NextG Security for Mission Critical Communication

Arupjyoti Bhuyan[1], William Edwards[2], Junaid Islam[3], and Jason Hilker[4]

[1] Idaho National Laboratory, Idaho Falls, Idaho, USA arupjyoti.bhuyan@inl.gov
[2] US Navy Retired, Kansas City, Kansas, USA will.edwards@deepbluekrypto.com
[3] Zero Trust User Group, San Jose, Califirnia, USA junaid@ooda.com
[4] US Marine Retired, Omaha, Nebraska, USA jason@smbgservices.com

Abstract. NextG or 6G will continue the transformation started by 5G in cellular communications worldwide. 6G seeks to improve key performance indicators (KPI) such as data rates, latency, and reliability significantly along with pervasive use of AI/ML as well as adding sensing capability to the 6G networks. While improving and extending the capabilities of cellular networks, 6G will introduce new security issues that have to be addressed adequately. At the same time, existing and new security procedures will have to be resilient to quantum computing enabled adversarial attacks. After summarizing the current and emerging security land-scape of cellular networks, this paper discusses the Post Quantum Cryptography (PQC) algorithms published by the U.S. National Institute of Standards and Technology (NIST). Next it analyzes the challenges and approaches for incorporating PQC in 5G and 6G followed. Using a specific user scenario for the advanced mobile system (AMS) with integration of ground and air based communication, the first step of securing the user data with PQC is presented. Specific challenges in this use case, including constraints in available resources at the end devices, limited bandwidth and dynamic nature of the RF channels, communication latency are considered. Use of AI agentic solutions with specific results are presented to illustrate a practical approach to making cellular communication resilient to Quantum enabled attacks.

Keywords: NextG · 6G · Post Quantum Cryptography (PQC).

1 Introduction

Although security for users of cellular connectivity has improved across generations, from 2G through 5G, some challenges still remain. Mission-critical use cases require authenticity, confidentiality, integrity, availability and reliability, along with resilience against adversarial attacks, with a higher level of security compared to consumer and commercial use cases. While each generation of cellular standards addresses some of the legacy vulnerabilities, it also introduces new attack surfaces with its enhancements. The security improvements introduced in 5G and new capabilities planned for 6G are discussed next.

1.1 5G Security

The 3GPP Service and System Aspects Working Group 3 (SA3), the standards body responsible for telecommunications security and privacy, introduced significant security improvements in the 5G specifications over 4G/LTE that included a shift from perimeter-based implicit trust in LTE toward mutually authenticated communication. The key security improvements are summarized below ([1], [2]).

Subscription Concealed Identifier (SUCI):International Mobile Subscriber Identity (IMSI) is now encrypted using the home network's public key, preventing IMSI catchers from harvesting permanent identifiers over the air.

User-plane integrity protection (UP-IP): This procedure to prevent data tampering is a critical security enhancement in 5G.

NF authorization with OAuth 2.0: Following the Zero Trust Architecture (ZTA), Network Functions (NF) in the 5G Core Network (5GC) need authorization to communicate and request service from another SF even though they are inside the same core network perimeter.

Service-Based Architecture (SBA) with mutual Transport Layer Security (mTLS) authentication: The 5GC NFs are also required to be authenticated for NF-NF communication.

Secure Roaming: a) A new SF called Secure Edge Protection Proxy (SEPP) safe-guards inter-network roaming signaling; b) subscriber authentication is performed directly in the home network. These improvements effectively address the well known SS7/Diameter roaming vulnerabilities.

Secondary authentication for specific network slices: A second layer of authentication can be added and customized for securing the data communication itself between the user and the terminating data network utilizing the extensible authentication protocol (EAP).

While these improvements have been specified by 3GPP, utilizing them effectively still requires the network operator to turn on optional procedures such as the user plane integrity protection and configure the relevant security keys e.g. for SUCI and security certificates e.g., for mutual TLS authentication.

