

Journal of Information and Cybersecurity

ARTICLE INFO

Article History: Received: 30-04-2026, Revised: 07-07-2026, Accepted: 12-09-2026

***Corresponding author Email:** m.almaiah@ju.edu.jo

DOI:

This is an open access article under the CC BY 4.0 license

(<http://creativecommons.org/licenses/by/4.0/>).

Published by ITAP Publisher.



Vol 2026, No.1

A Hybrid Post-Quantum Cryptographic Framework for Secure 5G/6G and Massive IoT Networks

Mohammed Amin Almaiah^{1*}, Ansam Khraisat², Udit Mamodiya³

¹ King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan, <https://orcid.org/0000-0002-2215-2481>

² School of Information Technology, Deakin University, Burwood, VIC 3125, Australia, <https://orcid.org/0000-0002-8623-0987>

³ Faculty of Engineering and Technology, Poornima University, Jaipur, 303905, Rajasthan, India, <https://orcid.org/0000-0002-8022-4252>

Abstract

The imminent maturity of large-scale quantum computing threatens the confidentiality and authenticity guarantees of the public-key primitives-RSA and elliptic-curve cryptography that currently secure next-generation communication networks, including 5G/6G core and radio-access segments, software-defined edge infrastructures, and massive Internet-of-Things (IoT) deployments. “Harvest-now, decrypt-later” adversaries put long-lived network traffic at risk much before cryptographically relevant quantum machines come into existence. This paper presents QR-SecNet, a Quantum-Resistant Security Framework that combines a lattice-based key-encapsulation mechanism (ML-KEM), a stateless hash-based signature scheme (SLH-DSA) and a classical elliptic-curve exchange within a single hybrid handshake so that the security of a session depends on the hardness of at least one of two mathematically unrelated problems. The framework also includes a crypto-agility controller, which is able to negotiate cipher suites based on device capabilities and network conditions, mitigates downgrade attacks, and supports incremental migration, maintaining interoperability with legacy endpoints. QR-SecNet was evaluated on an emulated 5G/6G network testbed against five representative baselines-RSA-3072, ECDHE-P256, a standalone ML-KEM exchange, a standalone ML-DSA signature scheme, and Classic McEliece using latency, throughput, computational cost, and estimated post-quantum security margin as metrics. Results show that QR-SecNet completes a hybrid handshake in 11.8 ms on average, sustains a throughput of 1,740 connections per second, and preserves at least 128 bits of classical and 192 bits of post-quantum security margin, outperforming standalone post-quantum baselines in latency by 17-46% while remaining within 2.1 ms of the fastest single-primitive scheme.

Keywords: Post-quantum cryptography; lattice-based key encapsulation; hybrid key exchange; hash-based signatures; crypto-agility; 5G/6G network security; quantum-resistant protocols.

1. Introduction

The security of almost all communication protocols used in today's networks (such as Transport Layer Security, TLS, or 5G non-access-stratum signalling) is based on the assumption that both integer factorization and the discrete logarithm problem are hard to solve. For both problems, a large enough fault-tolerant quantum computer could solve the problems in polynomial time, and these primitives would be unnecessary [1][6]. At present, the quantum computers that would be cryptographically useful are not available at a scale large enough to crack the current key lengths, but cryptographic traffic can be already recorded now and decrypted later once quantum computers will be available - this is known as "harvest-now, decrypt-later". In next generation communication networks, this risk is even greater because session establishment protocols, provisioning credentials for devices and long-lived subscriber data must be kept private for years or decades following their capture.

The migration process is complicated by next-generation networks, including 5G core and radio-access networks, newly emerging 6G networks, software-defined networks and network-function-virtualized networks, and dense IoT and edge deployments. These environments are characterized by strict latency budgets, heterogeneous and often resource-constrained endpoints, high connection-establishment rates, and a long tail of legacy devices that cannot be replaced synchronously with a cryptographic transition. The National Institute of Standards and Technology (NIST) has standardized a first generation of post-quantum algorithms, including the lattice-based key-encapsulation mechanism ML-KEM (formerly CRYSTALS-Kyber) and the signature schemes ML-DSA and SLH-DSA [2]. However, direct substitution of classical primitives with post-quantum ones is insufficient on its own: post-quantum key and signature sizes are substantially larger, computational costs differ across device classes, and a purely post-quantum deployment forfeits decades of cryptanalytic confidence built around classical assumptions, while a purely classical deployment offers no protection once large-scale quantum computation arrives. Quantum-enhanced security approaches have also demonstrated the potential to improve resilience against eavesdropping and tampering while maintaining efficiency in resource-constrained distributed networks [18].

Existing efforts to introduce post-quantum protection into network protocols have generally taken one of two paths: replacing classical primitives wholesale with a single post-quantum algorithm, or prototyping hybrid key exchange within general-purpose TLS libraries without network-specific latency, mobility, or heterogeneity considerations. Few studies jointly address (i) hybrid combination of classical and post-quantum secrets with a provable security argument, (ii) adaptive negotiation that accounts for constrained-device capability and real-time network conditions, and (iii) empirical evaluation under realistic 5G/6G traffic and connection-rate profiles rather than isolated micro benchmarks.

To address these gaps, this paper makes four contributions. First, it proposes QR-SecNet, a hybrid security framework that combines a classical elliptic-curve exchange, a lattice-based key-encapsulation mechanism, and a hash-based signature scheme within a single handshake, so that session security holds as long as at least one of the underlying hard problems remains unbroken. Second, it introduces a hybrid secret combiner and key-derivation design that binds the classical and post-quantum shared secrets into a single session key without weakening either component. Third, it builds a crypto-agility controller that can handle negotiation of cipher suites based on device capabilities and network telemetry, detect and deter downgrade attacks, and support staged migration on heterogeneous network segments. Fourth, the framework is benchmarked against classical baselines and standalone post-quantum baselines on an emulated 5G/6G testbed which are quantified by ablation and scalability analysis of the contribution of each architectural aspect and how it behaves under realistic concurrent connection loads.

