Q-RAN: Quantum-Resilient O-RAN Architecture

Vipin Rathi[1], Lakshya Chopra[2], Madhav Agarwal[2], Nitin Rajput[2], Kriish Sharma [2], Sushant Mundepi[2], Shivam Gangwar[2], Rudraksh Rawal[2], and Jishan[2]

[1]Ramanujan College, University of Delhi, New Delhi, India
[2]coRAN Labs Private Limited, New Delhi, India

Abstract

The telecommunications industry faces a dual transformation: the architectural shift toward Open Radio Access Networks (O-RAN) and the emerging threat from quantum computing. O-RAN's disaggregated, multi-vendor architecture creates a larger attack surface vulnerable to cryptanalytically relevant quantum computers (CRQCs) that will break current public-key cryptography. The Harvest Now, Decrypt Later (HNDL) attack strategy makes this threat immediate, as adversaries can intercept encrypted data today for future decryption. This paper presents Q-RAN, a comprehensive quantum-resistant security framework for O-RAN networks using NIST-standardized Post-Quantum Cryptography (PQC). We detail the implementation of ML-KEM (FIPS 203) and ML-DSA (FIPS 204), integrated with Quantum Random Number Generators (QRNG) for cryptographic entropy. The solution deploys PQ-IPsec, PQ-DTLS, and PQ-mTLS protocols across all O-RAN interfaces, anchored by a centralized Post-Quantum Certificate Authority (PQ-CA) within the SMO framework. This work provides a complete roadmap for securing disaggregated O-RAN ecosystems against quantum adversaries.

Keywords—Post-Quantum Cryptography (PQC), 5G RAN (5G-RAN), O-RAN Alliance, Quantum-Safe Networks (QSN), Quantum-Resilient 5G RAN, Hybrid PQC (HPQC), Quantum-Safe Authentication, Post-Quantum Migration, Post-Quantum TLS (PQ-TLS), Post-Quantum IPsec (PQ-IPsec), Hardware-Accelerated PQC, Post-Quantum PKI Infrastructure, Quantum-Safe Telecom, Post-Quantum Security for B5G/6G, QORE, xFAPI

1 Introduction

The global telecommunications industry is undergoing a major shift. Open Radio Access Networks (O-RAN) mark a significant departure from traditional, single-vendor base station designs. By breaking these systems into modular parts connected through open, standardized interfaces, O-RAN introduces greater flexibility and innovation. Driven by the O-RAN ALLIANCE, this approach separates the gNodeB into three key components — the Radio Unit (RU), Distributed Unit (DU), and Centralized Unit (CU) — and supports multi-vendor deployments. It also enables advanced network automation through the RAN Intelligent Controller (RIC).

As the industry advances toward an open RAN architecture, it faces a growing threat: quantum computing. Cryptographically Relevant Quantum Computers (CRQCs) have the potential to break widely used public-key cryptosystems such as RSA and Elliptic Curve Cryptography (ECC) [1]. Notably, Shor's algorithm [2] can efficiently factor large integers and compute discrete logarithms, making it capable of defeating these asymmetric cryptography schemes. This poses a serious risk to authentication, key exchange, and digital signatures across the entire network infrastructure.

This threat is immediate due to the Harvest Now, Decrypt Later strategy, where adversaries capture encrypted data today for decryption once quantum computers become available. For telecommunications networks with sensitive data and operational lifecycles spanning decades, this creates urgent vulnerability. O-RAN's open, disaggregated architecture inherently expands the attack surface, making quantum-resistant security not optional but essential.

The solution lies in Post-Quantum Cryptography (PQC), a family of algorithms designed to resist both classical and quantum attacks. In August 2024, the U.S. National Institute of Standards and Technology (NIST) finalized the first PQC standards [3], providing a clear path forward. This paper presents Q-RAN, a comprehensive framework for migrating O-RAN networks to quantum-resistant security, addressing every interface and component with standardized PQC algorithms and crypto-agile implementation strategies.

1.1 Contributions

This paper makes the following contributions:

- A comprehensive analysis of quantum threats to O-RAN architecture and identification of vulnerable interfaces and protocols
- Detailed implementation specifications for PQ-IPsec, PQ-DTLS, and PQ-mTLS using NIST-standardized algorithms (ML-KEM-768, ML-DSA-65)

- Integration of Quantum Random Number Generators (QRNGs) to ensure cryptographic operations use truly random, non-deterministic entropy sources.
- A Post-Quantum Certificate Authority (PQ-CA) placed within the SMO framework, serving as the central trust point for all RAN components.
- Practical deployment using open-source tools like strongSwan and OpenSSL (with the OQS provider), along with configuration examples drawn from real O-RAN stacks.
- Complete roadmap outlining how classical security can realistically evolve into a quantum-safe O-RAN setup, with the main hurdles and open problems clearly stated.

1.2 Paper Organization

This paper starts by introducing the key elements of the O-RAN architecture, including its modular structure and built-in security mechanisms. It also offers a brief overview of post-quantum cryptography (PQC) to set the stage for the challenges ahead. From there, we explain why current O-RAN systems need to be adapted to resist quantum-era threats and walk through the steps involved in upgrading the existing 5G security framework. This includes proposed protocols, implementation enhancements, and a look at the practical hurdles of moving to PQC. We then present Q-RAN, our end-to-end tested solution that puts these ideas into practice. Finally, we share the main insights from our work and outline possible directions for future development.

2 Background

This section takes a closer look at the O-RAN architecture, focusing on its modular design and security features that are already in place. We then introduce the basics of post-quantum cryptography and talk about how current security protocols need to evolve to stay protected against future quantum threats.

2.1 O-RAN Architecture

Open RAN disaggregates traditional base station functions into interoperable components [4]. While this encourages innovation, it also often leads to a larger attack surface. Because of its open design, Open RAN needs stronger, quantum-resistant security mechanisms.

2.1.1 Logical Components

O-RAN Centralized Unit (O-CU): This unit handles higher-layer protocol functions and is split into the Control Plane (O-CU-CP) and User Plane (O-CU-UP). The O-CU-CP manages RRC (Radio Resource Control) signaling and mobility management, while the O-CU-UP processes user data through the PDCP (Packet Data Convergence Protocol) layer, including encryption.
O-RAN Distributed Unit (O-DU): The DU is responsible for handling real-time layers—RLC, MAC, and High-PHY layers, handling tasks such as error correction, retransmission, scheduling, and modulation mapping. It interfaces with the RU over the Open Fronthaul (O-FH) and communicates with the CU using the F1 Application Protocol (F1AP).
O-RAN Radio Unit (O-RU): The RU is responsible for Low-PHY processing and the transmission and reception of radio signals over the air interface. It handles tasks such as signal modulation and demodulation, analog-to-digital conversion, as well as MIMO processing and beamforming. All these operations must be performed within tight timing and computational constraints..

2.1.2 Service Management and Orchestration (SMO)

The SMO orchestrates the RAN's disaggregated components through a variety of management interfaces, delivering FCAPS capabilities via the O1 interface and handling orchestration tasks through O2. It also hosts the Non-RT RIC, where rApps enhanced with AI/ML are responsible for policy enforcement and optimizations. As a result of its central function, the SMO is well suited to function as both a Post-Quantum Certificate Authority (PQ-CA) and a Post-Quantum Authorization Server, serving as a unified trust anchor for the network—a quantum-secure counterpart to a traditional root of trust or Post-Quantum PKI (PQ-PKI).

2.1.3 RAN Intelligent Controllers

Near-RT RIC: Controls O-CU/O-DU behavior on 10ms–1s timescales through xApps executing AI-guided radio resource management.
Non-RT RIC: Operates above 1s timescales, hosting rApps for long-term optimization and model training. It interfaces with the Near-RT RIC through the A1 interface for policy delivery.

2.2 O-RAN Interfaces and Security Requirements

O-RAN defines multiple interfaces with differing latency and security demands:
A1: Connects Non-RT and Near-RT RICs using mTLS for authenticated policy exchange.
E2: Links Near-RT RIC with O-CU/O-DU, secured via IPsec; compromise could enable resource manipulation.
F1: Connects O-CU and O-DU—F1-C (control) and F1-U (user)—protected by IPsec/DTLS.
O1: Management interface between SMO and O-RAN nodes, secured via mTLS.
O2: Connects SMO to O-Cloud for lifecycle management, using mTLS.
Open Fronthaul: High-throughput O-RU $\leftrightarrow$ O-DU interface; employs mTLS on the M-Plane and IEEE

802.1X authentication, but faces performance constraints for PQC adoption.

2.3 Classical Security Mechanisms in O-RAN

Current O-RAN security [5] relies on classical cryptographic primitives, such as RSA, DH and ECC, which are soon to be broken by quantum computers.

Public Key Infrastructure (PKI): PKI is a system concerned with establishing trust in cryptographic communications over insecure public networks. It typically achieves this with the use of digital X.509 Certificates [6], which are used to confirm an entity's true identity. The certificates comprise digital signatures, created using classical cryptosystems like RSA / ECC, making them vulnerable to quantum attacks that are capable of forging certificates and breaking authenticity.

IPsec: Internet Protocol Security is a suite of open standards for achieving confidentiality, integrity, and authenticity over insecure IP connections via the use of cryptographic techniques and PKI [7]. The protocol employs a set of asymmetric and symmetric primitives (e.g., AES) to guarantee security. Symmetric AES remains secure with 256-bit keys, but IKEv2 key exchange (e.g., Diffie-Hellman) is quantum-vulnerable. IPsec is the backbone of O-RAN security, being frequently deployed in various interfaces (N2, N3, E2, Xn).

DTLS: Datagram Transport Layer Security is a higher layer protocol designed to protect datagram oriented transport protocols (e.g., UDP, SCTP) (RFC 9147) [8] using cryptographic techniques. Vulnerable in key exchange and authentication phases.

mTLS: Mutual TLS extends the TLS protocol for guaranteeing mutual authentication between client and server. mTLS is mandated for A1, O1, O2, and M-Plane; both certificate and key exchange stages are quantum-breakable.

OAuth 2.0: An authorization framework designed to provide delegated access to protected resources (RFC 6749) [9]. Bound to mTLS certificates (RFC 8705) [10], but vulnerable if certificates can be forged via quantum attacks.

2.4 Post-Quantum Cryptography Fundamentals

Post-Quantum Cryptography (PQC) employs algorithms secure against both classical and quantum attacks. NIST-standardized lattice-based schemes—ML-KEM and ML-DSA—are key to future-proofing O-RAN security.

2.4.1 ML-KEM (FIPS 203)

ML-KEM [11] is an IND-CCA2-secure Key Encapsulation Mechanism (KEM) derived from the CRYSTALS-Kyber [12]. It enables secure shared key establishment through the standard **KeyGen, Encaps, and Decaps** operations. It is built upon the **Module Learning with Errors (MLWE)** problem, a widely studied hardness assumption in lattice-based cryptography that is believed to be resistant to attacks from both classical and quantum adversaries.

ML-KEM guarantees cryptographic security by leveraging the difficulty of distinguishing structured noisy linear equations from uniform randomness—**Decision LWE (D-LWE)**. The scheme samples error and noise terms from a centered binomial distribution, which offers both efficiency and compactness while preserving the required level of entropy for post-quantum security.

Parameter sets: ML-KEM-512 (AES-128 equivalent), 768 (AES-192), 1024 (AES-256), summarized in Table 1. *ML-KEM-768* balances efficiency and security for telecom deployments.

Set	Pub (B)	Sec (B)	Ct (B)	SS (B)
ML-KEM-512	800	1,632	768	32
ML-KEM-768	1,184	2,400	1,088	32
ML-KEM-1024	1,568	3,168	1,568	32

Table 1: ML-KEM parameter set sizes (bytes)

2.4.2 ML-DSA (FIPS 204)

Based on the CRYSTALS-Dilithium [13] signature scheme, ML-DSA [14] is a post-quantum digital signature algorithm designed to replace classical schemes like RSA and ECDSA. Being a signature scheme, it supports the standard **KeyGen, Sign, and Verify** operations, and is defined across three parameter sets—ML-DSA-44, ML-DSA-65, and ML-DSA-87—with *ML-DSA-65* offering approximately 192-bit classical security, making it well-suited for applications such as O-RAN environments. **HashML-DSA** is another standardized version of the algorithm.

ML-DSA is built upon two core hardness assumptions: the Module Learning With Errors (MLWE) problem and the Module Short Integer Solution (MSIS) problem, both of which are believed to be resistant to attacks even by quantum computers. Specifically, MLWE generalizes the standard Learning With Errors (LWE) problem, where the goal is to distinguish between valid LWE samples and uniformly random noise (D-LWE). ML-DSA parameter sets are shown in Table 2.

Set	Pub (B)	Sec (B)	Sig (B)
ML-DSA-44	1,312	2,560	2,420
ML-DSA-65	1,592	4,032	3,309
ML-DSA-87	2,592	4,896	4,627

Table 2: ML-DSA parameter set sizes (bytes)

The type and security of Post-Quantum Schemes are summarized in Table 3.

2.4.3 Quantum Random Number Generators (QRNGs)

Quantum Random Number Generators (QRNGs) extract entropy from inherently probabilistic quantum

Scheme	Type	Security Goal	Security Level (NIST)
ML-KEM	KEM (Lattice)	IND-CCA	Level 1–5
ML-DSA (Dilithium)	Signature (Lattice)	SUF-CMA	Level 1–5
SLH-DSA	Signature (Hash-based)	EUF-CMA	Level 1–5
NTRU	KEM (Lattice)	IND-CCA	Level 1–5
X-Wing	KEM (Structured Lattice)	IND-CCA	Level 1–5
Composite-Signatures	Hybrid	SUF-CMA/EUF-CMA (composite)	Variable

Table 3: Security Properties of Selected PQ Schemes

processes—such as photon arrival times, quantum vacuum fluctuations, or single-photon path superposition—to generate truly random bitstreams. Unlike pseudo-random number generators (PRNGs), which are algorithmically deterministic and thus potentially vulnerable to state compromise, QRNGs offer information-theoretic security.

