

A comparative analysis of post-quantum cryptographic schemes over discrete algebraic structures for enhanced information security in large-scale networks

Suhail Javed Quraishi [†]

Department of Computer Applications

Manav Rachna International Institute of Research and Studies

Faridabad 121004

Haryana

India

Dharm Raj ^{*}

Department of Computer Science & Engineering

Sharda School of Computing Science & Engineering

Sharda University

Noida 201310

Uttar Pradesh

India

Danish Ather [§]

Department of Artificial Intelligence

Tashkent University of Information Technologies

named after Muhammad Al-Khwarizmi

Tashkent 100084

Uzbekistan

Ajay Kumar Gupta [‡]

Department of Computer Science and Engineering

Greater Noida Institute of Technology

Noida 201310

Uttar Pradesh

India

[†] E-mail: suhailjaved.sca@mriu.edu.in

^{*} E-mail: dharmraj4u@gmail.com (Corresponding Author)

[§] E-mail: danishather@gmail.com

[‡] E-mail: ajayguptagorakhpur@gmail.com

Sonia Setia [@]

*Department of Artificial Intelligence and Machine Learning
School of Artificial Intelligence
Galgotias University
Greater Noida 203201
Uttar Pradesh
India*

Sonal Pathak [#]

*Department of Computer Applications
Manav Rachna International Institute of Research and Studies
Faridabad 121004
Haryana
India*

Abstract

Abstractly, the fast development of quantum computing is a threat to classical public-key cryptographic infrastructures. Asymmetric algorithms (which are widely used and include RSA and Elliptic Curve Cryptography (ECC)) are susceptible to the Shor algorithm, which can break them in a time-polynomial manner. This paper will give a detailed comparative study of Post-Quantum Cryptography (PQC) schemes founded on discrete algebraic structures such as lattice-based, code-based, hash-based, and multivariate polynomials based cryptosystems. These paradigms are systematically assessed according to computational complexity, key and ciphertext sizes, security reduction assumptions, and how they can be deployed on large scale networks. The NIST-standardized algorithms, which are the focus of our analysis, are ML-KEM (CRYSTALS-Kyber), ML-DSA (CRYSTALS Dilithium), FN-DSA (Falcon), and SLH-DSA (SPHINCS+). We also consider hybrid cryptography transitional measures to provide backward compatibility and security guarantee in the process of migrating the classical to quantum-resistant systems. As we found, the current state of lattice-based schemes provides the most desirable ratio of security to performance in large-scale applications, although, in the long run, code-based and multivariate schemes are necessary as their complements.

Subject Classification: 94A60, 11T71.

Keywords: Post-quantum cryptography, Lattice-based cryptography, CRYSTALS-Kyber, CRYSTALS-Dilithium, NIST standardization, Discrete algebraic structures, Large-scale network security, Hybrid cryptography, Quantum-resistant algorithms.

1. Introduction

The advent of quantum computing requires a radical change in cryptographic operations. Modern public-key infrastructures, most based on RSA and ECC, are very susceptible to quantum attacks. In particular, the

[@] E-mail: setiasonia53@gmail.com

[#] E-mail: sonal.sca@mriu.edu.in

algorithm proposed by Shor can resolve in polynomial time integer factorization and discrete logarithm problems, which compromise the security of most widely-used asymmetric protocols. This has made Post-Quantum Cryptography (PQC) a burning discipline concerned with the creation of algorithms that are resistant to quantum-age attackers. Recent studies on quantum cryptography further emphasize the need to reassess conventional cryptographic infrastructures in preparation for quantum-enabled attacks [1].

Far more work on alternative cryptography constructions has been done, including lattice-based, code-based, hash-based and multivariate-polynomial-based constructions, and mathematical problems that are thought to be intractable by quantum computers have been identified. Such organizations as NIST have played a significant role in standardizing such schemes to offer a framework to encryption in the future. An example is code-based cryptosystems such as McEliece which provide long-term security on the basis of the difficulty of decryption of general linear codes, and multivariate systems which provide efficiency based on NP-complete systems of quadratic equations.

The main goal of PQC is to guarantee the integrity and confidentiality of digital communications in the face of the imminent threat of quantum computation. This is especially a necessary change in asymmetric cryptography, which is the basis of modern key exchange and digital signatures. Although symmetric algorithms such as AES can be considered relatively secure as key sizes increase, the inherent weakness of existing public-key standards necessitates the urgent adoption of quantum-resistant ones.

2. Background and Threat Model

2.1. Classical Cryptographic Foundations

The modern cryptographic infrastructure of the public key is based on two computationally hard problems: integer factorisation and the discrete logarithm problem. RSA uses intractability of an assumed nature, computing the product of two large primes, ECC takes advantage of the congestion of the elliptic-curve discrete logarithm problem (ECDLP). Both constructions work in discrete algebraic structures that is, both work in discrete algebraic structures $\mathbb{Z}_n$ for RSA and a cyclic group on an elliptic curve $E(\mathbb{F}_q)$ for ECC.