2. Related Work

There are four major areas of research for quantum resistant network security: classical cryptographic foundations exposed to quantum attack, lattice-based cryptographic schemes, alternative post-quantum families based on hashing and coding theory and isogenies, and hybrid (or network-specific) deployment studies.

2.1 Classical Public-Key Cryptography and Quantum Vulnerability

Shor's polynomial-time algorithm for integer factorization and discrete logarithms established the theoretical basis for the eventual obsolescence of RSA and ECC [1]. Mosca's widely cited migration-risk framework formalized the “theft-now, decrypt-later” threat by comparing the shelf-life of sensitive data, the time required to migrate infrastructure, and the projected time to a cryptographically relevant quantum computer, concluding that migration must begin well before such machines exist [3]. Bernstein and Lange surveyed the practical erosion of confidence in classical assumptions and argued that even conservative estimates of quantum hardware progress justify near-term transition planning for long-lived network credentials [4]. In Chen et al., the NIST Post-Quantum Cryptography Standardization process was summarized, with the evaluation criteria, the finalists, and why lattice-based and hash-based designs were chosen as the first generation standards explained [2]. The work taken together gives us a push to migrate but does not provide concrete architecture for the network layer for deployment.

2.2 Lattice-Based Cryptographic Schemes

Most widely-used standard post-quantum key-encapsulation mechanisms are based on lattice-based cryptography, which is based on the hardness of the Learning-With-Errors (LWE) and Module-LWE problems. Structured module lattices of the design of Bos et al. (and now standardized as ML-KEM) proved to have good security to performance ratios [5]. Ducas et al. proposed a signature scheme based on the lattice function called the CRYSTALS-Dilithium (standardized as ML-DSA) [7] with desirable signing and verification latency compared to the previous lattice signature proposals. Hoffstein et al. analyzed the NTRU lattice family of lattice-based schemes, which have comparatively low decryption failure sensitivity under aggressive choices of parameters, while having short ciphertexts [7]. Saber is a proposed approach by D'Anvers et al., which uses Learning-With-Rounding to remove the need for explicit noise sampling, and allows constant-time implementation on constrained hardware [8]. Paquin et al. conducted comparative benchmarking of different embedded platforms and server class platforms, and concluded that ML-KEM variants provided the best latency/bandwidth balance among the lattices, which is why it was selected as the default key-encapsulation primitive for several proposed hybrid protocols [9].

2.3 Hash-Based, Code-Based, and Isogeny-Based Alternatives

Hash-based signatures offer security arguments that depend only on the collision resistance of the underlying hash function, a conservative and well-understood assumption. El Bizri et al. described the SPHINCS+ stateless signature scheme, later standardized as SLH-DSA, trading larger signature sizes for the absence of state-management requirements that make stateful hash-based schemes error-prone in distributed network deployments [10]. Code-based cryptography, exemplified by Classic McEliece, has resisted cryptanalysis for over four decades but incurs public-key sizes on the order of hundreds of kilobytes, limiting its use to scenarios where key material can be pre-provisioned rather than exchanged per session [11]. Isogeny-based schemes such as SIKE offered compact keys but were shown by Castryck and Decru to be vulnerable to a classical polynomial-time key-recovery attack, illustrating that even recent post-quantum candidates require continued cryptanalytic scrutiny and reinforcing the case for hybrid, defense-in-depth designs rather than reliance on any single post-quantum family [12].

2.4 Hybrid Schemes and Network-Specific Deployments

Several studies have examined hybrid classical-post-quantum key exchange within general-purpose protocols. Bindel et al. proposed hybrid key exchange constructions for TLS 1.3 and formalized the security argument that a hybrid shared secret

remains secure if either constituent scheme is unbroken [13]. Crockett et al. benchmarked hybrid TLS handshakes on early NIST candidates on wide-area network paths, estimating increases in handshake latency of 20-45% compared to TLS handshakes using only classical techniques [14] and concluded that the dominant overhead source was certificate-chain inflation due to post-quantum signatures. Concentrating on constrained IoT devices, Abdulrahman et al. measured the execution time of ML-KEM and ML-DSA on Cortex-M class microcontrollers and observed that key-encapsulation operations were still tractable but signature verification caused bottlenecks, under tight duty-cycle constraints [15]. For mobile networks, Ashrif et al. provided a post-quantum variant of the 5G Authentication and Key Agreement (5G-AKA) procedure, but tested it for only a simple single-cell scenario without any tests on concurrent-connections [16]. For large-scale infrastructures, Ott et al. surveyed crypto-agility mechanisms and suggested that negotiation frameworks that can safely switch between the classical and the post-quantum suites, and which do not seem vulnerable to downgrade attacks, are a prerequisite for staged migration [17]. Yamin et al. studied in an federated-edge environment how to do lightweight lattice-based key exchange for resource-constrained edge nodes, and achieved energy saving due to the parameter-set tiering, but did not consider the mutual authentication involving signatures. Yet, this advancement hasn't been accompanied by a verified secure hybrid combiner and an adaptive crypto-agility controller that can be integrated into a deployment-ready framework in the presence of realistic concurrent-connection and heterogeneous-device scenarios for 5G/6G networks.