This makes them particularly well-suited for post-quantum cryptography (PQC), where classical entropy sources may not provide sufficient resistance against quantum-enabled adversaries. High-entropy QRNG outputs are used to seed key generation, key encapsulation/encryption, and signature randomization algorithms, ensuring robust entropy pools and resistance against side-channel entropy prediction.

In order to achieve FIPS 140-3 [15] compliance, a QRNG chip must be integrated using a FIPS specified RNG method and follow the rigorous and strict criteria for entropy and random number generation outlined in the FIPS standard. The integration shall also comply with NIST SP 800-90A [16]—requirements for random number generation. An example QRNG method combining entropy from two sources, for use in ML-KEM, is illustrated in the Figure 1.

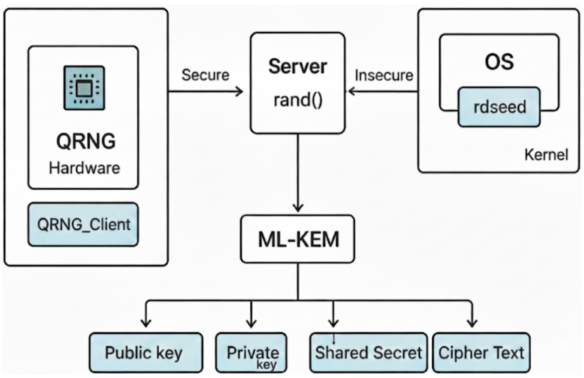

Figure 1: QRNG-based key generation feeding ML-KEM with true quantum entropy.

2.4.4 Quantum-Resistant Symmetric Cryptography

AES-256 remains secure against Grover's [17] algorithm with an effective 128-bit post-quantum strength [18]. SHA-3 [19] retains its collision and pre-image resistance properties, making it suitable for post-quantum cryptography (PQC) use cases such as hashing, digital signatures, and authentication.

SHA-3 is built using a sponge construction that incorporates the Keccak-f[1600] permutation as its core, along with additional steps such as domain separation and output truncation. In addition to the fixed-output hash functions, SHA-3 includes two extendable output functions (XOFs)—SHAKE128 and SHAKE256—which are now used in NIST FIPS 203 and 204 for internal hashing.

The algorithm is also well-suited for hardware acceleration, leveraging instruction sets such as AVX2 on x86 and NEON on ARM-based platforms.

2.4.5 Post-Quantum TLS/DTLS

PQ-TLS and PQ-DTLS integrate post-quantum and classical algorithms through hybrid handshakes, ensuring crypto-agility and backward compatibility while providing quantum resistance. These protocols allow for a secure migration path without compromising performance. The integration is illustrated in Figure 2.

2.4.6 Post-Quantum IPsec

PQ-IPsec is an extension to the classical IKEv2, which integrates Post-Quantum Hybrid KEMs, such as ECDHE+ML-KEM-768 for shared key establishment, simultaneously mixing Post-Quantum Pre-Shared Keys (PPKs, RFC 8784). Thus, it provides a mitigation to the Harvest-Now-Decrypt-Later risks and enhances the security of IPsec tunnel establishment.

2.4.7 Post-Quantum Certificate Authority (PQ-CA)

A PQ-CA issues and validates certificates using PQ signatures, such as ML-DSA / SLH-DSA, replacing RSA/ECC-based roots of trust. PQ-CAs provide long-term authenticity for devices, applications, and xApps/rApps within hierarchical O-RAN trust domains.

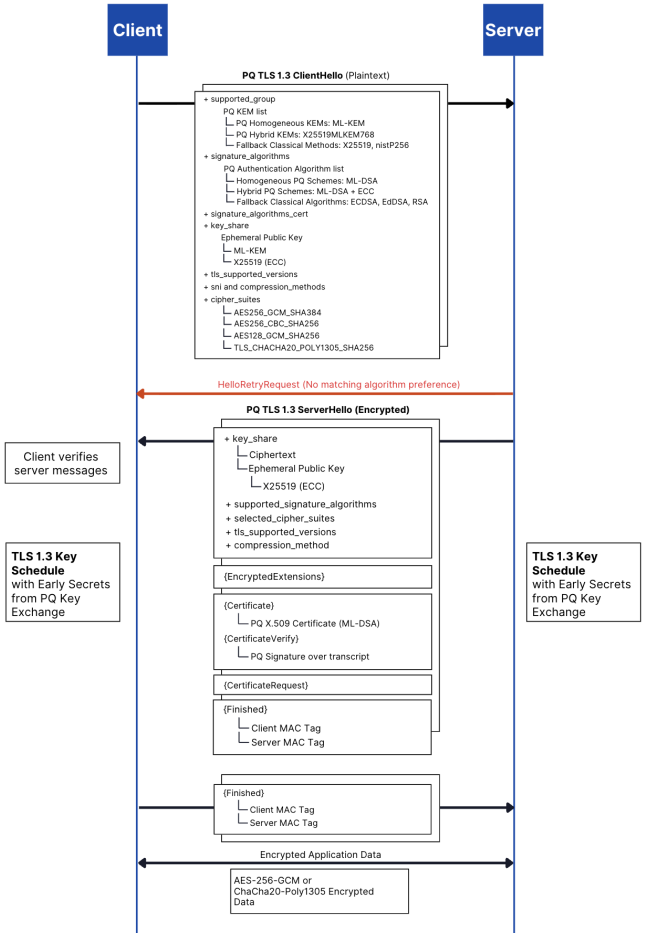

Figure 2: Post-Quantum TLS handshake flow with PQ KEM and authentication.

3 Migration to Quantum-Secure O-RAN

This section presents a comprehensive strategy for migrating O-RAN networks from classical to quantum-resistant security. The migration aims to address every interface, protocol, and component in the O-RAN architecture, ensuring a consistent and practical strategy feasible for network operators.

3.1 Migration Overview

A concise summary of O-RAN interfaces, their current classical security mechanisms, and required quantum-secure replacements is provided in Table 4. This systematic approach guarantees that no interface remains vulnerable to quantum attacks.

Prior research, such as [20], has addressed post-quantum security enhancements for specific protocols like IPsec and MACsec in RAN contexts. This work, however, presents a complete and practical migration strategy, covering all O-RAN interfaces and components to enable a seamless transition from classical to quantum-resistant security across the entire architecture.

3.2 Foundational Entropy: QRNG Integration

Strong cryptographic security is not just limited to the underlying hard problems but a variety of other supporting factors, with a quality, unpredictable, and safe randomness source being an equally important criterion. QRNGs, being an excellent source of true randomness, fulfill this requirement, and with their integration into cryptographic algorithms, we ensure the operations of keygen, encapsulation, and (optionally)signing are truly random.

3.2.1 QRNG Deployment Architecture

The QRNG infrastructure consists of hardware QRNGs strategically placed within the network architecture. A primary QRNG is provisioned within the SMO, which provides high-entropy randomness for the PQ-CA's root key generation and other certificate issuance/signing operations. The QRNGs utilized have undergone rigorous NIST's Entropy Validation Programs.

Network functions incorporate QRNGs in their local entropy pools, accessing them via FIPS 140-2/3 validated cryptographic modules, for use in TLS connections, long-lived IPsec sessions, and other cryptographic operations. The QRNG chips are typically connected via PCIe, and the random bitstream is processed inside secure memory enclaves—such as those provided by Intel SGX, or AMD SEV.

3.2.2 QRNG Applications in O-RAN

Securing Open Interfaces: O-RAN's disaggregated architecture exposes multiple open interfaces—Open Fronthaul, F1, E2, A1, O1, and Xn—that need robust protection. QRNGs generate keys for post-quantum protocols

Table 4: Classical O-RAN to Post-Quantum O-RAN Migration

Phase / Interface	Between Nodes	Existing Security	Quantum-Secure Mechanisms
MidHaul - F1AP	O-CU & O-DU; O-CU-CP & O-DU (F1-C); O-CU-UP & O-DU (F1-U)	IPsec or DTLS	PQ-IPsec or PQ-DTLS
E1AP	O-CU-CP & O-CU-UP	IPsec or DTLS	PQ-IPsec or PQ-DTLS
BackHaul - NGAP	O-CU & AMF; O-CU-CP & 5G Core	IPsec or DTLS	PQ-IPsec or PQ-DTLS
E2	Near-RT RIC & O-CU; Near-RT RIC & O-DU	IPsec or DTLS	PQ-IPsec or PQ-DTLS
Xn	Source gNB & Target gNB	IPsec or DTLS	PQ-IPsec or PQ-DTLS
BackHaul N3	O-CU & UPF; O-CU-UP & UPF	IPsec	PQ-IPsec
O-FH (M-Plane)	O-RU & O-DU/SMO	mTLS, SSHv2	PQ-mTLS or PQ-SSH
A1	Near-RT RIC & Non-RT RIC	mTLS	PQ-mTLS
O1	SMO & O-RAN Managed Elements	mTLS	PQ-mTLS
O2	SMO & O-Cloud	mTLS	PQ-mTLS
Y1	Near-RT RIC to authorized consumers	mTLS	PQ-mTLS
R1	rApps & Non-RT RIC framework	mTLS	PQ-mTLS

such as PQ-IPsec, PQ-mTLS, and PQ-DTLS, ensuring confidentiality, integrity, and authentication for all data passing through these interfaces.

RIC Security: The RIC is central to controlling and optimizing the RAN, making its security critical. QRNGs provide cryptographic keys for securing the RIC platform, its communications, and AI/ML-driven applications (xApps and rApps). This includes securing communications over the A1 interface (Non-RT RIC to Near-RT RIC) and the E2 interface (Near-RT RIC to RAN nodes).

Certificate Generation and PKI: O-RAN's Zero Trust Architecture [21] relies on certificate-based mutual authentication. QRNGs provide unpredictable randomness for generating private keys for post-quantum X.509 certificates, establishing a root of trust for all network functions (O-RU, O-DU, O-CU, RICs).

Secure Application Lifecycle: xApp and rApp integrity is critical. QRNGs generate keys for digital signatures that sign and verify software packages during application onboarding and lifecycle management, preventing deployment of malicious or compromised code.

Data at Rest Protection: RICs and management components store sensitive data including network policies, performance metrics, and configuration data. QRNGs generate symmetric encryption keys for encrypting this data at rest, protecting it from unauthorized access even if components are compromised. The keys are stored in a Hardware Security Module (HSM) provisioned at the RIC.

3.3 Control Plane Security: AES-128 to AES-256 Upgrade

The Radio Resource Control (RRC) layer handles the crucial control-plane signaling between the User Equipment (UE) and the gNB. Since it carries sensitive control messages (e.g., UE Identifiers and capabilities), it needs to be well protected against eavesdropping and tampering. To do this, RRC currently uses 128-bit algorithms like NIA and NEA (for example, AES-128 and SNOW-3G). If these protections are broken, attackers could interfere with control data, disrupt handovers, or even launch Denial-of-Service (DoS) attacks. However, with the rise of quantum threats, the 128-bit security level is no longer enough. Moving to stronger algorithms like AES-256 is necessary, but this shift will require coordinated updates across the NAS (Non-Access Stratum), the UE itself, and the 5G Core network.

The mathematical justification for the mentioned update lies in defense against Grover's algorithm, which pro-

vides square-root speedup over classical exhaustive key-search attacks. For a symmetric cipher with a k-bit key, classical key-search requires approximately 2^k operations, while Grover's algorithm reduces this to approximately $2^{k/2}$ quantum queries.

For AES-128, quantum attack effective security drops from 128 bits to 64 bits (2^{128} classical operations becomes 2^{64} quantum queries). A 64-bit security level is vulnerable to sufficiently powerful quantum computers. For AES-256, effective security under Grover's algorithm drops from 256 bits to 128 bits (2^{256} classical operations becomes 2^{128} quantum queries) [18]. A 128-bit security level remains computationally infeasible even for quantum computers, providing durable, long-term security.

The move to AES-256 applies not only to RRC traffic but to all symmetric encryption operations across the O-RAN architecture, with extensions to 5G core and UE in the future.

3.4 User and Control Plane Interfaces: PQ-IPsec and PQ-DTLS

The security (confidentiality and authentication) of interfaces like F1AP, E1AP, Xn, N2, N3, and E2 is typically provided by IPsec or DTLS, both of which are still susceptible to quantum attacks. Upgrading these protocols to PQ-IPsec and PQ-DTLS, which incorporate post-quantum cryptographic algorithms and QRNG-generated entropy, is necessary to achieve quantum-resistant security.
Figure 3 illustrates the deployment of PQ-IPsec and PQ-DTLS across O-RAN interfaces.

3.4.1 PQ-IPsec Implementation Strategy

The PQ-IPsec implementation modifies the Internet Key Exchange version 2 (IKEv2) protocol to support PQC for key establishment through a hybrid approach combining classical key exchange (ECDH) with PQ Key Encapsulation Mechanism (ML-KEM).