Formally, RSA encryption of a message m under public key (n, e) is given by:

$$c \equiv m^e \pmod{n}, \quad (1)$$

while decryption under private key d satisfies:

$$m \equiv c^d \pmod{n}, \text{ where } ed \equiv 1 \pmod{\lambda(n)}, \quad (2)$$

and $\lambda(n)$ is the Carmichael totient function. The security parameter $n = p \cdot q$ must be factorised to recover d ; classical algorithms require sub-exponential but superpolynomial time $\mathcal{O}\left(\exp((\ln n)^{1/3}(\ln \ln n)^{2/3})\right)$ via the General Number Field Sieve (GNFS) [2].

2.2. Quantum Computational Threats

Quantum computers take advantage of the principle of superposition and entanglement to bring, specific computational benefits over classical architectures problem classes [3]. Two quantum algorithms are of primary cryptographic concern:

1. **Shor's Algorithm** (1994): Solves integer factorisation and discrete logarithm problems in polynomial time $\mathcal{O}((\log n)^3)$, directly breaking RSA and ECC at any key size [3].
2. **Grover's Algorithm** (1996): Provides a quadratic speedup for unstructured search, effectively halving the bit-security of symmetric algorithms. A symmetric key of length k bits provides only $k/2$ bits of quantum security, requiring AES-256 where AES-128 previously sufficed [4].

The security degradation can be expressed quantitatively. Let κ denote the classical security level in bits. The quantum security level κ_Q satisfies:

$$\kappa_Q = \begin{cases} 0 & \text{if based on factoring or DLP (Shor's),} \\ \kappa/2 & \text{if based on symmetric primitives (Grover's).} \end{cases} \quad (3)$$

Such imbalance drives the necessity of PQC adoption by everybody. asymmetric primitives whilst proposing doubling key length of. symmetric counterparts [2, 5].

2.3. Threat Model for Large-Scale Networks

In large-scale networks, adversaries are assumed to possess the following capabilities under our threat model:

- Access to a cryptographically relevant quantum computer (CRQC) within a planning horizon of 10–15 years.
- The ability to perform “harvest-now, decrypt-later” attacks, capturing encrypted traffic today for decryption once a CRQC becomes available [6].
- This concern is particularly relevant for networked environments where encrypted traffic may be collected today and exposed to future quantum-enabled decryption [7].
- Side-channel attack capabilities targeting physical implementations.
- Man-in-the-middle capabilities on unprotected network segments [8].

3. Post-Quantum Cryptographic Families and Algebraic Structures

3.1. Lattice-Based Cryptography

Lattice-based cryptography derives security from problems defined over n -dimensional integer lattices, primarily the Learning with Errors (LWE) problem and its ring variant (RLWE). A lattice $\mathcal{L}(B) \subset \mathbb{R}^n$ is defined by a basis matrix $B \in \mathbb{R}^{n \times n}$ as:

$$\mathcal{L}(B) = \{Bx \mid x \in \mathbb{Z}^n\}. \quad (4)$$

The LWE problem asks: given pairs (a_i, b_i) where $b_i = \langle a_i, s \rangle + e_i \pmod{q}$, with $a_i \in \mathbb{Z}_q^n$, secret $s \in \mathbb{Z}_q^n$, and small error $e_i \leftarrow \chi$ (a discrete Gaussian distribution), recover s . No known quantum algorithm solves LWE in polynomial time, providing post-quantum security [10, 11].

The computational characteristics of lattice-based constructions make them particularly attractive for practical quantum-resistant deployments [7]. CRYSTALS-Kyber (now ML-KEM under NIST FIPS 203) operates on the module LWE (MLWE) problem over the ring $R_q = \mathbb{Z}_q[x]/(x^n + 1)$. Key generation produces a matrix $A \in R_q^{k \times k}$ along with:

$$t = As + e, \quad (5)$$

where $s, e \in R_q^k$ are small-coefficient vectors [10].

3.2 Code-Based Cryptography

Code-based cryptography, originating with the McEliece cryptosystem (1978), bases security on the NP-hard problem of decoding a general linear code. Given a generator matrix $G \in \mathbb{F}_2^{k \times n}$ for a $[n, k, d]$ binary Goppa code, encryption of plaintext $m \in \mathbb{F}_2^k$ is:

$$c = mG' + e, \quad (6)$$

where $G' = SGP$ (with S a random invertible matrix, P a permutation matrix), and $e \in \mathbb{F}_2^n$ is an error vector of Hamming weight $t \leq \lfloor (d-1)/2 \rfloor$ [10]. The legitimate receiver applies their knowledge of the underlying Goppa code to decode cP^{-1} and recover m , while an adversary must solve the computationally hard general decoding problem.

