INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 01 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-578 PAGE NO: 021-027

TOWARDS QUANTUM-RESILIENT 6G: STATE-OF-THE-ART IN POST- QUANTUM AUTHENTICATION AND KEY EXCHANGE PROTOCOLS

V. TAMILSELVI
Research Scholar,
Department of Computer Science,
Edayathangudy. G.S. Pillay Arts and Science College (A),
Affiliated to Bharathidasan University,
Nagapattinam, Tamil Nadu, India.

Dr. S. JAYAPRAKASH
Research Advisor,
Department of Computer Science,
Edayathangudy. G.S. Pillay Arts and Science College (A),
Affiliated to Bharathidasan University,
Nagapattinam, Tamil Nadu, India.

Abstract

The transition from 5G to 6G networks promises revolutionary capabilities, including terahertz communication, holographic telepresence, and massive Internet of Everything (IoE) connectivity. However, this hyper-connected ecosystem faces an existential threat from the advent of cryptographically relevant quantum computers (CRQCs). Shor's algorithm renders current public-key standards (RSA, ECC) obsolete, exposing 6G networks to "Store Now, Decrypt Later" (SNDL) attacks. This paper surveys the state-of-the-art in Post-Quantum Cryptography (PQC) specifically tailored for 6G Authentication and Key Exchange (AKE) protocols. We analyze the integration of NIST-standardized lattice-based algorithms (CRYSTALS-Kyber, Dilithium) into the 6G service-based architecture, evaluate hybrid schemes for transitional security, and review lightweight protocols for resource-constrained 6G IoT devices. Comparative analysis reveals that while lattice-based Key Encapsulation Mechanisms (KEMs) offer acceptable latency for Ultra-Reliable Low-Latency Communication (URLLC), PQC digital signatures introduce significant bandwidth overheads, necessitating novel architectural optimizations in the 6G control plane.

Keywords: Post-Quantum Cryptography (PQC), 6G Security, Authentication and Key Agreement (AKA), Lattice-Based Cryptography, Quantum-Resilient Networks, URLLC (UltraReliable Low-Latency Communication).

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 01 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-578 PAGE NO: 021-027

1. Introduction

1.1 The 6G Vision and Security Landscape

Sixth-generation (6G) wireless networks are designed to transcend the limitations of 5G, targeting peak data rates of 1 Tbps, sub-millisecond latency, and connection densities of 10^7 devices/km² [1]. Unlike its predecessors, 6G integrates intelligence at the edge, relying heavily on AI-driven orchestration and Zero-Trust Architecture (ZTA). However, the trust models underpinning these innovations currently rely on classical cryptographic primitives—Elliptic Curve Diffie-Hellman (ECDH) for key agreement and ECDSA for authentication—which are mathematically vulnerable to quantum adversaries.

1.2 The Quantum Threat: Shor and Grover

The security of 6G is threatened by two primary quantum algorithms. Shor's Algorithm offers an exponential speedup in factoring large integers and computing discrete logarithms, effectively breaking RSA and ECC-based PKI systems used in the 6G Authentication and Key Agreement (AKA) protocols [2]. Grover's Algorithm provides a quadratic speedup for searching unstructured databases, effectively halving the security strength of symmetric ciphers like AES256, though this can be mitigated by doubling key sizes.

1.3 The "Store Now, Decrypt Later" (SNDL) Urgency

A critical concern for 6G is the SNDL attack vector. Adversaries can harvest encrypted 6G traffic today and store it until a sufficiently powerful quantum computer becomes available to decrypt it [3]. For 6G applications with long-term confidentiality requirements—such as telesurgery records, autonomous vehicle logs, and government communications—immediate integration of Post-Quantum Cryptography (PQC) is mandatory, well before the physical realization of large-scale quantum processors.

2. Preliminaries & Background

2.1 Evolution of AKA Protocols

Authentication and Key Agreement (AKA) protocols are the gatekeepers of mobile networks. 5G-AKA improved upon 4G by introducing the Subscription Concealed Identifier (SUCI) to prevent IMSI catching. However, 6G requires a shift from centralized authentication (SIMbased) to decentralized, heterogeneous trust models involving edge clouds and non-terrestrial networks (NTN) [4].