Hybrid Key Exchange: The IKE_SA_INIT exchange establishes a secure channel using classical algorithms (e.g., ECDH with Curve 25519). Subsequently, ML-KEM-768 key exchange occurs within an encrypted IKE_INTERMEDIATE message. This two-step process accommodates large PQC key sizes that cannot be fragmented in initial handshakes. The encrypted nature of IKE_INTERMEDIATE provides traffic flow confidentiality.

Post-Quantum Pre-shared Keys: RFC 8784 defines Post-Quantum Pre-shared Keys (PPKs) providing an additional quantum resistance layer. High-entropy, quantum-generated pre-shared keys (256 bits classical security) are provisioned out-of-band to communicating peers. These PPKs are mixed into key derivation functions (KDFs) which ensures that even if adversaries record entire IKEv2 exchanges and later break asymmetric cryptography with quantum computers, they cannot derive final session keys without PPKs, rendering harvested data useless.

QRNG for PPK Generation: PPK security depends entirely on unpredictability. QRNGs generate PPKs ensuring highest possible entropy, making them truly random secrets immune to prediction.

Table 5 provides the specifications for Post-Quantum TLS and IPsec.

3.4.2 PQ-DTLS Implementation Strategy

For interfaces using DTLS over SCTP [22] (F1AP, N2, E1AP), migration to quantum-safe posture involves upgrading to PQ-DTLS 1.3 with multiple quantum-safe enhancements. Figure 4 shows the PQ-DTLS 1.3 protocol over the F1AP interface (DU-CU).

Upgraded Cipher Suites: Handshakes are fortified by replacing classical key exchange with ML-KEM. For symmetric encryption, cipher suites upgrade to AES-256, providing 128-bit security against Grover's algorithm attacks.

PQ Signature Schemes: Authentication becomes quantum-safe by replacing traditional signatures (RSA, ECDSA) with PQC signature schemes. This involves issuing and validating PQ X.509 certificates signed with ML-DSA.

QRNG for Keys and Nonces: PQC scheme security critically depends on true randomness. QRNGs provide high-entropy seeds for generating ML-KEM secret keys and unpredictable nonces for ML-DSA signature operations, preventing attacks exploiting predictable or repeated random values.

Figure 5 illustrates the PQ-DTLS 1.3 handshake sequence between O-DU and O-CU. It demonstrates the exchange of PQ X.509 certificates (ML-DSA-65), mutual verification of signatures, and encrypted session establishment using ML-KEM, achieving end-to-end post-quantum secure communication over the F1 interface.

3.5 Management Interfaces: PQ-mTLS Deployment

Management and control interfaces (A1, O1, O2, Y1, R1) facilitate communication between essential components including the SMO, RICs, and O-Cloud. Traditionally secured using mTLS, these interfaces must be upgraded to Post-Quantum mTLS (PQ-mTLS) which integrates quantum-resistant algorithms (e.g., ML-KEM and ML-DSA) into TLS 1.3 handshakes and certificate infrastructure. Figure 6 illustrates PQ-mTLS deployment across management interfaces.

3.5.1 PQ-mTLS Implementation

Securing API-driven management interfaces involves upgrading to PQ-mTLS, applying PQC algorithms to TLS 1.3 handshakes with focus on mutual authentication and backward compatibility.

Hybrid Key Exchange: Implementation adopts hybrid cipher suites. During TLS 1.3 handshakes, classical key exchange (ECDHE) and PQC KEM (ML-KEM) run in parallel. Final shared secrets derive from both computations, ensuring connection security as long as at least one algorithm remains unbroken.

Mutual Authentication with PQ Certificates: Quantum-resistant mutual authentication requires both entities to exchange and validate PQ Certificates signed with ML-DSA. This ensures, for example, that Non-RT RIC and Near-RT RIC can cryptographically verify each other's identity before establishing connections.

QRNG-Hardened Key Generation: QRNGs provide truly random seeds for all sensitive cryptographic material, including ephemeral keys for each ML-KEM exchange and long-term private keys for PQ certificates.

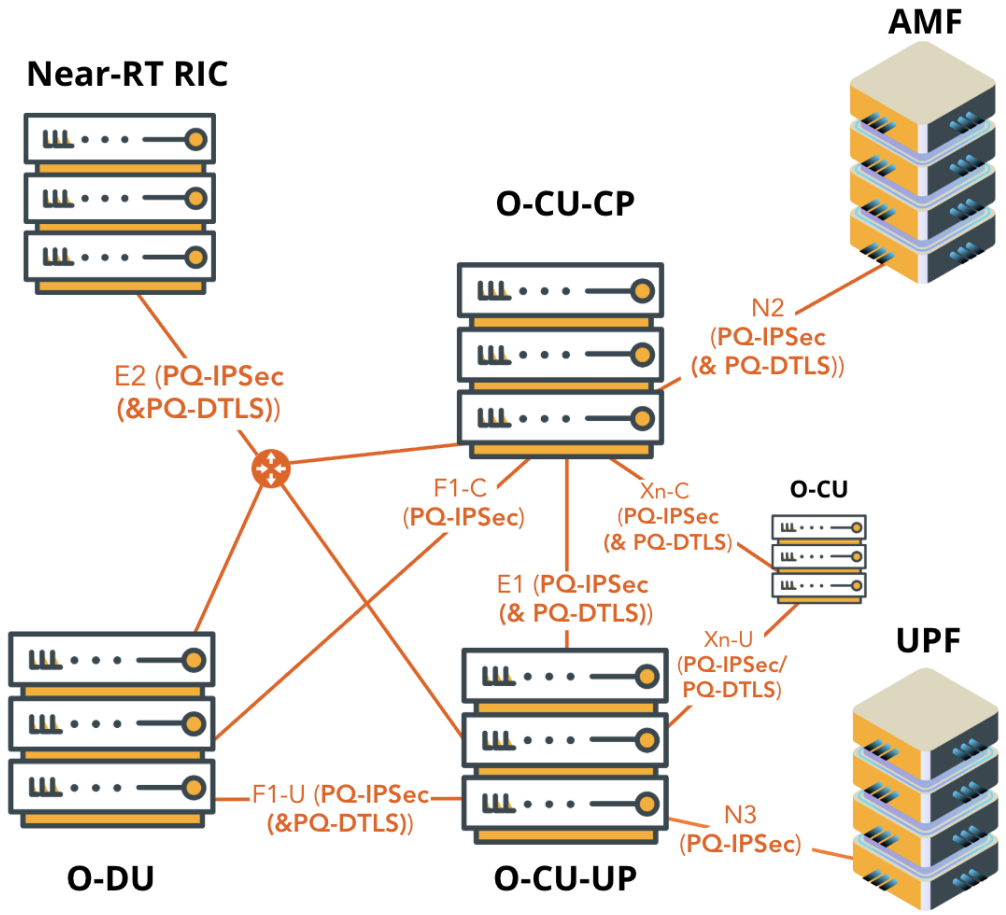

Figure 3: O-RAN Architecture with Security Protocols showing PQ-IPsec(& PQ-DTLS) on various interfaces (F1-C, F1-U, E1, Xn-C, Xn-U, N2, N3, E2) connecting Near-RT RIC, O-CU-CP, O-CU-UP, O-DU, AMF, and UPF.

Protocol	PQ TLS /IPsec Specification
PQ TLS 1.3	Hybrid KEM (X25519 + ML-KEM) for key exchange
PQ IPsec	PQ SA negotiation using composite KEM proposals
Cipher Suites	AES-GCM / ChaCha20-Poly1305 + SHA-384
Cert Format	X.509 with PQ SubjectPublicKeyInfo extensions
Handshake	Post-Quantum + Classical hybrid authentication

Table 5: Post-Quantum TLS and IPsec Specification Overview

3.6 Centralized Trust: PQ-CA and PQ-OAuth in SMO

The SMO's central management and automation role makes it the logical anchor for establishing network-wide root of trust. Upgrading the SMO to host a Post-Quantum Certificate Authority (PQ-CA) establishes the cornerstone of Post-Quantum PKI, issuing and managing cryptographic identities for all components and applications—a foundational requirement for O-RAN's Zero Trust Architecture [21]. The CA specifications are summarized in the Table 6.

3.6.1 Post-Quantum Certificate Lifecycle Management

The Post-Quantum Certificate Authority (PQ-CA), deployed within the SMO, manages the full lifecycle of quantum-resistant digital certificates for O-RAN components, covering generation, issuance, distribution, renewal, and revocation.

Certificate Generation and Hierarchy: The PQ-CA issues quantum-resistant X.509 certificates for all critical O-RAN entities including Non-RT RIC, Near-RT RIC, rApps, and xApps. The PKI structure follows a standard hierarchy with a PQ Root Certificate at the top, one or more PQ Intermediate CAs, and PQ Leaf Certificates for individual devices and applications. Certificates are signed using quantum-secure signature schemes such as ML-DSA, ensuring signatures remain secure against quantum adversaries.

Key Material Security via QRNG: To guarantee cryptographic strength, the PQ-CA generates private keys using a Quantum Random Number Generator (QRNG). This source of true quantum entropy strengthens the unpredictability of keys, essential for resisting brute-force attacks both now and post-quantum era.

Certificate Renewal and Revocation:

Renewal: Certificates are issued with short validity periods (7 to 90 days) to limit exposure in case of key compromise. The PQ-CA supports automated renewal workflows

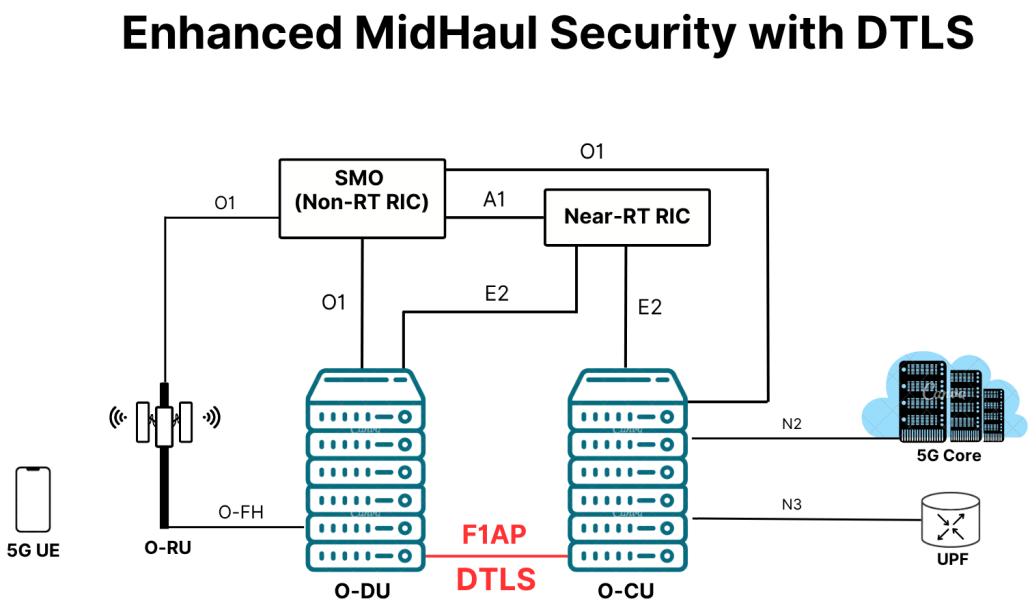

Figure 4: PQ-DTLS 1.3 Protocol at F1AP Interface

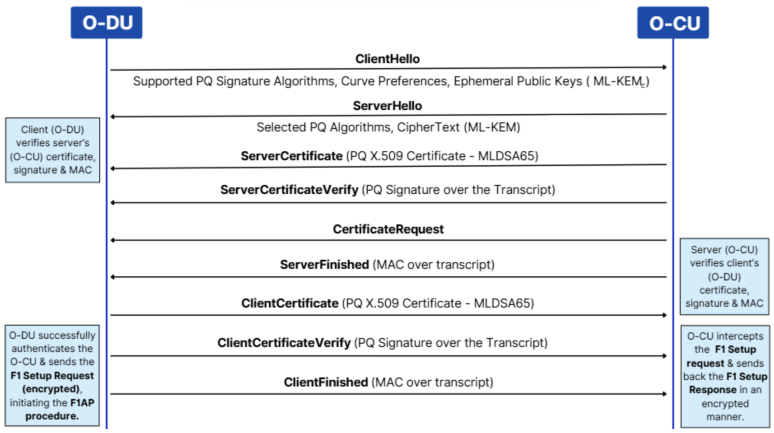

Figure 5: Post-Quantum DTLS 1.3 Handshake Flow between O-DU and O-CU showing ML-KEM-based key exchange and ML-DSA-65 signed X.509 certificates for mutual authentication, ensuring a quantum-resilient F1 interface setup.

Component	PQ Certificate Authority (CA) Specification
Root CA	Hybrid keypair (Ed448/p384 + ML-DSA-65)
Certificate Profile	Composite or hybrid public key + PQ extensions
OCSP / CRL	Signed with PQ-compatible algorithm
Key Storage	Hardware Security Modules
Key Usage	CA Signature, CRL Sign

Table 6: Post-Quantum Certificate Authority Specification

triggered before expiration, minimizing service disruption.

Revocation: Certificate revocation relies on digital records like Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responders, which have been extended to support post-quantum certificates. These mechanisms allow operators to verify certificate status in real time and revoke certificates promptly, which is critical for maintaining security in fast-changing 5G environments.