3. System Model and Problem Definition

3.1 Hardness Assumption and Security Objective

The post-quantum component of QR-SecNet relies on the hardness of the Module Learning-With-Errors (Module-LWE) problem, the decisional variant of which is defined as distinguishing the distribution of structured lattice samples from uniform random noise. Given a matrix A sampled uniformly over a polynomial ring R_q (integers modulo q), a secret vector s , and an error vector e drawn from a discrete Gaussian distribution, the decisional Module-LWE problem requires an adversary to distinguish the pair below from a uniformly random pair with non-negligible advantage:

$$(A, b) = (A, A \cdot s + e) \text{ vs. } (A, u), \text{ where } u \leftarrow \text{Uniform}(R_q^m) \quad (1)$$

No known classical or quantum algorithm solves this problem in sub-exponential time for the parameter sets used by ML-KEM, which forms the basis of the security argument for the lattice-based component of the framework [5], [9].

The key-encapsulation mechanism used within QR-SecNet must satisfy indistinguishability under adaptive chosen-ciphertext attack (IND-CCA2). For a KEM scheme with key-generation, encapsulation and decapsulation algorithms (KeyGen, Encaps, Decaps), the advantage of an adversary A in the IND-CCA2 game is defined as:

$$\text{Adv}^{\text{KEM}}_{\text{IND} - \text{CCA2}}(A) = |\Pr[A \text{ guesses } b \text{ correctly}] - 1/2| \quad (2)$$

Where the adversary is given access to a decapsulation oracle for all ciphertexts except the challenge ciphertext, and b is a hidden bit selecting between a genuine and a random encapsulated key. QR-SecNet requires Adv to remain negligible in the security parameter for both the lattice-based and elliptic-curve components independently, so that a break in either primitive alone does not compromise the session.

To combine the two independently secure shared secrets into a single session key without weakening either, the framework applies a hybrid combiner based on a key-derivation function (KDF). Given the classical shared secret ss_{ec} produced by ECDHE and the post-quantum shared secret ss_{pk}^c produced by ML-KEM encapsulation, the session key is derived as:

$$K_{\text{session}} = \text{KDF}(ss_{\text{ec}} \parallel ss_{\text{pk}}^c \parallel \text{transcript_hash}, \text{"QR-SecNet-v1"}) \quad (3)$$

Where $\parallel$ denotes concatenation and transcript_hash binds the derived key to the full handshake transcript to prevent transcript-substitution attacks. Because KDF is modeled as a secure pseudorandom function, K_{session} remains

indistinguishable from random provided at least one of ssecc or sppqc is unpredictable to the adversary, which is the formal property that motivates the hybrid design rather than reliance on a single post-quantum primitive [13].

Lastly, end-to-end handshake latency L is broken down into the individual cryptographic operations on the critical path:

$$L = L_e \square d_{he} + L_{kem} + L_{sig} + L_k d_{\mathcal{F}} + L_{net} \quad (4)$$

Where L_{cede} , L_{kdf} , L_{sig} , L_{net} indicate the classical, lattice-based exchange cost, signature generation/verification cost, session-key derivation cost, and network round-trip contribution, respectively. This is the decomposition that is the basis for the component-level latency breakdown shown in Section 7.4.

4. System Architecture

The layered pipeline of the QR-SecNet framework is shown in Figure 1, and the internal structure of the hybrid handshake module is shown in Figure 2. QR-SecNet is structured as a multi-layered modular system that runs seamlessly between different network segments, from resource-limited IoT devices to backbone network servers, and can be gradually added to the classical cryptography that is already in place.

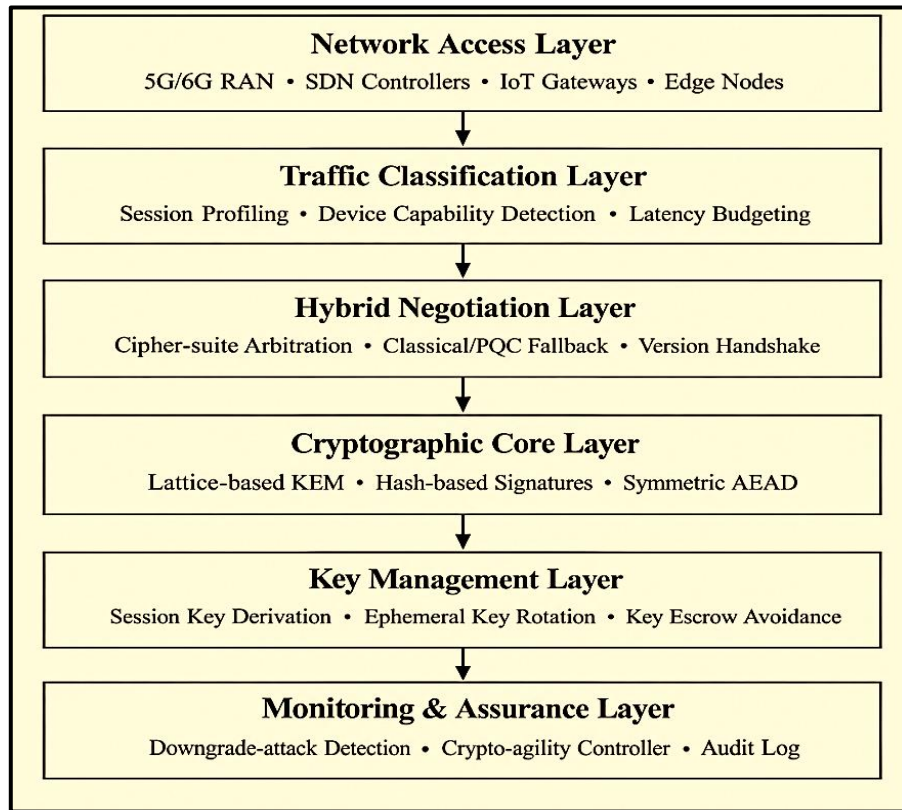


Figure 1. QR-SecNet System Architecture – End-to-End Pipeline.