2.2 Taxonomy of Post-Quantum Cryptography

NIST has recently standardized several PQC families, categorized by their underlying mathematical problems:

- Lattice-based: Relies on the hardness of the Learning with Errors (LWE) problem. Examples include ML-KEM (Kyber) for key encapsulation and ML-DSA (Dilithium) for signatures. These

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 01 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-578 PAGE NO: 021-027

are currently the most promising for 6G due to balanced performance [5].

- Code-based: Relies on error-correcting codes (e.g., McEliece). Features very fast encryption but prohibitively large public keys for mobile payloads.

- Hash-based: (e.g., SPHINCS+). Stateless and stateful signatures. Extremely secure but slower and with larger signatures, limiting their use in low-latency 6G handshakes [6].

3. State-of-the-Art in Post-Quantum Key Exchange (KEM) for 6G

3.1 Lattice-Based KEMs in the 6G Control Plane

The primary candidate for replacing ECDH in 6G is ML-KEM (formerly CRYSTALS-Kyber). Recent benchmarks on 6G Open RAN (O-RAN) controllers demonstrate that Kyber-768 adds only negligible computational latency compared to ECDH. However, the ciphertext size (1088 bytes for Kyber-768 vs. 32 bytes for ECC) introduces transmission overhead [7]. For 6G URLLC (Ultra-Reliable Low-Latency Communication) slices, this additional payload must be fragmented carefully to avoid jitter.

3.2 Hybrid Key Exchange Schemes

Given the relative immaturity of PQC compared to ECC, 6G standards are moving toward Hybrid KEMs. In this model, the User Equipment (UE) and Base Station (gNB) perform both an ECDH and a Kyber key exchange, deriving the final session key from both secrets ($K = K_{classical} \oplus K_{quantum}$). This ensures that the session remains secure even if the PQC algorithm has a hidden flaw, while protecting against future quantum attacks [8].

3.3 Code-Based KEMs for Backhaul Security

While lattice schemes are preferred for the air interface (UE-to-gNB), code-based systems like Classic McEliece are being explored for the optical backhaul links connecting 6G base stations. The static nature of backhaul infrastructure tolerates the large public keys of McEliece in exchange for its extremely fast decapsulation speeds and conservative security proofs [9].

4. State-of-the-Art in Post-Quantum Authentication

4.1 The Signature Size Problem

Authentication poses a harder challenge than key exchange for 6G. ML-DSA (Dilithium) signatures are significantly larger (2.4 KB) than ECDSA signatures (64 bytes). In a 6G handshake involving mutual authentication, transmitting these large signatures can degrade the connection setup time, particularly in weak signal areas (cell edge) [10].

4.2 Falcon and SPHINCS+ in 6G

Falcon (now FN-DSA) offers smaller signatures than Dilithium and is faster, making it attractive for V2X (Vehicle-to-Everything) authentication where latency is critical. However, its implementation requires complex floating-point arithmetic, which is

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 01 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-578 PAGE NO: 021-027

challenging for low-cost IoT hardware [11]. SPHINCS+ (SL-DSA) serves as a conservative **SPHINCS+** (SL-DSA) serves as a conservative backup but is generally considered too slow for the real-time requirements of the 6G radio interface [12].

4.3 Lightweight Authentication for Massive IoT (mMTC)

For the billions of battery-constrained sensors in 6G (Massive Machine-Type Communications), standard PQC signatures are too energy-intensive. Recent research focuses on:

- Hash-Based Mutual Authentication: Protocols using lightweight hash chains and Physically Unclonable Functions (PUFs) to avoid heavy asymmetric cryptography entirely [13].
- Zero-Knowledge Proofs (ZKPs): Post-quantum ZKP schemes are being adapted for privacy-preserving authentication in 6G, allowing a device to prove its identity without revealing its ID, thus enhancing privacy [14].

5. Comparative Performance Analysis

The following analysis synthesizes performance data from recent 6G-PQC testbeds [15] [16].