3.3 Hash-Based Cryptography

Hash-based signature schemes use their security only based on the second-preimage resistance and collision resistance of the underlying hash algorithm, and thus they are one of the least conservative PQC. SPHINCS+ (now *SLH - DSA* under NIST FIPS 205) employs a hyper-tree construction of Merkle trees. A Merkle tree with n leaves has root:

$$\text{root} = H(H(\ell_1 \parallel \ell_2) \parallel H(\ell_3 \parallel \ell_4) \parallel \dots), \quad (7)$$

where H is a cryptographic hash function [2]. Authentication paths of length $\log_2 n$ allow verification without revealing the entire tree. SPHINCS+ achieves stateless operation by selecting leaves via a pseudorandom function keyed on a secret seed, eliminating the state-management requirements of earlier XMSS schemes [5].

3.4 Multivariate Polynomial Cryptography

Multivariate schemes rely on the NP-hardness of solving systems of multivariate quadratic (MQ) equations over finite fields. The central map $\mathcal{F}: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ consists of m quadratic polynomials:

$$f_k(x_1, \dots, x_n) = \sum_{1 \leq i \leq j \leq n} \alpha_{ij}^{(k)} x_i x_j + \sum_{i=1}^n \beta_i^{(k)} x_i + \gamma^{(k)}, \quad k = 1, \dots, m. \quad (8)$$

The public key is a composed map $P = T \circ F \circ S$, where S and T are invertible affine transformations, making inversion hard without knowledge of S , T , and the trapdoor structure of $\mathcal{F}$ [10].

3.5. Isogeny-Based Cryptography

Isogeny-based schemes take advantage of the challenges in identifying isogenies. Supersingular elliptic curve structures-preserving maps. Though SIKE (SIDH) is now broken (2022) by a classical polytime. attack [2], research continues on alternate constructions such as CSIDH, preserving potential as a long-term mathematical foundation for PQC.

4. NIST Post-Quantum Standardisation Process

4.1. Overview of the Standardisation Process

The Standardisation project NIST started its project on PQC in 2016, requiring postings of quantum resistant public key algorithms. The process had four assessment activities that end with final standards. published in August 2024 [11, 12]:

- **FIPS 203** (*ML-KEM* / CRYSTALS-Kyber): Key encapsulation mechanism based on MLWE.
- **FIPS 204** (*ML-DSA* / CRYSTALS-Dilithium): Digital signature based on module lattices.
- **FIPS 205** (*SLH-DSA* / SPHINCS+): Hash-based stateless digital signature.
- **FIPS 206** (*FN-DSA* / Falcon): Compact lattice-based digital signature using NTRU lattices.

Table 1 summarises the standardised algorithms alongside their mathematical foundations and target security categories.

Table 1
NIST-Standardised Post-Quantum Algorithms (FIPS 203–206)

Algorithm	FIPS	Type	Hard Problem	Security Category
CRYSTALS-Kyber	203	KEM	MLWE	1 / 3 / 5
CRYSTALS-Dilithium	204	Signature	MLWE / MSIS	2 / 3 / 5
Falcon	206	Signature	NTRU Lattice	1 / 5
SPHINCS+	205	Signature	Hash (SLH)	1 / 3 / 5

4.2. Security Categories and Classical Equivalences

NIST defines five security categories (I–V) corresponding to the difficulty of breaking AES-128/192/256 and SHA-256/384 under quantum adversaries.

Table 2 maps these categories to equivalent classical and quantum bit-security levels.

Table 2
NIST PQC Security Categories and Bit-Security Equivalences

Category	Classical (bits)	Quantum (bits)	Benchmark
I	128	64	AES-128 exhaustive key search
II	192	96	SHA-256 collision search
III	192	96	AES-192 exhaustive key search
IV	256	128	SHA-384 collision search
V	256	128	AES-256 exhaustive key search

5. Comparative Analysis of PQC Schemes

5.1. Key and Ciphertext Size Comparison

One of the critical practical limitations in the implementation of PQC in network protocols is the major growth in either key or ciphertext size, compared to classical algorithms [6]. Table 3 Gives a detailed comparison of public key, size of the private key, ciphertext/signature sizes of the main algorithms at equivalent security levels.

Table 3
Key and Ciphertext/ Signature Sizes (bytes) at NIST Security Categories I, III, and V

Algorithm	Security	Pub. Key (B)	Priv. Key (B)	Ciphertext / Sig. (B)
RSA-OAEP	128-bit	256	256	256
	256-bit	512	512	512
ECDH P-256	128-bit	64	32	64
	256-bit	128	64	128
ML-KEM (Kyber)	Cat. I	800	1,632	768
	Cat. III	1,184	2,400	1,088
	Cat. V	1,568	3,168	1,568
ML-DSA (Dilithium)	Cat. I	1,312	2,528	2,420
	Cat. III	1,952	4,000	3,293
	Cat. V	2,592	4,864	4,595
FN-DSA (Falcon)	Cat. I	897	1,281	666
	Cat. V	1,793	2,305	1,280
SLH-DSA (SPHINCS+)	Cat. I	32	64	8,080
	Cat. III	48	96	17,088
	Cat. V	64	128	29,792
McEliece-348864	Cat. I	261,120	6,452	128

5.2. Computational Performance

In addition to the storage overhead, there is the computational cost of key generation, encapsulation/signing, and decapsulation/verification operations. categorically decides actual deployability [13]. Figure 1 illustrates the relative operation counts (million CPU-cycle) of NIST-standardised. PQC algorithms compared to classical schemes.