Automated Management Protocols: To handle cer-

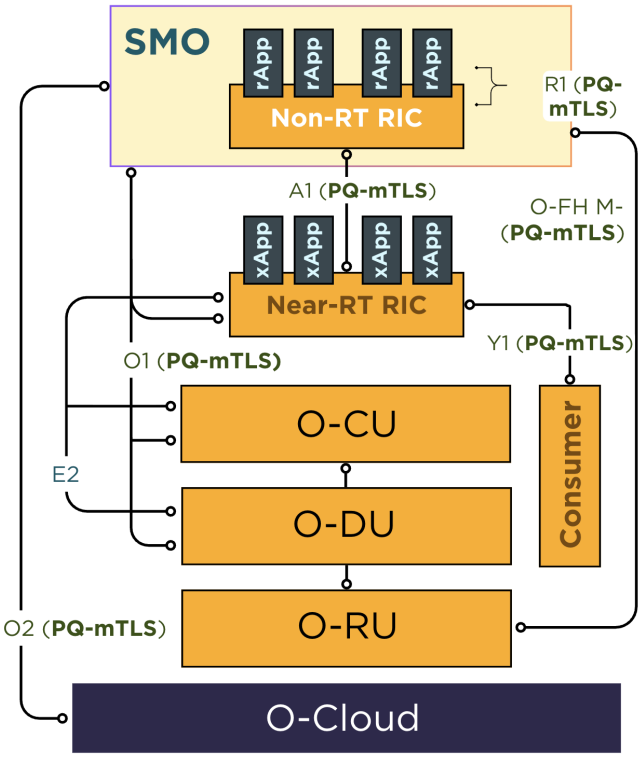

Figure 6: O-RAN SMO Architecture with Security Protocols showing PQ-mTLS on interfaces (R1, A1, O1, O2, O-FH M-Plane, Y1) and PQ-OAuth2.0 for rApps, xApps, and Y1 Consumers.

tificate lifecycles at scale, the ACME protocol [23] has been adapted for post-quantum cryptography. This allows for automatic issuance, renewal, and revocation of PQ X.509 certificates without manual steps. ACME protocol sessions are protected via PQ-mTLS, with regular re-keying to mitigate nonce reuse risks in GCM modes.

Operational Considerations: The post-quantum Certificate Authority (PQ-CA) integrates directly with O-RAN orchestration and monitoring tools, i.e., the SMO. It offers endpoints for provisioning and monitoring certificates, providing easily accessible certificate lifecycle monitoring functionalities to various participating entities.

Post-Quantum JWT (Signed with ML-DSA-65)

```
Header: {
"alg": "ML-DSA-65",
"typ": "JWT"
}
Payload: {
"iss": "SMO-OAuth",
"sub": "xApp-01",
"exp": 1799999999
}
Signature: ML-DSA-65 Signature (Base64URL)
```

Figure 7: Post-Quantum JWT Example

3.6.2 Quantum-Secure Authorization for RIC Applications

In multi-vendor environments with third-party applications, correct (and secured) authentication and authorization are critical. The SMO, enhanced with PQ-CA, and a PQ OAuth 2.0 Server (AS) functions as a quantum-secure authorization server managing access control for rApps and xApps.

PQ-Token Based Authorization: When rApps or xApps need access to protected resources or APIs (e.g., over R1 or A1 interfaces), they request access tokens from the SMO. The SMO issues Post-Quantum Tokens (PQ-Tokens), typically JSON Web Tokens (JWT) where signatures are generated using ML-DSA, making tokens verifiable and tamper-proof against quantum adversaries. A sample PQ-Token is shown in Figure 7.

Secure Communication Channels: Communication channels used by SMO components, RICs, and applications are secured using PQ-mTLS. Mutual authentication for connections uses PQ certificates issued by PQ-CA. This ensures when PQ-Tokens are transmitted, they travel over channels that are confidentially protected and authenticated with quantum-resistant identities, creating comprehensive, end-to-end secure frameworks.

4 Implementation of PQ-Security in Open RAN

Our Post-Quantum RAN security solution was implemented by extending the cryptographic and transport layers of the Open RAN software stack, using both standardized and experimental libraries that support quantum-resistant algorithms.

4.1 O-RAN Software Stack

To explore the integration of Post-Quantum security protocols, we adopted an O-RAN-compliant software stack. We chose **OpenAirInterface5G (OAI)** [24] as the base for

our disaggregated gNB (CU/DU) stack, given its commendable performance and close alignment with 3GPP and O-RAN specifications. We plan to extend this Post-Quantum framework to the O-RAN Distributed Unit (DU) and evaluate other open-source RAN implementations as well.

4.2 Cryptographic Libraries

Most current cryptographic libraries lack full support for PQC-enhanced versions of security protocols, primarily due to the rapidly evolving nature of the field. However, through custom patches and by integrating multiple libraries, we were able to achieve functional Post-Quantum support—albeit not at full production maturity. The following libraries were used to support PQC primitives:

- **liboqs** [25]: A C library providing quantum-safe Key Encapsulation Mechanisms (KEMs) and digital signature algorithms. It was used to enable PQ support in TLS handshakes and certificate verification across TLS/DTLS protocols.
- **OpenSSL** [26]: One of the most widely used cryptographic libraries, supporting TLS/DTLS and certificate management. Recent versions offer support for ML-KEM-based hybrid key exchanges in TLS 1.3, which we utilized in our mTLS and DTLS implementations.
- **strongSwan** [27]: A robust and widely deployed IPsec/IKEv2 implementation, supporting advanced features like EAP-AKA, MOBIKE, and Traffic Confidentiality. Since version 6.0.0, strongSwan supports the Post-Quantum IPsec extensions defined in RFC 8784 and RFC 9370.
- **wolfSSL** [28]: A lightweight TLS/DTLS implementation with native support for PQ algorithms and TLS 1.3. We used wolfSSL to validate PQ-DTLS integration at the RAN layer and to gain additional debugging visibility.
- **cuPQC** [29]: A CUDA-based library for accelerating PQ primitives on NVIDIA GPUs, offering significant performance increases in comparison to CPU-based or software-level implementations. This library is especially useful in cases where we have to serve multiple client requests using IPsec/TLS concurrently (e.g., at SMO). It provides configuration options to tune thread parameters in CUDA-kernels. **cuHash** is another library for offloading SHA-2 / SHA-3 and SHAKE-128 / 256 hash functions on the GPU, which are highly useful in speeding up KDFs, MACs, Merkle Tree based applications, etc.

Figure 8 shows the layered approach to achieve PQ Security using the specified libraries.

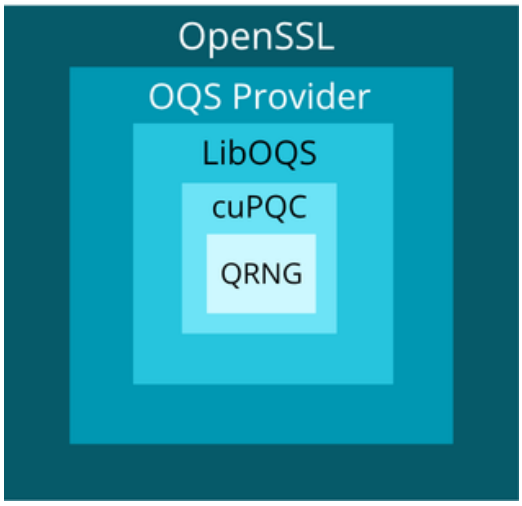

Figure 8: Cryptographic Libraries stack utilized in Q-RAN

4.3 Integration into Open RAN Stack

4.3.1 gNodeB: PQ-DTLS and PQ-IPsec

Since OAI does not natively support DTLS on RAN interfaces, DTLS 1.3 was integrated manually, with built-in certificate authority (CA) support and modular configuration for certificate and protocol parameter selection across vulnerable interfaces. In this setup, DTLS 1.3 was layered on top of SCTP, similar to how TLS operates over TCP. The DTLS stack was built using OpenSSL's SSL objects—designed to work over datagram sockets—and further extended using liboqs to add support for post-quantum cryptographic primitives. Post-quantum operations were offloaded to NVIDIA GPUs using **cuPQC** — to accelerate PQC primitives — significantly improving throughput, especially for short-lived DTLS sessions that require frequent rekeying. It further helped in sustaining the desired throughput expected from 5G RAN.

The IETF Draft [30] extends the DTLS 1.3 protocol for use over SCTP datagrams, adding support for SCTP-AUTH chunks, multihoming, multiple streams, and preserving SCTP's built-in reliability mechanisms. However, most open-source TLS/DTLS libraries do not natively support these features. As a result, a key challenge was ensuring interoperability between DTLS 1.3 implementations and OAI's native SCTP interfaces—without compromising any existing SCTP functionality.

The encryption overhead added by DTLS also had to be carefully optimized to closely match the throughput of unencrypted links. Additionally, IKEv2 and IPsec ESP were configured in tunnel mode via strongswan to guarantee confidentiality and authentication for payloads, as well as the endpoint metadata. Rekeying intervals were appropriately set up to maintain forward secrecy and ensure connection freshness. To sustain the high-throughput requirements on the 5G data plane, IPsec ESP processing was offloaded to NVIDIA BlueField-3 (BF3) DPUs using the DOCA libraries [31], enabling performance levels suitable for production-grade deployments.

4.3.2 SMO: PQ-mTLS and PQ-OAuth 2.0

Post-Quantum mTLS 1.3 was integrated into the O-RAN's SMO and RIC components using a dedicated service mesh enhanced with support for PQ algorithms. This allowed us to deploy primitives such as ML-KEM-768 and ML-DSA-65. A Post-Quantum OAuth 2.0 server was deployed at the SMO, issuing and verifying PQ-signed tokens over interfaces like A1 and R1. Other control-plane elements were connected to each other using PQ-IPsec via strongSwan, ensuring consistent security across the RAN management domain.

4.3.3 TLS Handshake Modes and Algorithms

Our implementation supports both hybrid and pure Post-Quantum TLS 1.3 handshakes:

- **Hybrid KEMs**: ECDHE combined with Kyber or ML-KEM (FIPS 203).
- **Signature Algorithms**: Ed448-ML-DSA-65, SLH_DSA_SHA2_256F, Falcon_512/1024, other composite or pure PQ signature schemes.
- **Fallback and Interoperability**: The system falls back to a classical configuration using ECDHE and EdDSA/ECDSA when it detects that a peer does not support PQ-TLS 1.3 (typically when clients do not send PQ group preferences in ClientHello).

4.4 Deployment and Validation

The Post-Quantum secured O-CU/O-DU, SMO, and other components were deployed in a complete integrated stack (including 5G Core and Radio Units), validated against multiple end-to-end UE tests with tests for internet speed, and stability. The Post-Quantum nature of the services was verified as follows:

- **Interoperability**: Verified against Kubernetes components and classical TLS clients by integrating fallback certificate paths.
- **Performance**: Handshake times and encryption performance were logged and compared to classical baselines.
- **Security**: Validated using wolfSSL-based TLS sniffers, OpenSSL test clients for hybrid (D)TLS 1.3 draft extensions.

5 Challenges in Migrating to Post-Quantum O-RAN Security

Despite standardized PQC algorithms and hybrid specifications, deploying them across the O-RAN ecosystem introduces multiple technical, operational, and interoperability challenges. This section details critical issues encountered during transition to Post Quantum versions of IPsec, TLS/DTLS, OAuth 2.0, JWKS.

5.1 Challenges in PQ-IPsec Implementation

1) Use of Post-Quantum Certificates: Modern X.509 certificate infrastructures and protocols (such as IPsec) typically handle certificates in the size range of 0.5–1.5 KB, with complete certificate chains contributing a few additional kilobytes to the authentication data exchanged between peers.

However, with the advent of quantum computers, the need for post-quantum cryptographic (PQC) primitives has become critical. These newer primitives, such as ML-DSA, often do not integrate seamlessly into contemporary protocols due to their significantly larger sizes (10–20 KB). This increase frequently leads to practical challenges, including increased bandwidth usage, increased connection setup delays, and a higher risk of packet loss.

Practical deployments of PQC in IKEv2 must address these issues using techniques such as certificate compression through Hash and URL method specified in [32], and (or) IKE message fragmentation [33]. The contrast between key and signature sizes of classical and Post-Quantum Schemes is shown in Table 7.

5G RAN systems typically have sufficient computing capabilities and networking facilities available to them, thus reducing the impact of PQC on them. However, the increased message sizes can introduce delays in time sensitive 5G Interfaces, such as F1AP, NGAP, etc.

2) Fragmentation and Intermediate Exchange: Post-Quantum Key Exchanges (e.g., ML-KEM-768) introduce significantly larger key and ciphertext sizes ($\sim$ 2–3 KB), in contrast to the relatively small sizes of classical algorithms like ECDH. This increase in message size is a major contributor to fragmentation in IKEv2 messages, which are carried over UDP. When message sizes exceed the Path Maximum Transmission Unit (MTU) — often limited by middleboxes such as NATs and firewalls — it can result in packet loss and delays in completing the connection.

Given the inherent unreliability of UDP, such packet loss can lead to failures in the key agreement process, especially over longer network paths. [33] addresses this by introducing a mechanism to fragment large encrypted IKE messages into multiple IKE_Fragment payloads. However, it does not support fragmentation during the initial key exchange, where the post-quantum keys themselves are exchanged. This gap is addressed by [34] (Intermediate Exchange), which specifies a mechanism for handling fragmentation during the initial IKE_SA_INIT phase by introducing Intermediate Key Exchanges which are strategically used to place Post-Quantum Keys, creating a hybrid solution.

IPsec deployments over 5G interfaces require frequent re-keying to maintain forward secrecy, keep shared secrets fresh, and mitigate risks such as nonce reuse and birthday attacks associated with GCM modes [35] [36]. The use of post-quantum key encapsulation mechanisms (KEMs) may introduce slight delays in the re-keying process, potentially impacting time-sensitive operations in existing networks.