Protocol Family	Algorithm	Key (Pub/Priv)	Signature/ Ciphertext	6G Suitability
Classical	ECDH ECDSA	~32 Bytes	~64 Bytes	Obsolete Quantum Safe)
Lattice (KEM)	ML-KEM-768 (Kyber)	1184 / 2400 Bytes	1088 Bytes	High (Standard for 6G Key Ex)
Lattice (Auth)	ML-DSA (Dilithium)	1312 / 2528 Bytes	2420 Bytes	Medium (High Bandwidth Cost)
Lattice (Auth)	Falcon-512	897 / 1281 Bytes	666 Bytes	High Latency, Hard to implement)
Hashbased	SPHINCS+	~32 Bytes	~8000 Bytes	Low (Signature too large for Air Interface)

Analysis:

1. **Latency:** Kyber adds <10% overhead to handshake duration, meeting URLLC requirements.
2. **Bandwidth:** Dilithium increases the authentication payload by ~40x compared to ECDSA. This requires 6G control channels to support larger "jumbo frames" to avoid fragmentation delays [17].
3. **Energy:** Hash-based PQC consumes significantly more battery power than lattice-based approaches, making lattice the only viable option for mobile devices [18].

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 01 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-578 PAGE NO: 021-027

6. Challenges and Open Issues

6.1 The "Jumbo Frame" and Fragmentation Issue

Current cellular standards (3GPP) often optimize for small control packets. The introduction of multi-kilobyte PQC certificates and signatures necessitates a redesign of the Packet Data Convergence Protocol (PDCP) layer to handle fragmentation efficiently without causing packet loss or DoS vulnerabilities [19].

6.2 Hardware Acceleration and Co-Design

Software implementations of PQC are insufficient for the Tbps throughput of 6G. There is an urgent need for specialized hardware accelerators (ASICs/FPGAs) in 6G modems to perform lattice operations (NTT multiplication) at line rate [20].

6.3 Certificate Management

Replacing the global Public Key Infrastructure (PKI) with quantum-safe certificates is a logistical nightmare. The sheer size of PQC certificates creates storage bottlenecks for IoT devices and increases the time required for certificate chain verification.

7. Conclusion:

The migration to a quantum-resilient 6G architecture is not merely a cryptographic swap but a systemic overhaul. While Lattice-based cryptography (ML-KEM and ML-DSA) has emerged as the de facto standard for the 6G control plane, significant challenges remain regarding bandwidth efficiency and hardware optimization. Immediate deployment of hybrid modes is the most prudent path forward, securing current data against SNDL attacks while ensuring reliability. Future research must prioritize lightweight PQC adaptations for the massive IoT sector and hardware-software co-design to mask the latency overhead of these complex protocols.

References

1. M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G Networks: Use Cases and Technologies," IEEE Communications Magazine, vol. 58, no. 3, pp. 55-61, 2020.
2. P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994.
3. E. P. IQC, "Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges," European Telecommunications Standards Institute (ETSI) White Paper, no. 8, June 2015.
4. S. Siriwardhana, et al., "The 6G Security Landscape: Architectures, Threats, and Solutions," IEEE Access, vol. 12, pp. 10234-10255, 2024.
5. NIST, "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard," National Institute of Standards and Technology, August 2024.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 01 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-578 PAGE NO: 021-027

6. D. J. Bernstein, et al., "SPHINCS+: Stateless Hash-Based Signatures," NIST PQC Standardization Round 3 Submission, 2022.
7. A. A. Yavuz and T. G. Aslan, "Performance Analysis of CRYSTALS-Kyber in 6G Open RAN Architectures," IEEE Transactions on Wireless Communications, vol. 23, no. 4, pp. 2450-2462, 2024.
8. J. Zhang, "Hybrid Post-Quantum Key Encapsulation for 5G/6G Handover Security," Journal of Network and Computer Applications, vol. 210, 2023.
9. R. Misoczki, et al., "MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes," IEEE International Symposium on Information Theory, 2023.
10. L. Chen, et al., "Impact of Post-Quantum Cryptography on 6G Latency: A Comprehensive Survey," IEEE Communications Surveys & Tutorials, vol. 26, no. 1, 2024.
11. T. Prest, et al., "Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU," NIST PQC Standardization Round 3 Submission, 2022.
12. S. K. Singh, et al., "Evaluating Hash-Based Signatures for 6G V2X Communications," Vehicular Communications, vol. 39, 2024.