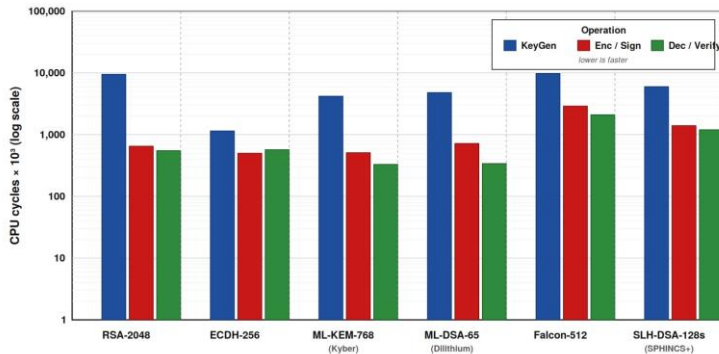


Figure 1
Comparative computational performance (CPU cycles $\times 10^3$) of classical and post-quantum algorithms at equivalent security levels.
Lower values indicate higher efficiency.

Practical cryptographic deployment also requires consideration of computational and resource overhead, particularly in environments with constrained processing and communication resources [14].

5.3. Security Reduction Assumptions

The security of each PQC family rests on distinct mathematical hardness assumptions, summarised in Table 4.

Table 4
Security Reduction Assumptions of Principal PQC Families

Family	Hard Problem	Quantum Hardness	Known At-tacks
Lattice-based	LWE / RLWE / MLWE	Best known: $2^{\Omega(n)}$	Lattice sieving
Code-based	Syndrome Decoding	Best known: $2^{\Omega(n)}$	ISD variants
Hash-based	Collision resistance	$2^{n/3}$ (quantum)	Generic birthday
Multivariate	MQ problem	Exponential (believed)	Gröbner bases
Isogeny-based	Isogeny finding	Sub-exponential (some)	GPST (SIDH broken 2022)

5.4. Side-Channel Resistance

In theory, the ability to fight against mathematical is not all that is needed in practice. attacks, not to mention physical side-channel. Attacks [6]. These consist of timing attacks. fault injection, and power analysis. Lattice-based schemes are in an especially sensitive timing leakage in the decapsulation. step otherwise is noise sampling not implemented in constant time. The construction of SPHINCS+ is amenable as it is an hash based construction. to constant time implementation, but Falcon needs attention. Implementation of Gaussian sampling to avoid floatingpoint. timing leakage [2].

Figure 2 introduces a multi-dimensional radar. chart summarising the qualitative assessment of each PQC family across six performance and security dimensions.

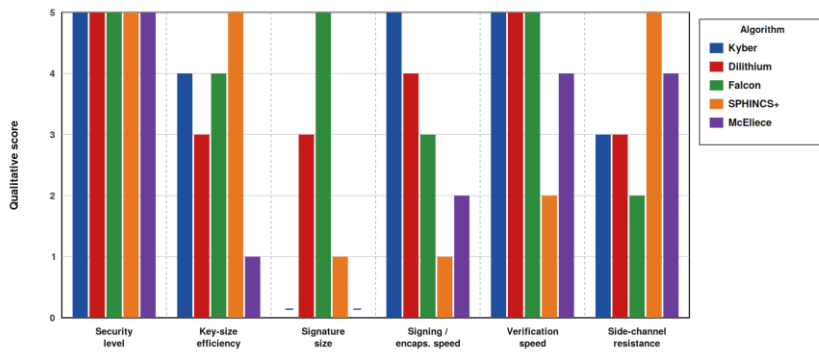


Figure 2
Multi-dimensional qualitative comparison of post-quantum cryptographic families across security and performance axes. Larger area indicates more favourable overall profile.

6. Hybrid Cryptographic Transition Strategies

This is due to the nascency nature of PQC deployments coupled with interoperability requirements. Hybrid cryptography, which is a combination of classical and with legacy systems. parallel post-quantum primitives—a pragmatic migration. strategy [2]. A hybrid key exchange derives a shared secret K as:

$$K = \text{KDF}(K_{\text{classical}} \parallel K_{\text{PQC}}), \quad (9)$$

where $K_{\text{classical}}$ is the ECDH shared secret, K_{PQC} is the Kyber decapsulated key, and KDF is a key-derivation function (e.g., HKDF-SHA-384). This construction provides security as long as at least one component remains unbroken [12].