3) PPK Synchronization: RFC 8784 Post-Quantum Pre-Shared Keys (PPKs) must be securely provisioned and rotated. Distribution through SMO or SDN controllers requires new key management APIs and synchronization protocols.

4) Hardware Acceleration: High-performance data processing units (DPUs), FPGAs, and cryptographic accelerators are widely employed in 5G networks to offload and accelerate IPsec and other security protocols, ensuring state-of-the-art throughput. However, most existing hardware accelerators currently lack native support for post-quantum cryptographic (PQC) algorithms. To sustain the required throughput on high-bandwidth and throughput interfaces such as N3 and E2, integration of PQC-capable hardware accelerators or FPGA implementations is essential.

5.2 Challenges in PQ-TLS/DTLS Integration

1) Certificate Chain Sizes:

Post-Quantum X.509 certificates cause noticeable bottlenecks in TLS/DTLS-secured connections due to their substantially larger size—a challenge also observed in IPsec contexts. As analyzed in [37, 38], post-quantum variants of TLS 1.3 introduce higher handshake overheads compared to classical cipher suites.

In TLS (e.g., TLS 1.3 [39]), these larger certificate payloads are transmitted over TCP, using segmentation and TLS record-layer fragmentation [40]. However, the efficiency of this process is influenced by the initial

Scheme	Key + Signature Size (KB)
ECDSA	0.1
RSA	0.5
Lattice-based	11
Stateful HBS	15
Stateless HBS	42
ZK Proofs (ex: Picnic L1FS)	66
Multivariate	100
Supersingular Isogenies	122
Code-based	190

Table 7: Broad estimates for key and signature sizes for selected cryptographic schemes.

TCP congestion window and the behavior of the selected congestion control algorithm. If the TCP window is too small—particularly during the handshake phase—transmission of large certificate chains may be throttled, resulting in increased latency and multiple round trips if the available `init_cwnd` or Maximum Segment Size is insufficient to transmit the full message. This is particularly impactful in high-latency paths or edge-cloud architectures where TCP slow start dominates short-lived control-plane sessions.

DTLS (e.g. DTLS 1.3 [8]), operating over UDP/SCTP, handles large handshakes by fragmenting handshake messages at the protocol level. Each fragment is acknowledged independently, and losses trigger retransmission of specific fragments, adding protocol overhead and increasing handshake latency—particularly over unreliable or constrained networks.

To mitigate certificate size overhead, TLS certificate compression has been standardized in [41], allowing endpoints to compress certificate chains using algorithms like zlib. However, the compression of Post-Quantum certificates is not well discussed as of now. Other methods include enabling hardware acceleration for TCP Segmentation Offload (TSO) and Large Receive Offload (LRO).

2) Larger Key Exchanges:

In addition to handshake overhead, post-quantum cryptography introduces rekeying challenges. TLS/DTLS-secured channels in 5G networks require frequent rekeying to maintain forward secrecy and mitigate nonce reuse vulnerabilities inherent in GCM modes [35]. Post-Quantum KEMs increase the computational and bandwidth costs of rekeying, contributing to an additional transport-layer stress.

Even in non–resource-constrained 5G infrastructure, these issues can manifest as:

- Increased handshake and rekeying latency across control and data-plane interfaces.
- Greater susceptibility to MTU fragmentation and packet loss, especially over DTLS.
- Suboptimal TCP performance due to limitations in window scaling during large initial handshakes.
- Delays in control-plane responsiveness during orchestration, scaling, or mobility events.
- Incompatibilities with middleboxes or firewalls enforcing strict packet size or fragmentation policies.

SCTP Encapsulation by PQ-DTLS 1.3: As specified in [22], when SCTP packets are encapsulated by DTLS, the protocol must respect SCTP's inherent packet reordering and reassembly mechanisms and avoid using compression algorithms. Large post-quantum (PQ) handshake messages can pose challenges for SCTP, as Path MTU Discovery (PMTUD) may not fully accommodate the increased sizes of keys and certificates. This can result in fragmentation at the IP or SCTP layers, introducing additional latency and processing overhead on both communicating peers. IP fragmentation is generally discouraged and considered fragile [42].

To ensure reliable and efficient integration of post-quantum TLS in 5G networks, requires several mitigation strategies. Techniques like certificate compression [41], tuning of TCP window sizes, DTLS 1.3 fragmentation [8], and adjustments to MTUs and middlebox behavior are all needed to manage the larger payloads introduced by PQC. Interoperability remains a key concern, especially since many vendors—particularly those supplying Physical Network Functions (PNFs)—have not yet adopted PQ algorithms or protocol extensions. This is particularly noticeable on radio-facing links like the O-FH M-Plane, where older equipment typically lacks support for PQ-enabled control and management.

5.3 Standardization Challenges

- **Multi-Vendor Environment:** O-RAN's disaggregated RAN architecture comprises components from multiple vendors, which increases the challenge of ensuring interoperability and consistency across PQC implementations.
- **Diverse Network Architecture:** O-RAN defines numerous interfaces (e.g., F1, N2, N3), each with distinct security and transport requirements. Integrating post-quantum cryptography for each interface increases complexity and necessitates customized testing and development.
- **Lack of Unified Conformance tests:** The lack of conformance tests for stability, connectivity in vendor-neutral O-RAN deployments adds hindrance to stable deployments of PQC-enabled RAN.
- **Developing Standards:** Post-quantum cryptography standards continue to evolve, with many algorithms (e.g., ML-KEM, ML-DSA) only recently standardizePost-quantum cryptography standards continue to evolved by NIST. PQ alternatives of protocols are still under development and performance testing. This uncertainty and fast-moving nature make it difficult to define stable, long-term cryptographic baselines for O-RAN interfaces, which de-

lays integration into official O-RAN Alliance specifications.

- **Limited Expertise in PQC:** A shortage of engineers skilled in both O-RAN and PQC has slowed down practical adoption and standardization efforts.

6 Q-RAN: Implementation Details

In this section we provide detailed implementation specifications for Q-RAN, the quantum-secure O-RAN solution. We provide protocol specifications, software libraries, and real solution logs from testing and evaluation environments.

Figure 9 illustrates the complete Q-RAN security architecture.

6.1 PQ-TLS/DTLS Enhancement Specifications

The Q-RAN solution integrates comprehensive, well-tested quantum-resistant upgrades into TLS and DTLS, ensuring cryptographic robustness across the entire lifecycle—from key generation and exchange to authentication and encryption. Building on the protocol-level upgrades outlined earlier, we now summarize the key architectural and cryptographic design choices made to implement a robust, forward-compatible security framework. These include:

6.1.1 Hybrid Key Exchange Mechanisms

Q-RAN supports both pure and hybrid PQ key exchange methods. The most commonly used hybrid method is summarized below:

X-Wing: A hybrid KEM, X-Wing combines X25519 and ML-KEM-768 into a general-purpose KEM designed for efficiency and simplicity, as detailed in [43]. This construction is suitable for use in protocols like TLS and DTLS. X-Wing is IND-CCA secure, with overall security bounded by the respective strengths of ML-KEM-768 and Curve25519 (gap C-DH). The hybrid KEM remains secure under the assumption that SHA-3 is collision- and preimage-resistant. X-Wing achieves superior performance by introducing optimizations such as omitting the hashing of ML-KEM ciphertexts and flattening DHKEM, a feature often missing in other hybrid KEMs. It also extends plain ML-KEM by providing additional binding properties, including MAL-BIND-K, CT-PK, and LEAK-BIND-K-CT. As described in [43], the key sizes for this hybrid KEM are 1184 octets for the public key and 2464 octets for the private key, with a ciphertext size of 1120 octets.

6.1.2 Hybrid Digital Signature Algorithms

Quantum-resistant authentication requires upgrading digital signatures using composite approaches that combine classical and post-quantum algorithms. A signature is valid only if both components verify correctly.

The hybrid signature scheme adopted in Q-RAN is **Ed448-ML-DSA-65**, which guarantees SUF-CMA (Strong Unforgeability under Chosen Message Attack) due to the individual properties of its underlying schemes [44]. The composite scheme utilizes pre-hashing for the Ed448 signature using the XOF SHAKE256. Pre-hashing is deliberately avoided for ML-DSA to mitigate potential collision risks [44]. We further incorporate context strings and algorithm-specific prefixes into the signing process and disallow standalone use of individual keys to achieve stronger non-separability (SNS), thereby preventing an attacker from producing a valid signature using only one component. [1]

6.2 Quantum-Resistant DTLS Implementation

DTLS 1.3 was selected for Q-RAN as it is the only version compatible with the addition of post-quantum key exchanges and signatures. DTLS 1.3 also provides mandatory forward secrecy and robust fragmentation—improvements over the optional forward secrecy and brittle fragmentation mechanisms in DTLS 1.2. The inclusion of frequent rekeying and reduced round-trip times (RTT) in version 1.3 enhances both security and performance. Figure 15 shows the packet capture logs for DTLS 1.3.

The post-quantum hybrid suites described earlier are reused in DTLS 1.3, wherein the client initiates the key share and the server responds with the PQ-KEM ciphertext. PQ certificate chains and signatures are employed in the Certificate and CertificateVerify payloads. Q-RAN also supports experimental testing with other PQ KEMs (HQC, BIKE, NTRU, Saber, FrodoKEM) and signature schemes (SLH, Falcon, CROSS, LMS/XMSS).

A practical demonstration of Post-Quantum DTLS 1.3 on the midhaul interface is available in the video *Securing Midhaul Interface Using PQ-DTLS 1.3*. The Post-Quantum DTLS 1.3 session details are briefed in Figure 10.

6.2.1 Certificate-Based Authentication

Authentication is anchored by a Post-Quantum Certificate Authority (PQ-CA) logically hosted within the SMO framework. The SMO issues and manages quantum-resistant identities for all network components, including RICs, CUs, DUs, and applications.

The PQ-CA issues X.509 certificates using composite signature algorithms. The `p384mldsa65` specification represents a hybrid signature combining:

- **p384:** Classical ECDSA using the NIST P-384 curve, a widely trusted standard.
- **mldsa65:** NIST-standardized post-quantum ML-DSA using the `ml-dsa-65` parameter set, offering an excellent security-performance balance.

This composite approach, aligned with current IETF drafts, ensures signatures are valid only when verified by both classical ECDSA and post-quantum ML-DSA algorithms, providing crypto-agility and backward compatibility.

6.2.2 Handshake and Symmetric Encryption

While authentication uses composite signatures, DTLS 1.3 handshakes are hardened through hybrid KEMs that combine classical key agreement (ECDHE) with PQC KEMs (ML-KEM). Figure 11 shows the various Handshake states for DTLS 1.3 during the handshake.

Once the hybrid handshake completes and shared secrets are established, the connection transitions to symmetric encryption for subsequent data transfer. The specified

[1] Note: All modes of ML-DSA and ML-KEM are supported in the Q-RAN solution, along with both pure PQ and hybrid configurations, providing flexibility for different security and operational requirements.

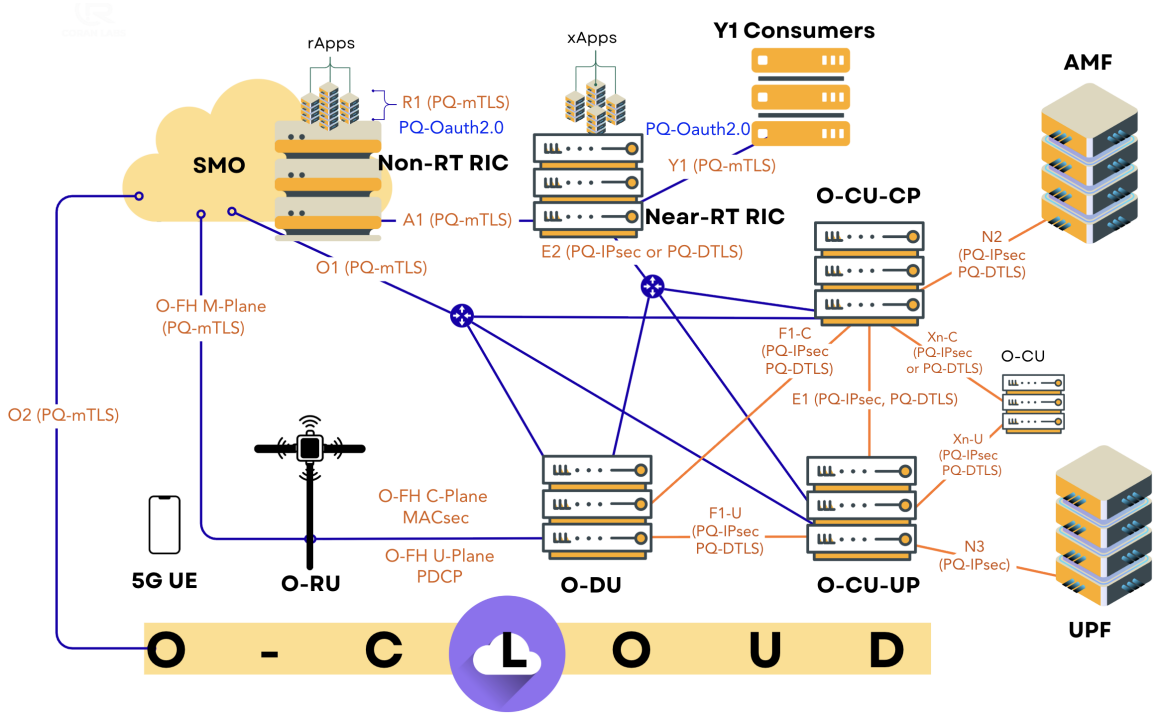

Figure 9: Q-RAN Security Architecture showing complete integration of PQ-mTLS, PQ-IPsec/PQ-DTLS, PQ-OAuth2.0 across all O-RAN interfaces connecting SMO, Non-RT RIC, Near-RT RIC, O-CU, O-DU, O-RU, O-Cloud, 5G UE, AMF, and UPF.

```
------------------DTLS SESSION Details------------------------
SSL-Session:
    Protocol  : DTLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID:
    Session-ID-ctx:
    Resumption PSK:
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1752846852
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---------------------------------------------------------------
[2025-07-18T13:54:12] [DEBUG ] [DTLS   ] No session ticket available.
Hostname: None
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] Hostname: None
```

Figure 10: PQ DTLS 1.3 Session between CU and DU

cipher suite, `TLS_AES_256_GCM_SHA384`, provides strong, standardized encryption for TLS 1.3:

- **AES-256-GCM:** AES-256 is widely considered quantum-resistant, making it the preferred choice for symmetric encryption. GCM mode provides AEAD (Authenticated Encryption with Associated Data), ensuring both data integrity and confidentiality via GHASH and AES-CTR operations. Due to AES-GCM's nonce reuse restrictions, extended nonce variants (e.g., XAES-GCM) may be used for high-throughput RAN interfaces.
- **SHA-384:** The SHA-384 hash function (SHA-2 family) is employed in the TLS/DTLS key schedule, specifically in the HKDF-based key derivation process (`Extract-Expand`), to produce pseudorandom secrets and expand them into subkeys (e.g., MAC keys, AEAD keys).

