4]
3) FALCON → Compact lattice signature [5]
4) SPHINCS+ → Hash-based signature alternative [6]

These are based on problems not known to be solvable by quantum computers.

IV. COMPARATIVE ANALYSIS FRAMEWORK

To evaluate classical vs PQC algorithms, we compare:

1) Security Basis
2) Key Sizes and Ciphertext Sizes
3) Runtime Performance
4) Memory and Implementation Complexity

Ecosystem Compatibility and StandardizationAlgorithm	Security Basis	Quantum Security	Vulnerability
RSA	Integer Factorization	Broken	Shor's Algorithm
ECC	Elliptic Curve DLP	Broken	Shor's Algorithm
ML-KEM	Module-LWE	Strong	No known attacks
ML-DSA	Module-SIS	Strong	No known attacks
FALCON	Lattice NTRU	Strong	Implementation sensitive
SPHINCS+	Hash-based	Very Strong	Large signatures

TABLE I: COMPARISON OF SECURITY FOUNDATIONS

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Algorithm	Public Key	Secret Key	Signature	Ciphertext
RSA-2048	256 B	256 B	256 B	256 B
ECC-P256	64 B	32 B	64 B	N/A
ML-KEM-768	1.18 KB	2.4 KB	N/A	1 KB
ML-DSA-2	1.3 KB	2.5 KB	2.4 KB	N/A
FALCON-512	0.9 KB	1.2 KB	0.7 KB	N/A
SPHINCS+-128s	32 B	64 B	7.8 KB	N/A

TABLE II: KEY AND SIGNATURE SIZE COMPARISON

Algorithm	CPU Speed	Memory Use	Implementation Ease
RSA	Fast	Low	Very Easy
ECC	Very Fast	Low	Medium
ML-KEM	Fast	Medium	Easy
ML-DSA	Medium	Medium	Easy
FALCON	Fast	Medium	Hard
SPHINCS+	Slow	High	Easy

TABLE III: PERFORMANCE & IMPLEMENTATION COMPLEXITY

Fig. 1: Algorithm Classification Diagram

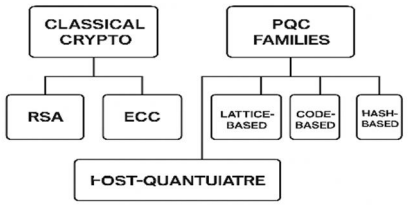
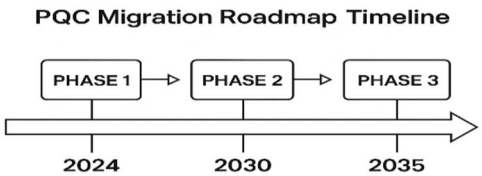


Fig. 2: PQC Migration Roadmap Timeline



V. MIGRATION STRATEGIES

A. *Hybrid Migration [9][10]*

Use combined classical + PQC algorithms during transition.
TLS example: ECDH + ML-KEM hybrid key exchange.

B. *Protocol Adaptation [9][10]*

Protocols needing modifications:

1) TLS 1.3 [11]
2) SSH
3) IKEv2 (VPN)
4) QUIC
5) Certificate-based authentications

C. *Certificate Ecosystem Upgrades [7][8]*

Must support:

1) PQC signatures (large)
2) PQC public keys
3) Hybrid certificates (dual signatures)
4) CA-level policy updates

D. *Infrastructure Readiness Assessment*

Organizations must perform:

1) Cryptographic asset discovery
2) Lifecycle analysis
3) Hardware capability analysis
4) IoT/embedded constraints examination

E. *Phased PQC Migration Roadmap*

Phase 1 (2024–2026): Preparation

- Inventory cryptographic use
- Identify long-term sensitive data
- Begin PQC testing in isolated systems
- Train security teams on PQC

Phase 2 (2026–2029): Hybrid Adoption

- Use ML-KEM + ECDH in parallel
- Deploy hybrid certificates
- Upgrade firmware signing to PQC
- Update TLS, SSH, VPN endpoints

Phase 3 (2030–2035): Full PQC Migration

- Remove RSA/ECC support
- Adopt PQC-only certificates
- Update all CA and PKI infrastructures
- Ensure backward compatibility for legacy systems through gateways
-

VI. DISCUSSION

A key challenge in PQC is balancing security and performance [2],[8]. PQC algorithms resist quantum attacks but require larger memory, increased computational load, and updated protocols. IoT devices pose serious challenges due to limited RAM and slow processors. Despite this, PQC adoption is essential. Industries like finance, defence, healthcare, and government must transition early to protect long-term sensitive data.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