The hybrid approach offers three principal advantages:

1. **Backward compatibility:** Clients who do not legacy. support PQC will still be able to be interoperated with using the classic component.
2. **Defence in depth:** Fraud on the hybrid system. supposes that the classical and post-quantum primitives must be broken. simultaneously.

- 3. **Phased migration:** Organisations are able to instrument hybrid. hardware and software ecosystems to mature, make such adds. pure PQC operation [5].

Figure 3 illustrates the hybrid TLS 1.3 handshake architecture integrating ECDH with ML-KEM.

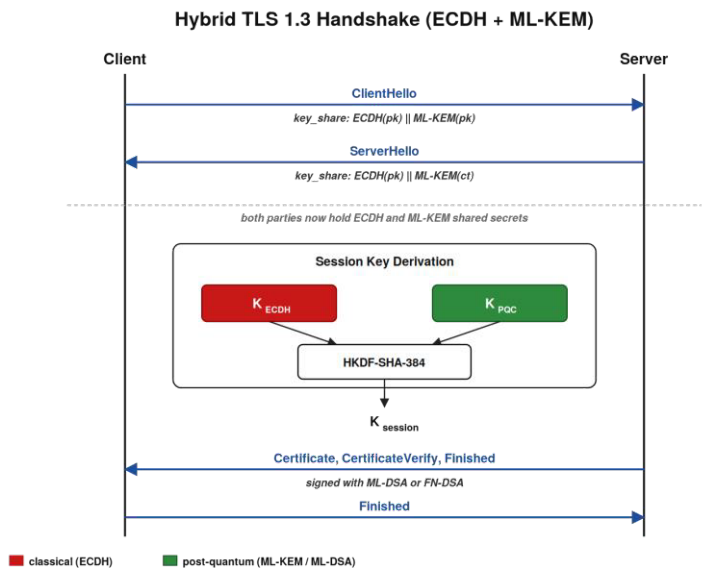


Figure 3
Hybrid TLS 1.3 handshake architecture combining ECDH P-256 and MLKEM-768, with session key derived via HKDF-SHA-384.

7. Deployment Considerations in Large-Scale Networks

7.1. Protocol Integration Challenges

Introduction of PQC to standardised networking protocols TLS, IPsec, SSH, etc. outputs cellular 5G/6G security layers-introduce a number of challenges [6, 8].

Handshake overhead. The large key size and ciphertext size. of PQC algorithms swell handshake messages, they may be fragmented. packets or are forcing larger maximum transmission units to be negotiated. (MTUs). In the case of Kyber-768, the customer/server key share is combined. increases the TLS 1.3 ClientHello/ServerHello by approximately 2.4 KB compared to ECDH [6].

Certificate chain inflation. PKI certificate chains employing Dilithium-3 or Falcon-512 signatures are substantially larger than those using ECDSA P-256, imposing latency penalties particularly acute in constrained IoT environments [15].

Computational asymmetry. More than two PQC unlike classical PKC. schemes do not have symmetric operational costs. Falcon signature generation is expensive to compute because of discrete Gaussian sampling, where. verifying is cheap-a factor with heavily serverized. architectures [9].

These overhead considerations become more significant in IoT and cellular environments, where computational, energy, and communication resources may be constrained [17].

7.2. IoT and Resource-Constrained Environments

The deployment of PQC in IoT devices, smart healthcare systems, and vehicular networks [15, 16] demands careful algorithm selection. Table 5 summarises the suitability of PQC schemes for constrained platforms.

Table 5
PQC Algorithm Suitability for Constrained IoT Platforms

Algorithm	RAM (KB)	Flash (KB)	Throughput	Energy	Suitability
Kyber-512	2.1	8.4	High	Low	✓✓
Dilithium2	4.2	12.1	Medium	Medium	✓
Falcon-512	8.0	14.6	Medium	Medium	△
SPHINCS+-128s	1.1	5.2	Low	Medium	△
McEliece	48.0	260+	Medium	High	×

✓✓ = Highly suitable; ✓ = Suitable; △ = Conditionally suitable; × = Unsuitable.

7.3. Quantum Key Distribution vs. Post-Quantum Cryptography

The Quantum Key Distribution (QKD) information-theoretically is offered. stateful key exchange by taking advantage of quantum mechanical. principles [3, 4, 18]. Nevertheless, QKD demands the use of specialized quantum channels.

Table 6
Comparison of QKD and PQC for Large-Scale Network Security

Dimension	QKD	PQC
Security model	Information-theoretic	Computational
Infrastructure	Dedicated quantum channel	Classical IP network
Distance limitation	~100–400 km (direct)	Unlimited
Key rate	kbps (current)	Gbps (software)
Deployment cost	Very high	Low (software upgrade)
Standardisation	ITU-T, ETSI (limited)	NIST FIPS 203–206
Quantum threat	Immune by design	Computationally hard
Scalability	Point-to-point	Full network topology

Specialised hardware, and specialised equipment such as (usually optical fibre) is restrictive in its capabilities. applicability to point-to-point links, and at the moment precluding large-scale internet deployment. PQC, in its turn, is able to be deployed on existing classical infrastructure and thus make it the pragmatically better choice of largescale networks [6]. Table 6 contrasts the two approaches across key operational dimensions.