Given the high throughput of 5G interfaces, it frequently triggers DTLS 1.3 key updates to maintain forward secrecy and limit key reuse. Figure 12 depicts the encryption of F1AP messages at the DU. The implementation (with support for split 7.2) is available at github.com/coranlabs/Q-RAN.

6.2.3 QRNG Integration

All PQC algorithms rely critically on high-entropy random numbers. Q-RAN integrates Quantum Random Number Generators (QRNGs) as entropy sources for all cryptographic operations.

Ephemeral Key Generation: For each DTLS session, hybrid KEMs require ephemeral key pairs. QRNGs supply high-entropy seeds to ensure these keys are unpredictable and independent across sessions.

Certificate and Signature Generation: The PQ-CA within the SMO uses QRNGs to generate long-term private keys for composite certificates. Additionally, ML-DSA depends on QRNGs for nonce generation, ensuring each signature operation is unique and resistant to private-key

```
[2025-07-18T13:54:11] [DEBUG ] [ F1AP  ] Message received in F1AP CU task: ID=112.
[2025-07-18T13:54:11] [ INFO ] [DTLS   ]
Received new DTLS handshake request
[2025-07-18T13:54:11] [ INFO ] [DTLS   ] SSL Handshake started

[2025-07-18T13:54:11] [ INFO ] [DTLS   ] SSL state: before SSL initialization
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: before SSL initialization
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: SSLv3/TLS read client hello
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: SSLv3/TLS write server hello
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: TLSv1.3 write encrypted extensions
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: SSLv3/TLS write certificate request
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: SSLv3/TLS write certificate
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: TLSv1.3 write server certificate verify
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: SSLv3/TLS write finished
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: TLSv1.3 early data
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: TLSv1.3 early data
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: SSLv3/TLS read client certificate
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: SSLv3/TLS read certificate verify
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL state: SSLv3/TLS read finished
[2025-07-18T13:54:12] [ INFO ] [DTLS   ] SSL Handshake finished
```

Figure 11: SSL States at each stage of the handshake

```
[2025-07-18T13:54:14] [ INFO ] [ F1AP  ]  F1AP Setup Response Transmisson Status [from CU]: Successfu
ll
[2025-07-18T13:54:14] [ INFO ] [DTLS   ] Encrypted buffer: 66 bytes

[2025-07-18T13:54:14] [ INFO ] [DTLS   ] SSL Write: 66 bytes

[2025-07-18T13:54:14] [ INFO ] [ SCTP  ] Sending the message (enc) :
40 01 00 3E 00 00 04 00  4E 00 02 00 01 00 52 40
0E 05 80 43 6F 72 61 6E  4C 61 62 73 2D 43 55 00
03 00 11 00 00 00 04 00  0B 40 00 F1 10 00 0B C6
14 E0 00 00 00 AA 00 0A  80 00 00 00 C7 40 03 11
03 00
[2025-07-18T13:54:14] [DEBUG ] [ SCTP  ] Successfully sent 96 encrypted bytes on stream 0 for assoc_i
d 1998
```

Figure 12: F1AP Messages under DTLS encryption

leakage attacks.

6.3 Quantum-Resistant mTLS Implementation

Following O-RAN specifications [5], Q-RAN adopts TLS 1.3 with post-quantum extensions similar to the PQ-DTLS 1.3 design described above. The same primitives are reused to maintain uniform security and cryptographic consistency across the RAN. We also acknowledge ongoing IETF developments such as [45], [46], and [47]. Figure 13 shows ML-KEM as the key exchange in the ClientHello message of TLS 1.3.

6.3.1 Authentication Architecture

The private PQ-CA hosted within the SMO issues quantum-resistant X.509 certificates to all O-RAN components, establishing a verifiable quantum-safe root of trust. Certificates employ hybrid signature schemes combining classical and post-quantum algorithms—typically NIST-standardized ML-DSA (e.g., ML-DSA-65) with Ed448 or Ed25519. Signatures are valid only if both the classical and quantum components verify successfully, ensuring resilience even if one algorithm is compromised.

6.4 Quantum-Resistant IPsec Implementation

Q-RAN's IPsec stack employs a multi-layered quantum-resistant approach built upon the strongSwan IKEv2 implementation. strongSwan's maturity and extensibility enable integration of modern post-quantum extensions. Packet capture for IPsec ESP working in conjunction with NGAP (SCTP) shown in Figure 14.

6.4.1 Hybrid Key Exchange and Authentication Implementation

Notes (Table 8:

- **ML-KEM-768** provides post-quantum key encapsulation (RFC 9370).
- **PPKs** offer hybrid PQ authentication (RFC 8784) — 256-bit classical, ≈128-bit quantum-safe.
- PQ KEM to strengthen rekeying (CREATE_CHILD_SA).

6.4.2 strongSwan Library Configuration

This quantum-resistant IPsec solution is implemented using strongSwan library, which can be compiled with Open Quantum Safe (OQS) liboqs plugin to enable support for necessary PQC algorithms. Latest strongSwan versions (6.0.0+) have begun integrating this functionality more directly, streamlining configuration of hybrid key exchanges.

Example strongSwan configuration for PQ-IPsec:

```
{conn pq-ikev2
    ppk=yes
    ppk_id=qrng-generated-ppk-id
child pq-ipsec-tunnel{
    ike=aes256-sha384-ecp384-ke1_mlkem768!
    esp=aes256gcm128-sha384-ecp384!
    }
}
```

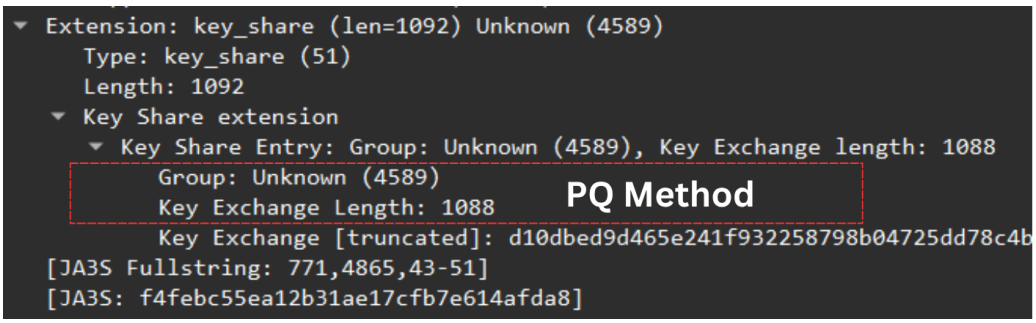

Figure 13: Packet capture for Post-Quantum KEMs in TLS 1.3

Direction	Message Content	Post-Quantum Component
`IKE_SA_INIT` Initiator → Responder	HDR, SAi1 (AES-CBC-256, HMAC-SHA2-256, PRF-HMAC-SHA2-256, DH14), KEi, Ni, N(INTERMEDIATE_EXCHANGE_SUPPORTED), [CERT]	–
Responder → Initiator	HDR, SAr1, KEr, Nr, [CERTREQ], N(INTERMEDIATE_EXCHANGE_SUPPORTED)	–
`IKE_INTERMEDIATE` Initiator → Responder	HDR, SK{ KEi(n) (**ML-KEM-768 public key**) }	**ML-KEM-768**
Responder → Initiator	HDR, SK{ KEr(n) (**ML-KEM-768 public key**) }	**ML-KEM-768**
`IKE_AUTH` Initiator → Responder	HDR, SK{ IDi, [CERT], [IDr], AUTH (with **PPK**), SAi2 (ESP proposal), TSi, TSr, N(**PPK_IDENTITY, PPK_ID**) }	**PPK**
Responder → Initiator	HDR, SK{ IDr, [CERT], AUTH, SAr2, TSi, TSr, N(**PPK_IDENTITY**) }	**PPK**
`CREATE_CHILD_SA` Initiator → Responder	HDR, SK{ SA (ESP proposal), Ni, [KEi], TSi, TSr }	(Optional **PQ KEM**)
Responder → Initiator	HDR, SK{ SA (selected), Nr, [KEr], TSi, TSr }	(Optional **PQ KEM**)
`INFORMATIONAL` Initiator → Responder	HDR, SK{ DELETE, NOTIFY: NAT_DETECTION_SOURCE_IP }	–
Responder → Initiator	HDR, SK{ DELETE Response / ACK }	–

Table 8: IPsec (IKEv2) message flow with post-quantum components highlighted.

6.4.3 Entropy Source Integration

The high-quality randomness provided by QRNGs, as discussed previously, is securely provisioned to each RAN component through encrypted peripheral links, preventing eavesdropping or tampering. The seeds and the required purpose are described in the Table 9.

Scheme	Keygen Seed	Encap Seed	Sign Seed
ML-KEM-768	64 B	32 B	—
ML-DSA-65	32 B	—	32 B (opt.)
X-Wing (Hybrid)	32 B	32 B	—
Ed448-ML-DSA-65	57 B	—	32 B (opt.)

Table 9: Seed sizes (bytes) used in key generation, encapsulation, and signing for various schemes.

6.4.4 Certificate-Based Authentication

Digital certificates used for IKEv2 peer authentication must be quantum-resistant. These certificates are issued by centralized Post-Quantum Certificate Authority (PQ-CA) lo-

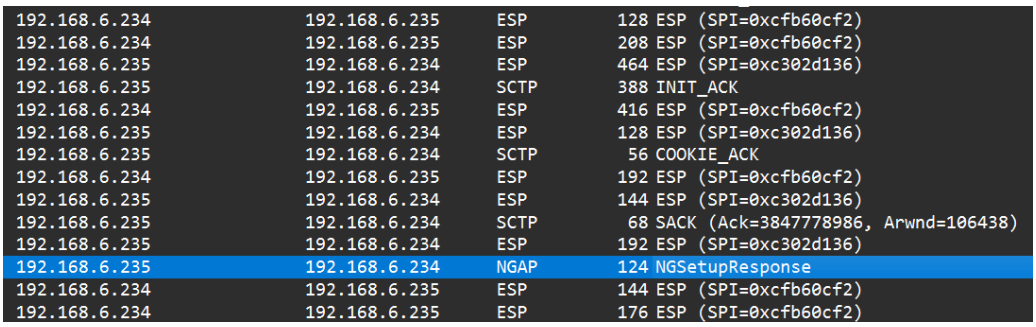

Figure 14: Packet Capture for IPsec ESP encryption and decryption for SCTP Packets

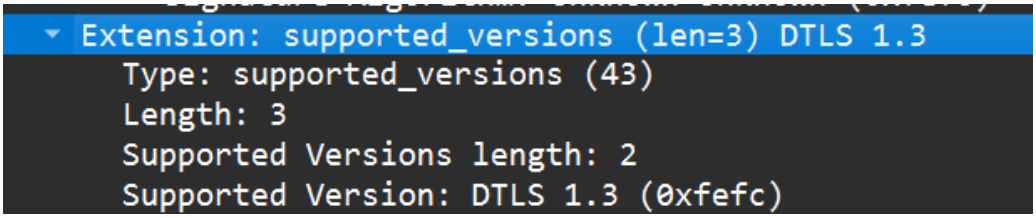

Figure 15: Packet Capture for DTLS 1.3

cated on the SMO. The PQ-CA uses composite signature schemes like p384mldsa65 to sign certificates, ensuring they are trusted and verifiable in both classical and post-quantum environments. The composite signature schemes are thought to provide dual-security until active quantum adversaries are not present, and provide an easier transition to pure Post-Quantum methods.

QRNGs serve as roots of trust for all randomness, used to generate high-entropy seeds for all ephemeral keys in Asymmetric Key exchanges and for PPKs. Furthermore, private keys for certificates issued by PQ-CA are also generated using QRNGs, ensuring entire cryptographic lifecycles and certificate truststore are secured with provably unpredictable randomness.