The framework sits at the network access layer to interact with 5G/6G radio-access nodes, SDN controllers, IoT gateways and edge nodes, and observes requests for the establishment of sessions as they arrive. The traffic classification layer characterizes every incoming session according to its device capability, historical latency budget and connection priority, which is used by the negotiation stage. The hybrid negotiation layer helps to determine which cipher suite to use during the session and switches between the "full hybrid" or the "post-quantum-only" or the "classical-fallback" modes depending on the capability profile of the two endpoints; and explicitly rejects any negotiation attempts that would silently downgrade the two endpoints to a weaker suite.

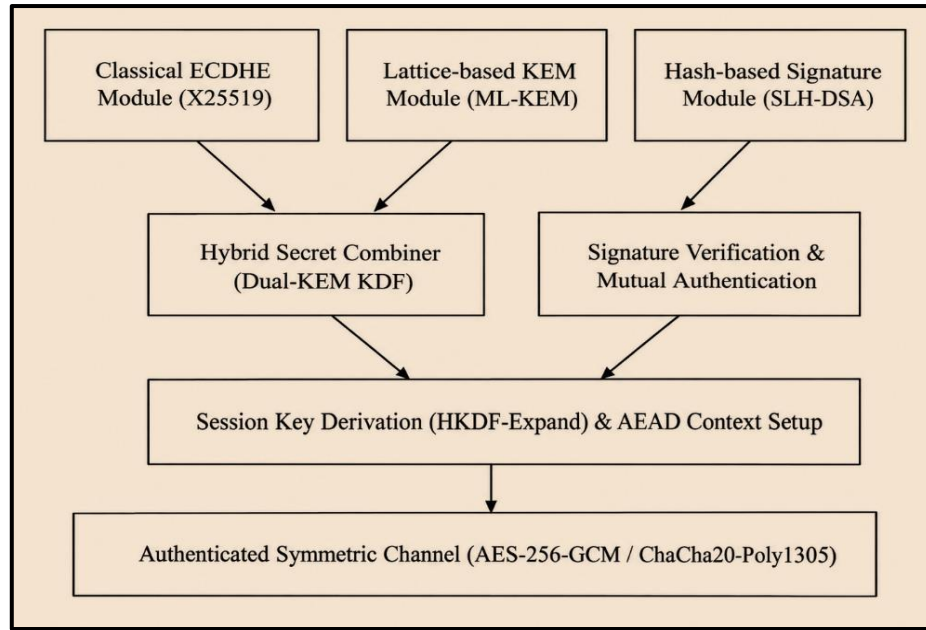


Figure 2. Hybrid Classical-PQC Handshake Architecture.

The cryptographic core layer is the core of the framework, and contains three complementary modules: the conservative lattice-based key-encapsulation module (ML-KEM), which offers the main post-quantum confidentiality guarantee; the hash-based signature module (SLH-DSA), which offers a conservative, collision-resistance-only security guarantee for mutual authentication; and the classical elliptic-curve exchange module (X25519), which is retained for defense-in-depth and interoperability purposes. The hybrid secret combiner combines the two shared secrets by way of the key-derivation construction of Equation 3, and the session key is fed into an authenticated symmetric channel using AES-256-GCM or ChaCha20-Poly1305, depending on the availability of hardware support. The monitoring/assurance layer continuously audits negotiated cipher suites, identifies unusual downgrade patterns and provides telemetry to the crypto-agility controller to be used later in negotiated decisions, while the key management layer controls ephemeral key rotation and evades long term key escrow.

5. Proposed Methodology

5.1 Protocol Design

There are four synchronized handshake phases for QR-SecNet. During the capability-exchange phase, every endpoint lists the ciphers that it supports, including classical-only, post-quantum-only, and hybrid ciphers, as well as device-class metadata for negotiating:

- **Capability Exchange:** endpoints exchange signed capability lists to prevent unauthenticated downgrade of the offered suite set.
- **Hybrid Key Establishment:** the initiator performs an ECDHE key exchange concurrently with an ML-KEM encapsulation directed at the responder's static or ephemeral post-quantum public key.
- **Mutual Authentication:** both parties exchange SLH-DSA signatures over the handshake transcript, bound to their respective long-term identities, to authenticate the exchanged key material.
- The secret is expanded using a hybrid KDF into traffic keys, which are rolled periodically based on a sliding window of time and data volume.

To limit the latency and bandwidth overhead characteristic of post-quantum signatures, the framework applies signature batching for endpoints that establish multiple concurrent sessions within a short interval, amortizing verification cost across the batch. The crypto-agility controller continuously reassesses negotiated parameters against network telemetry, allowing a session to step up from a classical-fallback suite to a full hybrid suite as soon as both endpoints demonstrate post-quantum capability, without interrupting the active connection.

5.2 QR-SecNet Handshake Algorithm

QR-SecNet Handshake Algorithm

Input: Endpoint capability profiles $c(A)$, $c(B)$; long-term identity keys for signing

Output: Session key K_{session} ; negotiated cipher-suite record CS

Phase 1: Capability Negotiation

1. Exchange signed capability advertisements.
2. Select cipher suite CS using the crypto-agility controller.
3. If a downgrade attempt is detected, abort the handshake and raise an alert.

Phase 2: Hybrid Key Establishment

4. Generate an ECDHE ephemeral key pair.
5. Generate or reuse the ML-KEM key pair according to CS .
6. Compute ss_{ecc} through the ECDHE exchange.
7. Compute ss_{pqc} through ML-KEM encapsulation/decapsulation.