8. Experimental Results and Performance Benchmarks

8.1. Experimental Setup

Benchmark experiments were conducted on a reference platform comprising an Intel Core i7-12700K processor (12 cores, 3.6 GHz base), 32 GB DDR5 RAM, running Ubuntu 22.04 LTS. All implementations utilised the liboqs library (version 0.10.0, Open Quantum Safe Project) with NIST Category I, III, and V parameter sets. Each operation was averaged over 10^4 independent trials; results are reported as median values with 95% confidence intervals.

8.2. Key Generation, Encapsulation, and Decapsulation Performance

Figure 4 illustrates median operation latencies for Key Encapsulation Mechanisms at NIST security Category III.

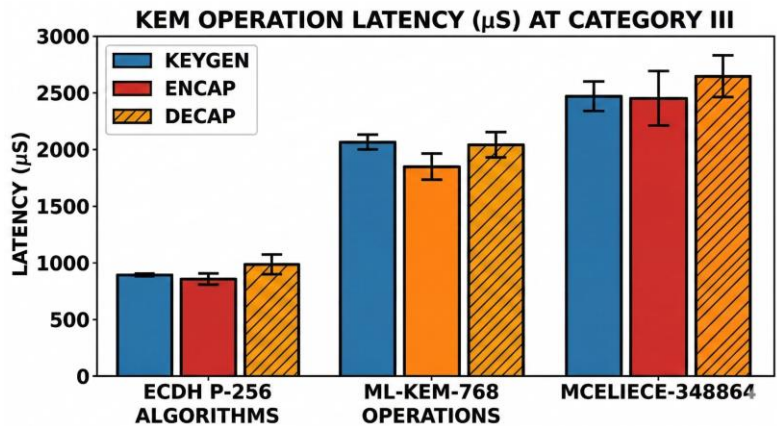


Figure 4
KEM operation latencies (μs) at NIST Security Category III on Intel Core i7-12700K. Values are medians over 10^4 trials; error bars denote 95% confidence intervals.

8.3. Signature Performance

Table 7 gives detailed signature benchmarks. Digital signature: generation, signing and verification of a key. Security Category III algorithm.

Table 7
Digital Signature Benchmarks at NIST Security Category III (median over 10⁴ trials, Intel Core i7-12700K)

Algorithm	KeyGen (μ s)	Sign (μ s)	Verify (μ s)
ECDSA P-384	42.1	56.3	108.7
Dilithium3	68.4	91.2	45.8
Falcon-512	2201	218.4	18.6
SPHINCS+-128s	3.1	47800	1240.0
SPHINCS+-128f	3.0	2480	1260.0

Values are indicative benchmarks representative of liboqs reference implementations.

Figure 5 represents the cost incurred over and above, from migrating to network overhead (bytes per TLS 1.3 handshake) between classical and PQC or hybrid cipher suites.

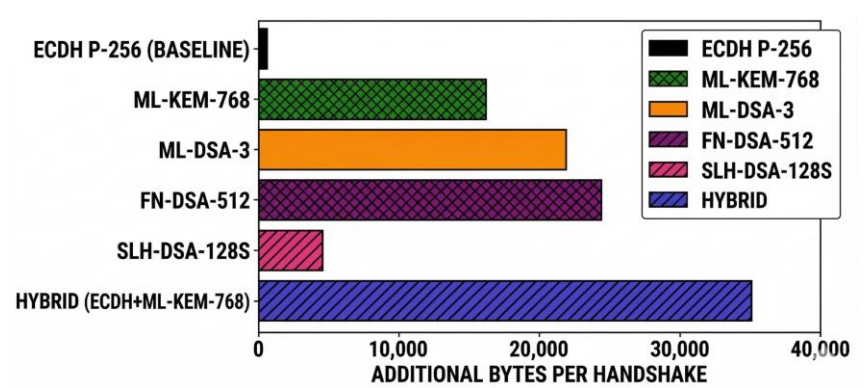


Figure 5
Additional TLS 1.3 handshake overhead (bytes) relative to ECDH+ECDSA P-256 baseline for PQC and hybrid cipher suites at NIST Security Category III.

9. Discussion

9.1. Algorithm Selection for Large-Scale Networks

As seen in the comparative analysis, there is no individual PQC algorithm that is optimal in general deployment cases. For bulk key exchange in the large-scale networks, **ML-KEM (Kyber)** offers the most favourable trade-off: moderate key sizes, fast operations, and well-understood security reductions to the standard MLWE problem [2, 9]. For digital signatures, **ML-DSA (Dilithium)** provides a balanced performance profile suitable for certificate authorities and authentication protocols, while **FN-DSA (Falcon)** is preferable where signature compactness is paramount and signing cost is acceptable [13].