6.5 Post-Quantum SMO Security Architecture

The SMO security strategy focuses on robustly protecting all communication channels—both external interfaces (O1, O2, A1, R1) and internal communications between microservices (SMOs) as shown in Figure 16 . This protection is provided via PQ-mTLS, and PQ-OAuth 2.0 between the participating entities.

6.5.1 PQ-mTLS 1.3 for All Communications

The mandated mechanism is mutual Transport Layer Security (mTLS), specifically based on TLS 1.3, enhanced to incorporate post-quantum (PQ) cryptography. The upgrade process aligns closely with proposals such as PQ-(D)TLS 1.3, but includes modifications to the `ClientCertificate` and `ClientCertificateVerify` messages on client side to support post-quantum X.509 certificates and post-quantum digital signatures.

6.5.2 Centralized Public Key Infrastructure

Beyond securing its own communications, the SMO functions as central PKI governance engine for the entire RAN, acting as management and registration authority for underlying Post-Quantum Certificate Authority (PQ-CA). The PQ-CA is the core trust anchor responsible for signing all quantum-resistant identities, while the SMO orchestrates complex lifecycles of these PQC certificates.

This includes automated issuance, renewal, distribution, and revocation for every network function, effectively translating operator policy into actions performed by PQ-CA. Centralized management is essential for enforcing consistent cryptographic policies and achieving crypto-agility necessary to respond to future threats.

6.5.3 Quantum-Resistant Application Authorization

RAN Intelligent Controllers (Non-RT RIC and Near-RT RIC) and third-party applications they host (rApps and xApps) are O-RAN's innovation engines, enabling AI/ML-driven network optimization. However, allowing third-party code to control RAN introduces significant security risks. A robust, quantum-resistant authorization framework is required.

The O-RAN Alliance specifies OAuth 2.0 framework for this purpose. A quantum-resistant implementation, termed PQ-OAuth, provides granular, token-based authorization aligning with Zero Trust Architecture principles [21] [48].

Authorization Architecture Roles

- **Authorization Server(AS):** Logical role fulfilled by dedicated service within SMO framework, responsible for authenticating clients and issuing access tokens. The AS also hosts a JSON Web Keys Set (JWKS) [49] endpoint for clients to fetch the PQ verification keys in JSON format.
- **Client:** rApp or xApp requesting access to protected resources.
- **Resource Server:** O-RAN service or function exposing protected APIs (e.g., R1 interface service provider within SMO for rApps, A1 interface on Near-RT RIC for xApps)

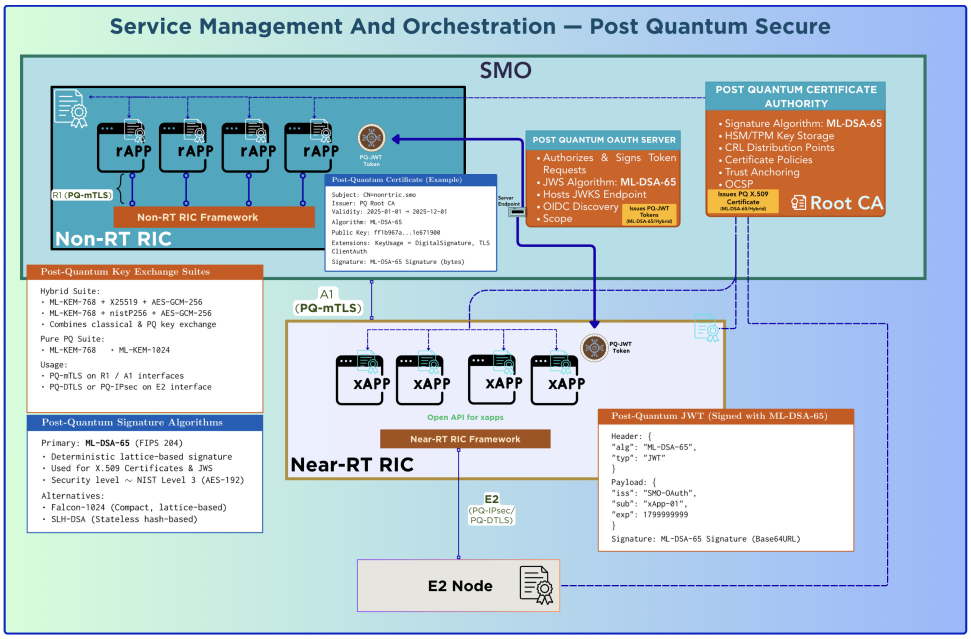

Figure 16: Post-Quantum Secure SMO architecture integrating PQ-mTLS, PQ-IPSec/PQ-DTLS, and PQ-OAuth 2.0 across Non-RT RIC, Near-RT RIC, and E2 nodes, enabling quantum-resilient authentication, authorization, and communication through ML-KEM key exchange and ML-DSA-65-based certificates and tokens.

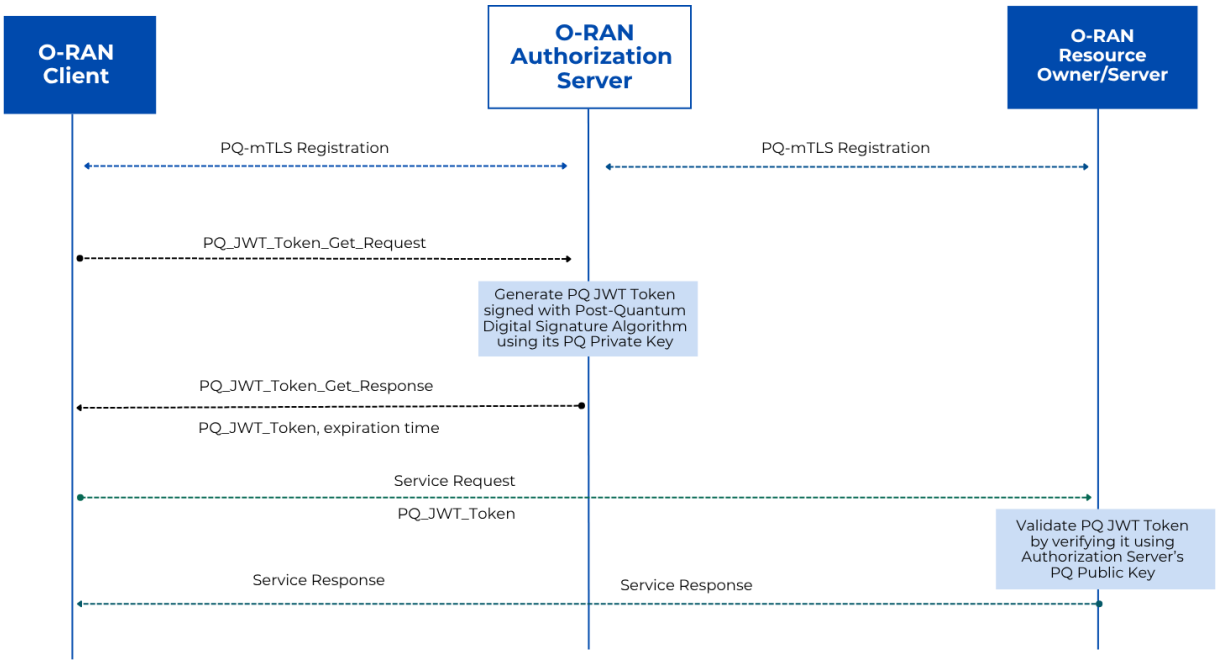

Figure 17: PQ-OAuth 2.0 Flow in Open RAN components

- **Resource Owner:** Network operator defining authorization policies enforced by Authorization Server

Quantum-Resistant Authorization Flow Onboarding and Authentication: rApps/xApps are onboarded onto appropriate RIC platforms by SMO. During onboarding, SMO facilitates requests to Post-Quantum Certificate Authority (PQ-CA), which provisions applications with long-term PQ digital certificates (e.g., composite p384ml-dsa65 certificates).

Token Request: To access protected resources, rApps/xApps initiate PQ-mTLS connections to Authorization Server's token endpoints in SMO. They authenticate themselves using their provisioned PQ certificates, then send requests for access tokens specifying desired scopes (e.g., o-ran-smo:performance-data:read or o-ran-a1:policy:write).

Token Issuance: Authorization Servers verify rApp/xApp identities via mTLS handshakes, consult policy engines to determine if specific applications are authorized for requested scopes. If authorized, they generate JSON Web Tokens (JWT).

PQ-Signed JWT: JWT security is paramount. Authorization Servers sign JWTs using high-assurance private keys. The ed448-dilithium3 specification points to composite signature schemes where JWT headers and payloads are signed separately by both Ed448 (classical) and ML-DSA (Dilithium at level 3) algorithms, with resulting signatures concatenated to form final JWT signatures. JWT header alg parameters contain unique identifiers registered for specific composite schemes, ensuring token integrity and authenticity are protected against both classical and quantum adversaries—active or passive.

Resource Access: rApps/xApps receive signed JWTs, then make requests to Resource Servers (e.g., API calls over R1 interfaces), including JWTs in Authorization HTTP headers as Bearer tokens.

Token Validation: Resource Servers receive requests and must validate JWTs before processing. They retrieve Authorization Server public keys. Trust in these keys is established because Authorization Server identity certificates were issued by network root PQ-CA, which Resource Servers are configured to trust. Resource Servers use trusted composite public keys to verify both Ed448 and ML-DSA signatures on tokens, also validating token claims such as expiration times (exp), intended audiences (aud), and ensuring requested actions are permitted by token scope claims. Only if all checks pass are requests processed.

The token authentication flow described above is summarized in the Figure 17.

A demonstration of the described implementation of Q-RAN, also featuring the usage of our Post-Quantum enabled 5G Core (QORE) and PKI solution is present at **YouTube**.

7 Future Works

This section outlines the prospective directions and development opportunities for advancing quantum-resistant Open RAN (Q-RAN) security and interoperability. Future work focuses on expanding the scope of post-quantum cryptographic (PQC) frameworks across different layers of the 5G Network, enhancing interoperability through xFAPI, integrating PQC with open-source RAN stacks, alongside leveraging hardware acceleration, and extending protection to radio and management interfaces.

7.1 xFAPI-PQC Integration for Vendor-Neutral Interoperability

xFAPI [50] is an interoperability framework designed to eliminate vendor lock-in within the Open RAN ecosystem by providing a standardized mechanism to connect any Radio Unit (RU) to any Distributed Unit (DU). It achieves this by employing inter-process communication (IPC) calls and SCTP-based data transfer mechanisms to ensure efficient interaction between disaggregated components.

To protect xFAPI against quantum-era attacks, we propose adding post-quantum cryptography either at the MAC layer or by encapsulating / layering SCTP traffic using PQ-DTLS 1.3. These upgrades allow secure, low-latency communication between multi-vendor components, with cryptographic primitives tailored specifically for the FAPI's real-time signaling needs.

This design supports cryptographic agility while maintaining interoperability across vendors. As shown in Figure 18, the proposed PQC-enhanced xFAPI architecture is built to serve as a security foundation for future quantum-resilient RAN deployments.

7.2 Extension to OSC and Other Open-Source RAN Platforms

Future work will also focus on bringing post-quantum cryptography to the O-RAN Software Community (OSC) [51] and other open-source RAN projects to expand the quantum-resistant safety net. The goal is to build standardized PQC implementations across open ecosystems, thereby encouraging interoperability, transparency, and long-term security against threats posed by quantum computers. Our presentation at O-RAN Working Group 11 [52] highlights the importance of introducing quantum-safe network architecture into Open RAN and provides insights on how this can be achieved smoothly.

7.3 Hardware Acceleration Dedicated for PQC and QKD

5G RAN is a time-sensitive, performance-driven network designed to serve users and other RAN components with low latency and high throughput. To achieve this, operators often rely on hardware accelerators such as FPGAs or ASICs. These cards handle compute-intensive tasks like error correction, DSP, cryptographic processing, and routing. However, current cryptographic accelerators lack support for PQC algorithms. To maintain network performance, hardware-specific PQC implementations will be needed, as RAN connections are long-lived and depend heavily on asymmetric cryptography.

In parallel, integrating Quantum Key Distribution (QKD) [53] systems adds an extra layer of information-theoretic protection, offering provably unbreakable security for network and critical interfaces. QKD can distribute Pre-Shared Keys (such as PPKs, discussed earlier) out-of-band between communication entities, enabling symmetric-only, air-gapped networks and reducing reliance on PQC for key exchange.

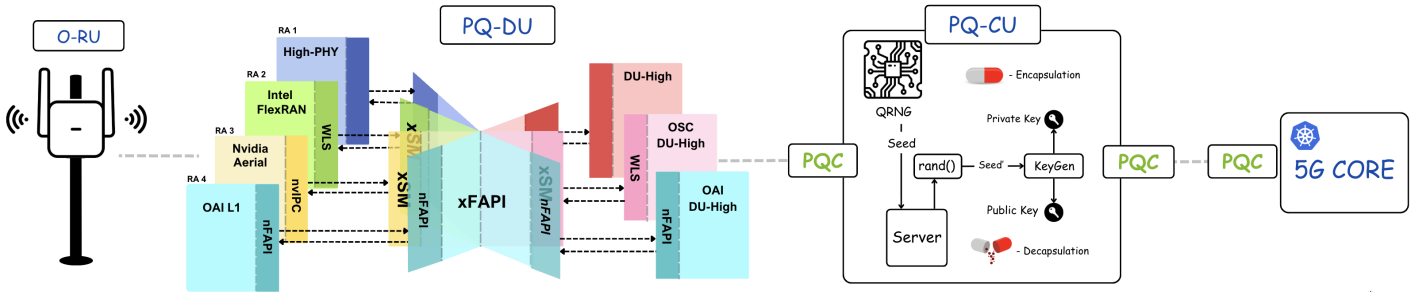

Figure 18: PQC-Enhanced xFAPI Architecture — illustrating secure interoperability between multi-vendor RUs and DUs through PQ extensions for SCTP and MAC Layers

7.4 Extension to Radio Interfaces, MACsec, and M-Plane

Early post-quantum migration efforts focused mainly on key exchange to mitigate HNDL attacks. As quantum computing advances, authentication mechanisms must also evolve to defend against "Trust Now, Forge Later" threats. Accordingly, upgrades have been introduced at the control plane and other key layers of the RAN stack. Future work will extend PQC to MACsec for Ethernet-based fronthaul links and to M-Plane communications between RUs and SMO/O-DU components through PQ-mTLS and PQ-SSH, while exploring methods to implement these enhancements at the RU level.