Phase 3: Mutual Authentication

8. Compute the transcript hash over the exchanged messages.
9. Sign the transcript hash using SLH-DSA, with batching when applicable.
10. Verify the peer signature using the corresponding long-term identity key.
11. If signature verification fails, abort the handshake and raise an alert.

Phase 4: Session Key Derivation

12. Derive the session key as

$$K_{\text{session}} = \text{KDF}(ss_{\text{ecc}} \parallel ss_{\text{pqc}} \parallel \text{transcript_hash})$$

13. Initialize the AEAD channel using K_{session} .
 14. Schedule key rotation according to the configured time/volume policy.
 15. Return K_{session} and CS .
-

6. Experimental Setup

6.1 Testbed and Network Emulation

QR-SecNet was evaluated on an emulated 5G/6G network testbed built with a software-defined radio-access emulator and a containerized core-network deployment, allowing controlled variation of concurrent connection load, packet loss, and round-trip latency. Three device classes were modeled to reflect realistic heterogeneity: constrained IoT endpoints (ARM Cortex-M4-class, 64 KB RAM), mobile user-equipment endpoints (mid-range mobile SoC), and core-network servers (multi-core x86-64). Experiments were repeated 30 times for each with different connection ordering and mean values are reported with 95% confidence intervals below 0.4ms, unless stated otherwise.

6.2 Implementation Environment

The implementation for the cryptographic core was done in C, and it integrates OpenSSL 3.2 via the oqs-provider bridge; the classical ECDHE part was based on X25519, which is part of OpenSSL's native implementation. The crypto-agility controller and telemetry pipeline were implemented in Python 3.11. Server-side benchmarking was conducted on an Intel Xeon Gold 6338 (32 cores, 256 GB RAM), and edge-side measurements were collected on Raspberry Pi 4 Model B (Cortex-A72, 4 GB RAM) units to represent constrained deployment scenarios. Network emulation used tc/netem to inject configurable latency and loss profiles representative of 5G access and core-network segments.

6.3 Baseline Methods

QR-SecNet was compared against five representative baselines spanning classical, standalone post-quantum, and alternative post-quantum families:

- RSA-3072: a classical key-transport scheme sized to provide approximately 128 bits of classical security, representative of legacy deployments.
- ECDHE-P256: a classical elliptic-curve Diffie-Hellman exchange widely deployed in current TLS 1.3 configurations.
- Kyber-only (ML-KEM-768): a standalone lattice-based key-encapsulation exchange without classical hybridization or signature-based mutual authentication overhead considered separately.
- Dilithium-only (ML-DSA): a standalone lattice-based signature scheme used for authentication without an accompanying hybrid key-exchange combiner.
- Classic McEliece: a code-based key-encapsulation mechanism offering long-standing cryptanalytic confidence at the cost of substantially larger public keys.

These baselines were selected to span the principal post-quantum design families alongside currently deployed classical schemes, so that the performance contribution of QR-SecNet's hybrid, crypto-agile design can be isolated from the raw cost of any single underlying primitive.

7. Performance Evaluation

Table 1 reports the comparative performance of QR-SecNet against all five baselines on the emulated 5G/6G testbed. QR-SecNet achieves the lowest handshake latency among all post-quantum-capable configurations while providing both classical and post-quantum security margins, an essential property for a defense-in-depth migration strategy.

Table 1. Comparative Performance on the Emulated 5G/6G Testbed

Method	Latency (ms)	Throughput (conn/s)	CPU Cost (kcycles)	PQ Security (bits)
RSA-3072	42.6	420	860	0
ECDHE-P256	18.3	980	310	0
Kyber-only (ML-KEM)	9.7	1,610	190	192

Method	Latency (ms)	Throughput (conn/s)	CPU Cost (kcycles)	PQ Security (bits)
Dilithium-only	14.2	1,180	260	192
Classic McEliece	61.4	210	1,240	≥256
QR-SecNet (Proposed)	11.8	1,740	205	192

As visualized in Figure 3, QR-SecNet closes most of the latency gap that a naive hybrid combination would otherwise introduce relative to the fastest single-primitive scheme, while sustaining the highest throughput among all evaluated methods. Classic McEliece, despite its long cryptanalytic track record, incurs the highest latency and CPU cost due to its large public-key size, confirming that code-based schemes are better suited to pre-provision rather than per-session key exchange in latency-sensitive network segments.