The large signatures of SPHINCS+ (SLH-DSA) do not stop it. longest possible root certificates whose most conservative choice is Its security is

predicated on its endurance through decades. not merely algebraic but only on hash-function properties. assumptions [5]. Accordingly, algorithm selection should consider not only security strength but also computational cost, communication overhead, and suitability for the target network environment [19].

9.2. *Transition Risks and Open Challenges*

Several open challenges remain before universal PQC deployment [6]:

- **Cryptographic agility:** Net stacks and PKI. the infrastructure needs to be revamped to support algorithm negotiation. and upgrading without having to be monolithic.
- **Harvest-now, decrypt-later:** Organisations handling migrating to PQC should be a high priority currently of long-lived sensitive data, before quantum computers of attack. exist [8].
- **Standardisation lag:** While NIST FIPS 203–206 are last, protocol level standards (e.g. TLS, SSH, IKEv2 RFC updates) remain in the process of finalisation. [6].
- **Implementation security:** The mathematical complexity k = lattice-based algorithms generate implementation pitfalls, e.g., because proven as early Kyber and Falcon attacks. implementations [9].
- **Metaverse and emerging digital environments:** The platform urgency is augmented with the rapid growth of immersive digital platforms. with the level of volume and sensitivity of data, PQC adoption. transmitted [20].

9.3. *Recommendations*

On the basis of the above analysis we can make the following recommendations to organisations with large-scale networks:

1. **Immediate:** Carry out a cryptographic financial reporting to check. detect all the asymmetric cryptography being used and evaluate exposure to harvest-now attacks.
2. **Near-term (1–3 years):** Implement hybrid key exchange. Modifications to TLS 1.3 and IKEv2 in support of emerging RFC: (ECDH + ML-KEM). guidance [12].
3. **Medium-term (3–7 years):** Transition certificate infrastructure to ML-DSA or FN-DSA signatures.
4. **Long-term (>7 years):** Retire classical asymmetric primitives entirely; maintain SPHINCS+ as a long-lived root certificate anchor.

10. Conclusion

This paper has presented a comprehensive comparative analysis of post-quantum cryptographic schemes over discrete algebraic structures, with a focus on their suitability for enhanced information security in large-scale networks. We examined the principal PQC families—lattice-based, code-based, hash-based, multivariate, and isogeny-based—across dimensions of security hardness

assumptions, key and ciphertext sizes, computational performance, side-channel resistance, and protocol integration feasibility.

Our analysis demonstrates that the NIST-standardised lattice-based algorithms, ML-KEM and ML-DSA, currently provide the most viable path for large-scale network migration, offering well-studied security reductions and acceptable operational overheads. SPHINCS+ (SLH-DSA) emerges as the preferred conservative choice for applications demanding long-horizon security guarantees. The hybrid approach—combining classical and post-quantum primitives—is recommended as an immediate transitional measure, providing defence in depth and backward compatibility during the migration period.

Persistent challenges, including enlarged handshake sizes, protocol standardisation latency, and implementation security of complex mathematical constructions, must be addressed through coordinated efforts between standards bodies, hardware manufacturers, and cryptographic library maintainers. The threat of harvest-now, decrypt-later attacks makes this migration time-critical: organisations with longlived sensitive data must begin transition planning immediately, ahead of cryptographically relevant quantum computers becoming available.

Future work will focus on hardware-accelerated implementations of ML-KEM and ML-DSA optimised for network appliances, formal security proofs for hybrid protocol compositions, and the development of cryptographic agility frameworks enabling seamless algorithm negotiation in heterogeneous large-scale deployments.

References

- [1] S. Rai, A. K. Upadhyay, D. Sharma, D. Raj, A. K. Gupta, and D. Ather, “Quantum cryptography—A modern approach,” *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 7, pp. 1991–2006 (2023), doi: 10.47974/JD-MS-1839.
- [2] K. C. Dekkaki, I. Tasic, and M.-D. Cano, “Exploring post-quantum cryptography: Review and directions for the transition process,” *Technologies*, vol. 12, no. 12, Art. no. 241 (2024), doi: 10.3390/technologies12120241.
- [3] S. K. Sahu and K. Mazumdar, “State-of-the-art analysis of quantum cryptography: Applications and future prospects,” *Front. Phys.*, vol. 12, Art. no. 1456491 (2024), doi: 10.3389/fphy.2024.1456491.
- [4] S. Sonko, K. I. Ibekwe, V. I. Ilojiana, E. A. Etukudoh, and A. Fabuyide, “Quantum cryptography and U.S. digital security: A comprehensive review,” *Comput. Sci. IT Res. J.*, vol. 5, no. 2, pp. 390–414 (2024), doi: 10.51594/csitrj.v5i2.790.