These extensions aim to deliver comprehensive, end-to-end quantum resilience across both wired and wireless interfaces, while remaining aligned with existing IEEE authentication/confidentiality and O-RAN security standards.

7.5 PQ Blockchain RAN (B-RAN)

Inspired by recent work on quantum-secure blockchain architectures [54] in 5G RAN, we see a clear path to extending Q-RAN into a decentralized, blockchain-backed RAN system—B-RAN. This would allow RAN components and IoT devices to securely authenticate and exchange data using a distributed trust model. Post-Quantum secure identities could be anchored to the blockchain, and smart contracts could automate key operations like credential rotation, device revocation, or audit logging. As more edge and IoT devices start supporting post-quantum cryptography, it become necessary to secure these endpoints against future threats.

8 Conclusion

This paper introduced Q-RAN, a practical framework for securing Open RAN architectures against emerging quantum computing threats by systematically integrating post-quantum cryptography (PQC). We discussed the challenges of replacing quantum-vulnerable primitives in key telecommunications security protocols—including mTLS, DTLS, IPsec, and OAuth 2.0—with NIST-standardized ML-KEM and ML-DSA algorithms. The proposed hybrid PQC model provides immediate protection against both active and passive quantum adversaries while supporting a smoother transition from classical systems.

Our analysis shows that lattice-based PQC algorithms can meet the latency and throughput demands of disaggregated 5G infrastructures, and hardware acceleration and optimized implementations would greatly help in minimizing computational overhead.

Q-RAN mitigates the "Harvest Now, Decrypt Later" threat by enabling quantum-safe encryption and authentication across O-RAN interfaces—from fronthaul and midhaul to management and control planes. The framework integrates quantum-generated entropy through QRNGs and designates the Service Management and Orchestration (SMO) layer as a unified trust anchor, hosting the Post-Quantum Certificate Authority (PQ-CA) and PQ-OAuth 2.0 service to ensure end-to-end confidentiality and integrity across certificate chains.

Rolling out Q-RAN in real deployments will require tight collaboration between network operators, equipment vendors, and standards bodies like the O-RAN Alliance, 3GPP SA3 [55], and the IETF. Standardization gaps, inconsistent PQ support across stacks, and integration at the edge (such as at RUs) are still open problems. Extending PQC across all relevant interfaces—without breaking existing workflows—remains a key focus.

The migration roadmap we've outlined lays out a practical path forward. With quantum computing evolving fast, it's important to start adapting networks now using proven solutions like Q-RAN—not just to stay ahead, but to keep critical systems secure and reliable.

Acknowledgments

This work reflects the ongoing efforts of the **coRAN Labs** research team to advance quantum-safe technologies in next-generation telecom systems. We'd like to thank the **O-RAN Alliance** for shaping the open RAN landscape and driving key security specifications, and the **NIST** community for leading the standardization of post-quantum cryptography.

We also acknowledge the invaluable tools and support from the open-source ecosystem. The **Open Quantum Safe** project made it possible to experiment with real-world PQC stacks; the **strongSwan** team continues to push innovation in IKEv2 and IPsec; and the relevant **IETF** working groups have laid the groundwork for secure, post-quantum-ready Internet protocols.

Finally, a big thanks to the **OpenAirInterface 5G** community—its open platform has been central to testing, integration, and validation throughout our project.

References

[1] IETF, "Elliptic Curves for Security," RFC 7748, Jan. 2016.

[2] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[3] National Institute of Standards and Technology, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," NIST, Tech. Rep., Aug. 2024, https://www.nist.gov/.../nist-releases-first-3-finalized-post-quantum-encryption-standards.

[4] O-RAN Alliance, "O-RAN Architecture Description," O-RAN Alliance, Tech. Rep. O-RAN.WG1.O-RAN-Architecture-Description, Mar. 2024.

[5] ——, "O-RAN Security Protocols Specifications," O-RAN Alliance, Tech. Rep. O-RAN.WG11.Security-Protocols, 2024.

[6] IETF, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, May 2008.

[7] ——, "IP Encapsulating Security Payload (ESP)," RFC 4303, Dec. 2005.

[8] ——, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3," RFC 9147, Apr. 2022, https://datatracker.ietf.org/doc/html/rfc9147.

[9] ——, "The OAuth 2.0 Authorization Framework," RFC 6749, Oct. 2012, https://datatracker.ietf.org/doc/html/rfc6749.

[10] ——, "OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens," RFC 8705, Feb. 2020, https://datatracker.ietf.org/doc/html/rfc8705.

[11] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," NIST, Tech. Rep. FIPS 203, Aug. 2024.

[12] R. Avanzi *et al.*, "CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation," NIST PQC Submission, 2020.

[13] L. Ducas *et al.*, "CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation," NIST PQC Submission, 2020.

[14] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Algorithm Standard," NIST, Tech. Rep. FIPS 204, Aug. 2024.

[15] ——, "Security Requirements for Cryptographic Modules," NIST, Tech. Rep. FIPS 140-3, Mar. 2019, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf.

[16] ——, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)," NIST, Tech. Rep. NIST SP 800-90A Rev. 1, Jun. 2015, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf.

[17] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219.

[18] D. J. Bernstein and T. Lange, "On the Practical Cost of Grover's Algorithm," in *Fifth NIST PQC Standardization Conference*, Gaithersburg, MD, USA, 2024, https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/on-practical-cost-of-grover.pdf.

[19] National Institute of Standards and Technology, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," NIST, Tech. Rep. FIPS 202, Aug. 2015, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf.

[20] P. Otero-García, A. Fernández-Vilás, and M. Fernández-Veiga, "Introducing post-quantum algorithms in open ran interfaces," *arXiv preprint arXiv:2501.10060v1*, 2025, available online.

[21] O-RAN Alliance, "O-RAN Security Focus Group: Applying Zero Trust Principles," White Paper, 2023.

[22] IETF, "Datagram Transport Layer Security (DTLS) Encapsulation of SCTP Packets," RFC 8261, Nov. 2017, https://datatracker.ietf.org/doc/html/rfc8261.

[23] ——, "Automatic Certificate Management Environment (ACME)," RFC 8555, Mar. 2019, https://datatracker.ietf.org/doc/html/rfc8555.

[24] OpenAirInterface Project, "OpenAirInterface 5G RAN Project Documentation," https://gitlab.eurecom.fr/oai/openairinterface5g, 2024, open-Source 5G RAN Implementation under OAI Alliance.

[25] Open Quantum Safe Project, "liboqs: C Library for Quantum-Resistant Cryptographic Algorithms," https://github.com/open-quantum-safe/liboqs, 2024.

[26] OpenSSL Project, "OpenSSL: Cryptography and SSL/TLS Toolkit," https://www.openssl.org, 2024, version 3.x Documentation and Source Repository.

[27] strongSwan Project, "Post-Quantum Cryptography Support Documentation in Strongswan," https://docs.strongswan.org/docs/latest/config/proposals.html, 2024.

[28] wolfSSL Inc., "wolfSSL Embedded SSL/TLS Library," https://www.wolfssl.com, 2024, lightweight TLS/DTLS and Cryptography Library for Embedded Systems.

[29] NVIDIA Corporation, "NVIDIA cuPQC," https://developer.nvidia.com/cupqc, 2025, an SDK for accelerating PQC primitives on GPUs.

[30] IETF Network Working Group, "Datagram Transport Layer Security (DTLS) 1.3 for Stream Control Transmission Protocol (SCTP)," Internet-Draft draft-tuexen-tsvwg-rfc6083-bis-04, work in progress, 2024, https://www.ietf.org/archive/id/draft-tuexen-tsvwg-rfc6083-bis-04.html.

[31] NVIDIA Corporation, "NVIDIA DOCA SDK and Libraries: Data-Centric Infrastructure Programming Framework," https://docs.nvidia.com/doca/sdk/doca+libraries/index.html, 2024, official NVIDIA DOCA Documentation and Developer Resources.

[32] IETF, "Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 7296, Oct. 2014, https://datatracker.ietf.org/doc/html/rfc7296.

[33] ——, "Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation," RFC 7383, Nov. 2014, https://datatracker.ietf.org/doc/html/rfc7383.

[34] ——, "Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 9242, May 2022.

[35] D. McGrew, T. Shrimpton, and K. G. Paterson, "Practical Challenges with AES-GCM: Randomness, Performance, and Security," in

Third NIST Workshop on Block Cipher Modes of Operation, Gaithersburg, MD, USA, 2023, https://csrc.nist.gov/.../third-workshop-on-block-cipher-modes-of-operation/documents/accepted-papers/PracticalChallengeswithAES-GCM.pdf.

[36] IETF CFRG Working Group, "Limits on Authenticated Encryption with Associated Data (AEAD) Algorithms," Internet-Draft draft-irtf-cfrg-aead-limits-01, work in progress, 2023, https://www.ietf.org/archive/id/draft-irtf-cfrg-aead-limits-01.html.

[37] M. Sosnowski, F. Wiedner, E. Hauser, L. Steger, D. Schoinianakis, S. Gallenmüller, and G. Carle, "The performance of post-quantum tls 1.3," in *Companion of the 19th International Conference on emerging Networking EXperiments and Technologies (CoNEXT Companion '23)*. New York, NY, USA: ACM, 2023, pp. 1–9. [Online]. Available: https://doi.org/10.1145/3624354.3630585

[38] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Post-quantum authentication in tls 1.3: A performance study," 2020, accessed: 2025-10-19. [Online]. Available: https://eprint.iacr.org/2020/071.pdf

[39] IETF, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018, https://datatracker.ietf.org/doc/html/rfc8446.

[40] S. Fluhrer, "Post-Quantum TLS: A Hybrid Approach," IACR Cryptology ePrint Archive, Tech. Rep. 2018/063, 2018, https://eprint.iacr.org/2018/063.pdf.

[41] IETF, "The Extended Master Secret Extension for TLS," RFC 8879, Jan. 2021, https://www.rfc-editor.org/rfc/rfc8879.html.

[42] ——, "IP Fragmentation Considered Fragile," RFC 8900, Sep. 2020, https://datatracker.ietf.org/doc/html/rfc8900.

[43] ——, "X-Wing: General-Purpose Hybrid Post-Quantum KEM," Internet-Draft draft-connolly-cfrg-xwing-kem-02, work in progress, 2024, https://datatracker.ietf.org/doc/html/draft-connolly-cfrg-xwing-kem-02.

[44] IETF LAMPS Working Group, "Composite Certificates and Certification Requests," Internet-Draft draft-ounsworth-lamps-composite-certs-03, work in progress, 2024, https://datatracker.ietf.org/doc/html/draft-ounsworth-lamps-composite-certs-03.

[45] IETF TLS Working Group, "Hybrid ECDHE and ML-KEM Key Exchange for TLS 1.3," Internet-Draft draft-tls-westerbaan-ecdhe-mlkem-03, work in progress, 2024, https://datatracker.ietf.org/doc/html/draft-tls-westerbaan-ecdhe-mlkem-03.

[46] IETF LAMPS Working Group, "Composite Signatures Combining ML-DSA and Classical Algorithms," Internet-Draft draft-ounsworth-lamps-composite-mldsa-01, work in progress, 2024, https://datatracker.ietf.org/doc/html/draft-ounsworth-lamps-composite-mldsa-01.

[47] IETF, "Use of ML-DSA in TLS and DTLS," Internet-Draft draft-ietf-tls-mldsa-00, work in progress, 2024, https://datatracker.ietf.org/doc/html/draft-ietf-tls-mldsa-00.

[48] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology (NIST), Special Publication 800-207, 2020, https://csrc.nist.gov/pubs/sp/800/207/final.

[49] IETF, "JSON Web Key (JWK)," RFC 7517, May 2015, https://datatracker.ietf.org/doc/html/rfc7517.

[50] coRAN Labs, "xFAPI: The Future of OpenRAN," https://github.com/coranlabs/xFAPI, 2024, making the OpenRAN Truly Open.

[51] O-RAN Alliance, "O-RAN Software," http://o-ran.org/software.

[52] coRAN Labs, "Q-RAN: Quantum Secure O-RAN," https://www.linkedin.com/feed/update/urn:li:activity:7313457657019805712, 2025, post-Quantum Upgradation for Open RAN.

[53] ETSI, "Quantum Key Distribution (QKD); Application Interface," Tech. Rep. GS QKD 004, 2020.

[54] T. Group, "Engineering quantum-resilient security for next-gen networks," https://www.thalesgroup.com/en/news-centre/insights/public-security/civil-identity/engineering-quantum-resilient-security-next-gen, 2025, accessed: 2025-10-19.

[55] 3GPP, "Technical Report on Study on Security Aspects of Quantum Computing," 3GPP, Tech. Rep. TR 33.850, 2024, release 18.