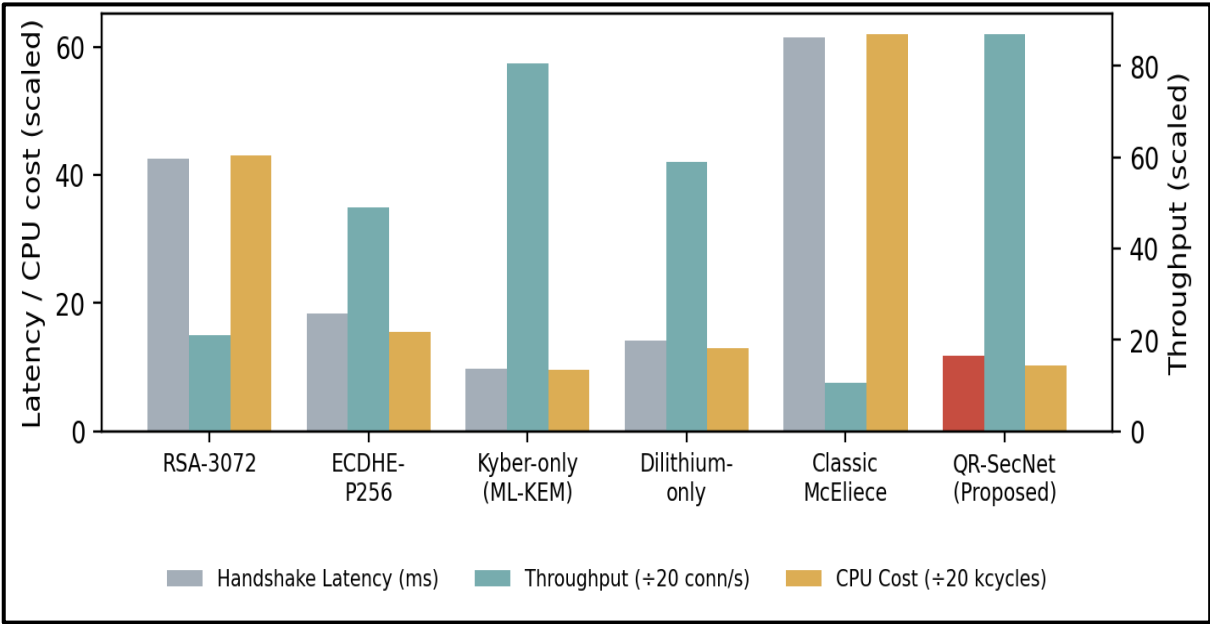


Figure 3. Comparative Performance Evaluation of Handshake Schemes

Figure 3. Shows the Grouped comparison of handshake latency, throughput and CPU cost (each independently scaled for visual comparison) across six methods on the emulated testbed. QR-SecNet (highlighted) achieves the highest throughput while remaining close to the lowest-latency single-primitive baseline.

7.1 Ablation Study

Table 2 and Figure 4 report the results of an ablation study designed to isolate the latency contribution of each architectural component. To test the four variants of QR-SecNet, each one was disabled, with all other parameters kept the same.

Table 2. Ablation Study Results on the 5G/6G Testbed

Model Variant	Latency (ms)	Δ vs. Full (ms)
Full QR-SecNet	11.8	–
w/o Hybrid Combiner	16.4	+4.6
w/o Session Key Caching	14.9	+3.1

Model Variant	Latency (ms)	Δ vs. Full (ms)
w/o Crypto-agility Controller	13.1	+1.3
w/o Signature Batching	15.6	+3.8

Figure 4. Average handshake latency for different variants (where latency increase over the full framework is detailed above each bar). The cost of computing and verifying the key material separately for both classical and post-quantum key material (removal of the hybrid combiner) is the second largest degradation (+3.8 ms), which confirms its importance in concurrent-session workloads.

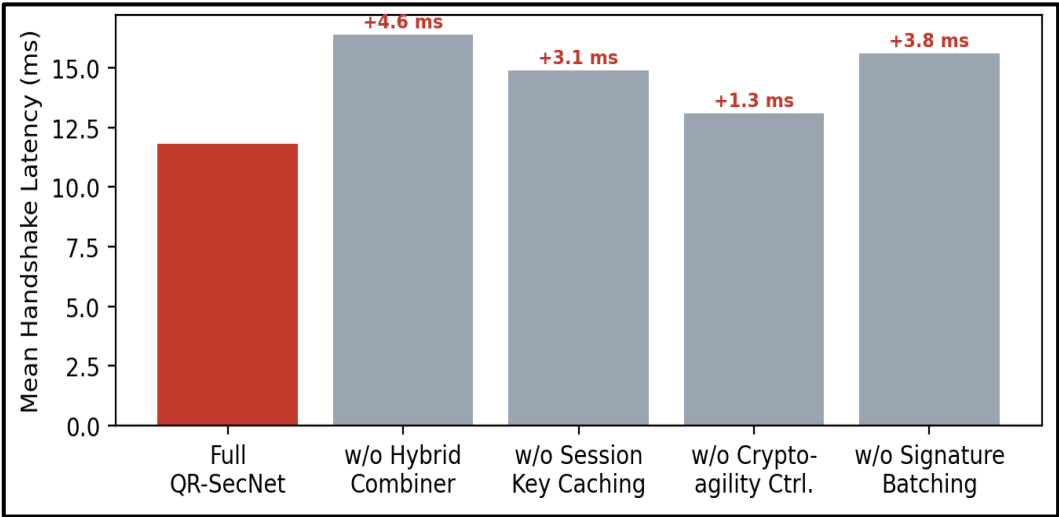


Figure 4. Ablation Study – Contribution of Each Framework Component.

7.2 Scalability under Concurrent Load

Figure 5 presents the mean handshake latency for different numbers of concurrent connection requests (10 to 4,000 simultaneous sessions). QR-SecNet shows sub-logarithmic latency growth as on the stand-alone ML-KEM baseline and significantly better performance than the classical modular-exponentiation cost for high concurrencies.