1.2 New 6G Capabilities

Plans for 6G, the next 3GPP standards for cellular networks worldwide, are well underway while 5G deployments have yet to deliver their transformation capabilities of massive Machine Type Communications (mMTC) and ultra reliable low latency. 3GPP releases for 5G capabilities will end with Rel-20 [3] which contains two parallel tracks, 5G-Advanced and 6G Study Item. Rel-20 is planned for completion in June 2027, while the timeline for Rel-21, the first 6G standards, will be finalized in June 2026. The 6G Service requirements study TR22.870 [4] has been approved in March, 2026. The key areas listed below show how 6G intends to add innovative and transformative capabilities to cellular networks with an ambitious plan.

Key Performance Indicators (KPI) 6G targets 20 times faster peak downlink data rate of 1 Tbps from 20 Gbps, 10 times faster user experienced downlink data rate of 1 Gbps from 100 Mbps, 10 times reduced latency of 0.1 msec from 1 msec along with 100 times increase in reliability of 99.99999 % from 99.999 %, 100 times improved positioning accuracy of 1-10 cm from 1-20 m, and 10 times higher connection density.

Native AI While 5G integrates AI/ML for monitoring network operations and detecting anomalies etc., use of AI is projected to become pervasive in 6G networks with e.g., AI-for-physical layer, digital twins for real-time optimization and network AI agents for dynamic optimization of 3GPP services.

Integrated Sensing and Communication (ISAC) 6G plans to add radar like sensing capability to the cellular network that is designed so far for communication. While connected devices can be located by the networks, with ISAC, detection and localization of objects not connected to the network will be possible. ISAC fundamentally redefines the role of wireless networks, extending them from data transport infrastructure to environment-aware systems.

Native Integration of Non-Terrestrial Network (NTN) 6G aims to provide ubiquitous connectivity with seamless integration of LEO, MEO, GEO (low, medium, geostationary earth orbit) satellite, HAP (high altitude platform), as well as drone/UAS with ground based radio links for a unified radio access layer.

1.3 6G Security Study

The 3GPP SA3 working group has started "Study on Security for the 6G system" in Release 20 draft TR 33.801-01 [5]. Following are the guiding design principles. 1) **Security-by-design**: Security is embedded as a fundamental requirement during architecture design, not bolted on later. 2) **S**elective continuity: Determining what security mechanisms carry over from 5G, what must be enhanced, and where new security procedures are essential. 3) **Q**uantum-safe from inception: Unlike 5G, where PQC is a retrofit challenge, 6G specifications are intended to incorporate quantum-safe cryptographic primitives from the first normative release. 4) **Zero Trust Architecture (ZTA) evolution**: 6G extends continuous, context-aware, per-transaction verification across all network domains, building on 5G ZTA studies (TR 33.894, TR 33.794). 5)**AI** security: AI governance frameworks, adversarial ML protections, and AI lifecycle security are integral to the architecture.

The security study in 33.801-01 is structured around seven primary areas that are summarized below.

Security Architecture This addresses security and privacy aspects for the overall 6G system architecture with focus on Zero Trust Architecture (ZTA) for 6G, Post-Quantum Cryptography (PQC) and Cryptographic agility, AI security governance framework, Edge and cloud trust boundaries and Cryptographic agility.

RAN Security This focuses on AI/ML model security in the RAN, ISAC security and privacy, Physical Layer Security (PLS), NTN and drone-BS security and Open RAN security.

UE to Core Network Security This area covers Identity privacy evolution (post-SUCI), Authentication protocol agility, NTN UE handover security, and Device onboarding at scale.

Core Network, Interconnect and Roaming Security This area focuses on SBA security evolution, Security Edge Protection Proxy (SEPP) enhancements for 6G roaming, Interconnect attack surface including legacy vulnerabilities of SS7 & Diameter), End-to-end protection in multi-domain NTN.

Subscription Authentication and Authorization Focuses on Post-quantum Authentication and Key Agreement (AKA) protocol design, AI-assisted authentication anomaly detection, Credential agility and fleet management and Secondary and application-layer authorization.