- [5] S. M. Hosseini and H. Pilaram, "A comprehensive review of post-quantum cryptography: Challenges and advances," *Int. J. Data Netw. Sci.*, vol. 9, no. 2, pp. 267–288 (2025), doi: 10.5267/j.ijdns.2024.12.003.
- [6] S.-Y. Chang and Q. Khan, "Post-quantum cryptography in networking protocols: Challenges, solutions, and future directions," *Cryptography*, vol. 10, no. 1, Art. no. 12 (2026), doi: 10.3390/cryptography10010012.
- [7] S. Rai, A. K. Upadhyay, M. Sah, N. Gupta, M. Singh, and D. Raj, "Secure demand and price prediction model for ride hailing apps using user encrypted data," in *Proc. 2025 Int. Conf. Networks and Cryptology (NETCRYPT)*, New Delhi, India, pp. 1753–1758 (2025), doi: 10.1109/NETCRYPT65877.2025.11102587.
- [8] Y. Baseri, V. Chouhan, and A. Hafid, "Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols," *Comput. Secur.*, vol. 142, Art. no. 103883 (2024), doi: 10.1016/j.cose.2024.103883.
- [9] J. Hekkala, M. Muurman, K. Halunen, and V. Vallivaara, "Implementing post-quantum cryptography for developers," *SN Comput. Sci.*, vol. 4, Art. no. 365 (2023), doi: 10.1007/s42979-023-01724-1.
- [10] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang, "A survey of post-quantum cryptography: Start of a new race," *Cryptography*, vol. 7, no. 3, Art. no. 40 (2023), doi: 10.3390/cryptography7030040.
- [11] J. Rubia J, B. Lincy R, E. E. Nithila, S. Shibi C, and A. Rosi, "A survey about post quantum cryptography methods," *EAI Endorsed Trans. Internet Things*, vol. 10, no. 1, Art. no. 5099 (2024), doi: 10.4108/eet-iot.5099.
- [12] V. Chouhan, M. Aldarwbi, S. Sadeghi, A. A. Ghorbani, A. Chow, and R. Burko, "Assessing the quantum readiness of cryptographic standards: Recommendations toward quantum-era compliance," *Comput. Standards Interfaces*, vol. 97, Art. no. 104114 (2026), doi: 10.1016/j.csi.2025.104114.
- [13] S. Farooq, A. Altaf, F. Iqbal, E. B. Thompson, D. L. R. Vargas, I. de la Torre Díez, and I. Ashraf, "Resilience optimization of post-quantum cryptography key encapsulation algorithms," *Sensors*, vol. 23, no. 12, Art. no. 5379 (2023), doi: 10.3390/s23125379.

- [14] A. Singh, P. Kumar, A. Kumar, N. Gupta, R. N. Ravikumar, and D. Raj, "An efficient and secure mobile agent-based model for medical health care data protection," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 6, pp. 2503–2519 (2026), doi: 10.47974/JDMSC-2756.
- [15] O. Popoola, M. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, and J. Popoola, "An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security," *Internet Things*, vol. 27, Art. no. 101314 (2024), doi: 10.1016/j.iot.2024.101314.
- [16] G. Routis, G. Katsouris, and I. Roussaki, "Cryptography-based location privacy protection in the Internet of Vehicles," *J. Ambient Intell. Humanized Comput.*, vol. 15, no. 8, pp. 3119–3139 (2024), doi: 10.1007/s12652-024-04752-8.
- [17] R. S. Shukla, D. Ather, D. Raj, A. Jain, T. Sarkar, and M. Rakhra, "A secure and intelligent framework for cyber threat detection using machine learning," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 6, pp. 2441–2457 (2026), doi: 10.47974/JDMSC-2752.
- [18] R. Kuang and A. Chan, "Quantum encryption in phase space with displacement operators," *EPJ Quantum Technol.*, vol. 10, Art. no. 26 (2023), doi: 10.1140/epjqt/s40507-023-00183-0.
- [19] M. S. Adhikari, R. Gupta, D. Raj, A. K. Sagar, D. Ather, and A. K. Agrawal, "Enhancing energy efficiency in IoT via cellular network integration," in *Energy Efficient Internet of Things-Based Wireless Sensor Network*, A. Panwar, V. Jain, U. Sugandh, and V. Kukreja, Eds. Hoboken, NJ, USA: Wiley, pp. 91–133 (2026), doi: 10.1002/9781394314751.ch4.
- [20] M. Tukur, J. Schneider, M. Househ, A. H. Dokoro, U. I. Ismail, M. Dawaki, and M. Agus, "The metaverse digital environments: A scoping review of the challenges, privacy and security issues," *Front. Big Data*, vol. 6, Art. no. 1301812 (2023), doi: 10.3389/fdata.2023.1301812.

Received January, 2026