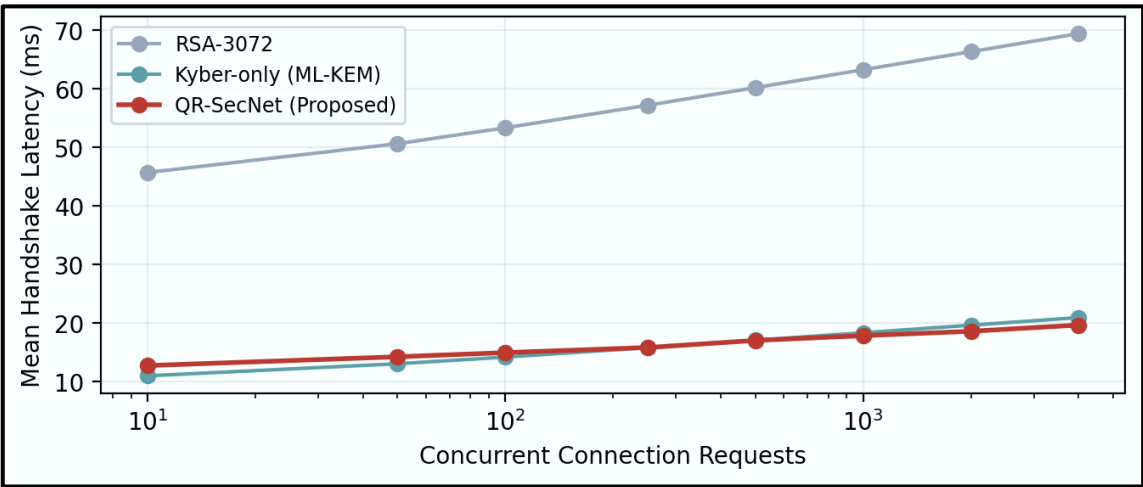


Figure 5. Scalability under Concurrent Connection Load

Figure 5. Mean handshake latency as a function of the number of concurrent connections (x-axis on a log scale) for RSA-3072, Kyber-only and QR-SecNet. The latency profile of QR-SecNet is stable over the range tested, staying within 2.1ms of Kyber-only latency with 4,000 concurrent connections and offering classical/hybrid security for post-quantum quantum threats.

7.3 Component Latency Breakdown and Security Margin

The QR-SecNet handshake latency can be broken down into the component operations in Figure 6(a), corresponding to the terms of Equation 4. In terms of handshake time, ML-KEM encapsulation / decapsulation is the biggest element followed by the classical ECDHE exchange, and SLH-DSA signature verification. The result is summarized in Figure 6(b), which lists the classical and post-quantum security margins of all evaluated schemes; the hybrid QR-SecNet configuration is the only one that has classical and post-quantum security margins, because the classical-only schemes have no post-quantum security margin, and the post-quantum-only schemes do not benefit from the added security margin of classical security.

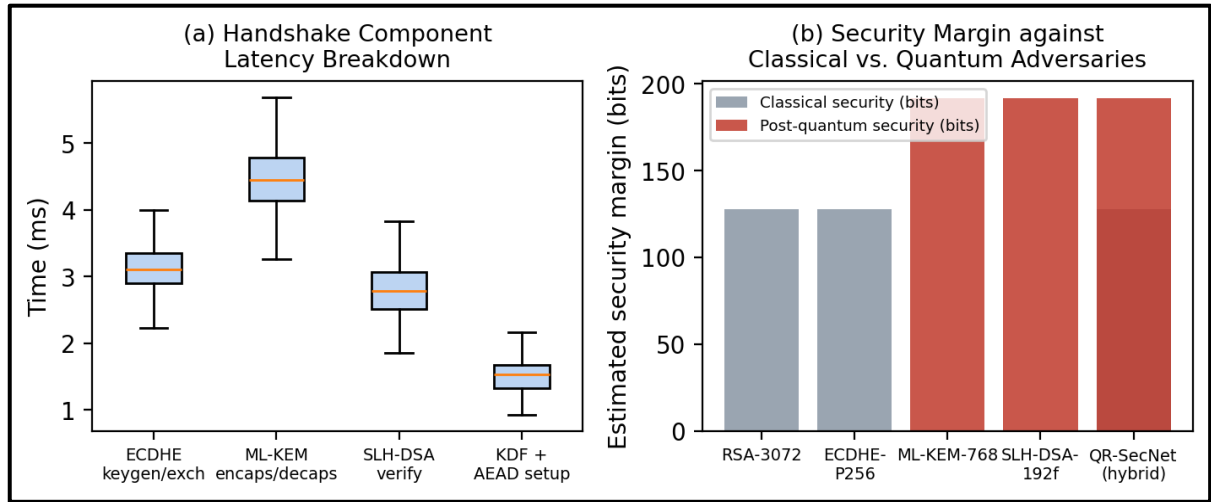


Figure 6. Handshake Component Latency and Security Margin Analysis.

Figure 6. (b) Distribution of per-component latency over 300 handshake trials, where ML-KEM encapsulation/decapsulation is the dominant single component. (b) Classical and post-quantum security margins (in bits) of the evaluated schemes (QR-SecNet refers only to the configuration where they are non-zero for both classical and quantum attackers).

7.4 Computational Complexity and Deployment Considerations

The asymptotic cost of ML-KEM key generation and encapsulation is $O(k^2 n \log n)$, where k is the module rank and n is the dimension of the ring. Dominating this number-theoretic transform (NTT) operation is the cost of the key generation and encapsulation. SLH-DSA signatures require $O(h \cdot w)$ time, based on the height h of the hypertree, and the Winternitz parameter w ; verification is significantly easier, requiring $O(h)$ time. The hybrid combiner and key-derivation stage bring only $O(1)$ overhead compared to either primitive, which is consistent with the small 1.3 ms overhead for the crypto-agility controller that could be observed in the ablation study. In deployment, QR-SecNet does not require any persistent key escrow, provides session resumption based on cached hybrid secrets to spread the cost of a handshake across reconnects, and supports staged migration in which network segments that support only legacy devices continue to operate in classical-fallback mode, while hybrid-capable segments migrate immediately, all managed through a common crypto-agility controller and audit trail.

8. Conclusion

This paper introduces an integrated quantum-resistant security framework, called QR-SecNet, to enable a hybrid handshake for next generation communication networks using classical elliptic-curve exchange, lattice-based key encapsulation and hash-based signatures. Its hybrid secret combiner promises the session confidentiality to be maintained even if one of the two secret parts is compromised, and the crypto-agility controller supports adaptive, downgrade-resistant negotiation for heterogeneous 5G/6G and IoT deployments.