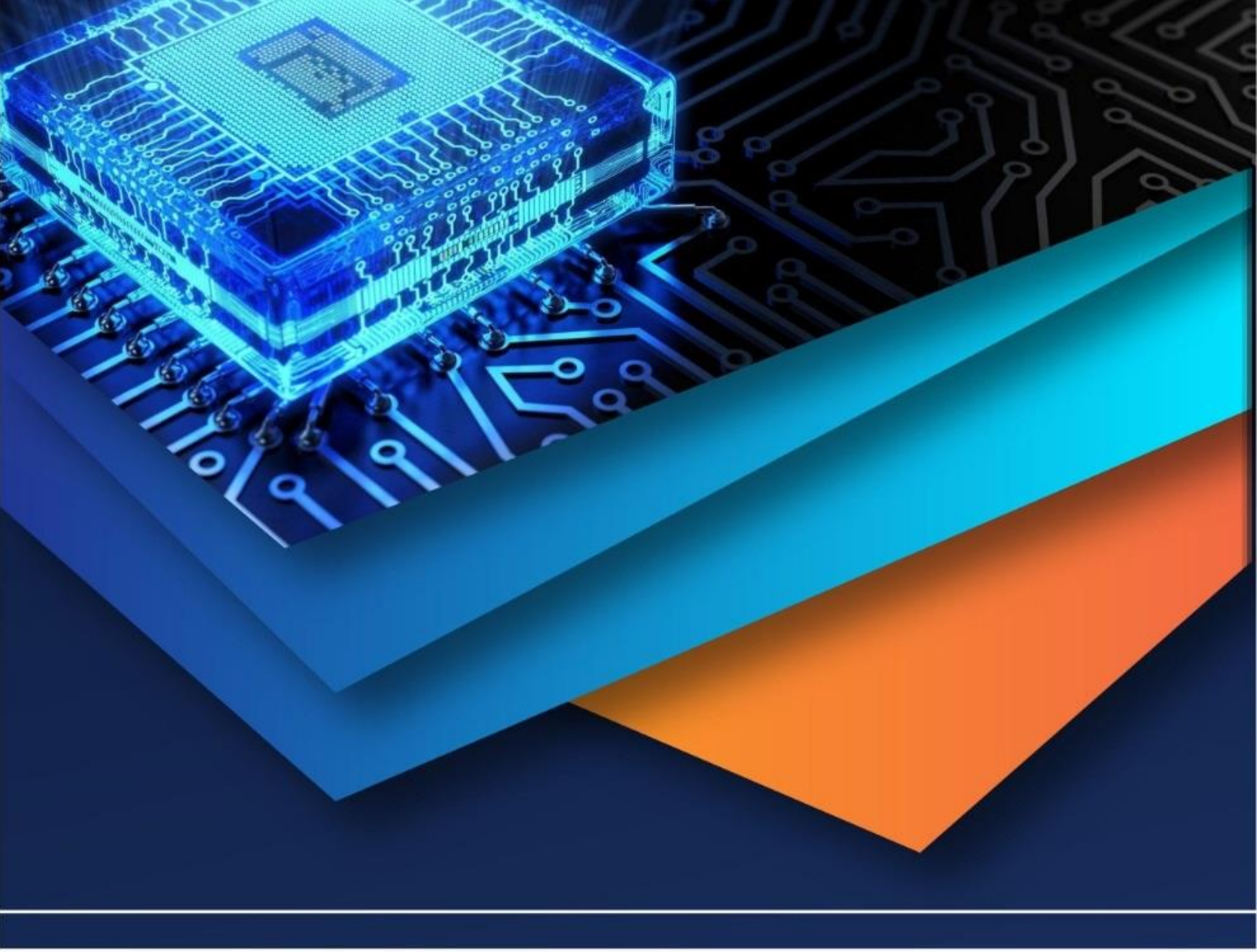
VII. CONCLUSION

The research clearly establishes that classical public-key cryptography cannot survive the advent of quantum computing. NIST-standardized PQC algorithms provide robust long-term security and will be the future backbone of secure global communication [2]. Migration requires [8],[9] careful planning through hybrid adoption, infrastructure upgrades, certificate transformation, and phased transition. This paper's comparative analysis and migration roadmap serve as a foundation for academic researchers, organizations, and policymakers planning quantum-resilient digital infrastructure.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proc. 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134.
[2] National Institute of Standards and Technology (NIST),"Post-Quantum Cryptography Standardization Project," NIST, Gaithersburg, MD, USA, 2024.
[3] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky et al., "CRYSTALS–Kyber: A CCA-secure module-LWE based KEM," in Proc. IEEE EuroS&P, 2018.
[4] J. Bos, L. Ducas, T. Lepoint, V. Lyubashevsky et al., "CRYSTALS–Dilithium: Digital signatures from module lattices," NIST PQC Round 3 Submission, 2020.
[5] D. Cousins, C. Peikert, P. Schwabe et al., "FALCON: Fast Fourier lattice-based compact signatures," NIST PQC Round 3 Submission, 2020.
[6] A. Hülsing, L. R. Reyzin, S. Song et al., "SPHINCS+: Submission to the NIST post-quantum standardization project," 2020.
[7] National Security Agency (NSA), "Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)," NSA Cybersecurity Directorate, 2022.
[8] National Cybersecurity Center of Excellence (NCCoE), "Migration to Post-Quantum Cryptography: Readiness and Planning Guide," NIST, 2024.
[9] Internet Engineering Task Force (IETF), "Guidance for Migrating to Post-Quantum Cryptography," IETF Internet-Draft, 2025.
[10] A. Kwiatkowski, S. Fluhrer, D. Stebila et al., "Hybrid key exchange in TLS 1.3," IETF Internet-Draft, 2024.
[11] Quantum Resistant Security Group (PQCC), "PQC Migration Roadmap," PQCC Te

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)