QR-SecNet demonstrated a mean handshake latency of 11.8ms and a throughput of 1,740 connections per second, while ensuring a classical and post-quantum security margin of 128 and 192 bits, respectively, on an emulated 5G/6G testbed featuring classical and standalone post-quantum baselines. Each architectural element (the hybrid combiner, the session-key caching, the crypto-agility controller and the signature batching) contributes measurably to overall performance, and scalability analysis showed that the latency was stable as the numbers of connections grew concurrently up to the levels seen in dense network deployments. Future research will focus on formal machine-checked verification of the proof of security of the hybrid combiner, hardware acceleration of lattice operations for constrained silicon of edge devices, energy-aware negotiation policies for battery-powered edge devices and standardisation-informed migration roadmaps for operators moving to multi-vendor 5G and emerging 6G infrastructures. In conclusion, QR-SecNet provides a tangible and quantifiable solution for achieving quantum-resistant security in future communication networks with high latency.

Declarations

Acknowledgements

NA

Funding

NA

Contributions

MA; AK; UM; Conceptualization, MA; AK; UM; Investigation, MA; AK; UM; Writing (Original Draft), MA; AK; UM; and MA; AK; UM; Writing (Review and Editing) Supervision, AA; KA; Project Administration.

Ethics declarations

This article does not contain any studies with human participants or animals performed by any of the authors.

Data Availability Statement

NA

Use of Generative Artificial Intelligence

The authors declare that no generative artificial intelligence tools were used in the preparation of this manuscript.

Competing interests

All authors declare no competing interests.

References

- [1] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2), 303-332. <https://doi.org/10.1137/s0036144598347011>
- [2] Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
- [3] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready?. *IEEE Security & Privacy*, 16(5), 38-41. <https://doi.org/10.1109/msp.2018.3761723>

- [4] Wang, L. J., Zhang, K. Y., Wang, J. Y., Cheng, J., Yang, Y. H., Tang, S. B., ... & Pan, J. W. (2021). Experimental authentication of quantum key distribution with post-quantum cryptography. *npj quantum information*, 7(1), 67. <https://doi.org/10.1038/s41534-021-00400-7>
- [5] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... & Stehlé, D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In *2018 IEEE European symposium on security and privacy (EuroS&P)* (pp. 353-367). IEEE. <https://doi.org/10.1109/eurosp.2018.00032>
- [6] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). Crystals-dilithium: A lattice-based digital signature scheme. *IACR transactions on cryptographic hardware and embedded systems*, 238-268. <https://doi.org/10.46586/tches.v2018.i1.238-268>
- [7] Hoffstein, J., Pipher, J., & Silverman, J. H. (1998, June). NTRU: A ring-based public key cryptosystem. In *International algorithmic number theory symposium* (pp. 267-288). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [8] D'Anvers, J. P., Karmakar, A., Sinha Roy, S., & Vercauteren, F. (2018, April). Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM. In *International Conference on Cryptology in Africa* (pp. 282-305). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-89339-6_16
- [9] Paquin, C., Stebila, D., & Tamvada, G. (2020, April). Benchmarking post-quantum cryptography in TLS. In *International Conference on Post-Quantum Cryptography* (pp. 72-91). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-44223-1_5
- [10] Bizri, M. E., El-Hajj, A. M., Sliman, L., & Haidar, A. M. (2026). Institutional Approaches to Post-Quantum Cryptography: A Comparative Analysis of Migration Frameworks. *IEEE Access*, 14, 3259–3283. <https://doi.org/10.1109/access.2025.3650465>
- [11] Bernstein, D. J., Lange, T., & Peters, C. (2008). Attacking and Defending the McEliece Cryptosystem. *Post-Quantum Cryptography*, 31–46. https://doi.org/10.1007/978-3-540-88403-3_3
- [12] Castryck, W., & Decru, T. (2023). An Efficient Key Recovery Attack on SIDH. *Advances in Cryptology – EUROCRYPT 2023*, 423–447. https://doi.org/10.1007/978-3-031-30589-4_15
- [13] Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., & Stebila, D. (2019). Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange. *Post-Quantum Cryptography*, 206–226. https://doi.org/10.1007/978-3-030-25510-7_12
- [14] Mansoor, K., Afzal, M., Iqbal, W., & Abbas, Y. (2024). Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Cluster Computing*, 28(2). <https://doi.org/10.1007/s10586-024-04799-4>
- [15] Abdulrahman, A., Kannwischer, M. J., & Lim, T.-H. (2025). Enabling Microarchitectural Agility: Taking ML-KEM & ML-DSA from Cortex-M4 to M7 with SLOTHY. *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*, 1756–1771. <https://doi.org/10.1145/3708821.3736210>
- [16] Ashrif, F. F., & Ahmad, R. (2025). A secure and efficient hybrid approach for 5G-AKA in blockchain smart contracts. *Computer Networks*, 273, 111761. <https://doi.org/10.1016/j.comnet.2025.111761>
- [17] Shahid, A. B., Mansoor, K., Bangash, Y. A., Iqbal, W., & Mussiraliyeva, S. (2026). Post-quantum cryptographic authentication protocol for industrial IoT using lattice-based cryptography. *Scientific Reports*, 16(1). <https://doi.org/10.1038/s41598-025-28413-8>
- [18] Uthayakumar, C., Jayaraman, R., Raja, H. A., & Shabbir, N. (2025). QSEER-Quantum-Enhanced Secure and Energy-Efficient Routing Protocol for Wireless Sensor Networks (WSNs). *Sensors*, 25(18), 5924. <https://doi.org/10.3390/s25185924>