Network Exposure Security Key focus areas are API gateway protection, Unified exposure framework, ISAC sensing data exposure and Third-party access controls under ZTA.

Data Collection for Security Monitoring Focuses on Real-time, network-wide security telemetry, AI-driven threat detection, Network Data Analytics Function (NWDAF) evolution for 6G, Distributed ISAC sensing data security, and Privacy-preserving monitoring.

A foundational task is the development of a preliminary 6G attacker model that provides the common threat framing referenced by all seven security study areas. This model is currently being developed and represents one of the earliest deliverables of the SA3 6G study. While the model remains in formation, its key dimensions reflect the substantially expanded attack surface of 6G relative to 5G driven by AI/ML integration, ISAC sensing data, NTN expansion. Quantum adversqaries, Autonomous network functions, and Edge compute.

est of this paper is organized as follows. Section 2 describes the proposed ZAP framework. Section 3 provides an example ZAP workflow with this framework. Section 4 addresses key areas that ZAP has to consider as it evolves in the future. Finally section 5 presents the conclusions of this paper.

2 Post Quantum Cryptography (PQC)

The U.S. National Institute of Standards and Technology (NIST) is responsible for setting federal cryptographic standards under the Federal Information Security Modernization Act (FISMA). In 2016, NIST launched the Post-Quantum Cryptography (PQC) Standardization Project to "Select and standardize one or more quantum-resistant public-key cryptographic algorithms" which can remain interoperable, efficient, and secure well into the 2030s [6].

Module-Lattice–based Digital Signature Algorithm (ML-DSA), Dilithium, is the primary NIST-selected post-quantum digital signature (DS) standard. Fast Fourier Lattice-based Compact Signatures over NTRU (FALCON) is another lattice-based post-quantum digital signature algorithm which has smaller signature size; but is computationally complex. Stateless Practical Hash-based INcredibly Compact Signature+ (SPHINCS+) is another secondary post-quantum DS algorithm selected by NIST.

Module-Lattice–based Key Encapsulation Mechanism (ML-KEM), Kyber, is the NIST-selected post-quantum key establishment standard (formerly known as CRYSTALS Kyber). Code based Classic McEliece is the secondary postquantum KEM selected by NIST but not standardized yet.

NIST has created an implementation and migration framework that includes the following components: 1) New Federal Information Processing (FIPS) Standards: They define PQC algorithm specs, FIPS 203–205, and testing requirements ([7], [8], [9], [10]); 2) NIST SP 800-series which provide guidance for cryptographic modules and key management incorporating PQC ([11], [12]); 3) NIST PQC Migration Guidance (SP 800-208 [13], 800-57 updates [14]) with recommended hybrid and cryp-to-agile transition strategies; 4) Algorithm Profiles which define performance tiers, e.g., ML-KEM-512, 768, 1024, for different risk and performance environments [15]; 5) Interoperability Testing for Collaboration with Open Quantum Safe, IETF, and vendors to ensure consistent API and parameter sets.

2.1 ML-DSA

The Dilithium public key is the pair (ρ, t), where $\mathbf{t} = \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$. Here, $\mathbf{A}$ is a $k \times l$ matrix where each entry is a polynomial in $\mathbb{Z}_q[X]/(X^n + 1)$ with $n = 256$, regenerated deterministically from seed ρ, $\mathbf{s}_1$ is a secret vector of small polynomials, and $\mathbf{s}_2$ is a second secret vector of small polynomials that serves as the error term, invoking MLWE hardness. Both $\mathbf{s}_1$ and $\mathbf{s}_2$ are retained in the private key and used during signing. NIST specifies three parameter sets to balance security and performance.The three parameter sets differ primarily in

module rank k (2, 3, and 4 respectively), which directly governs the size of $\mathbf{A}$, $\mathbf{s}_1$, and $\mathbf{s}_2$, and consequently the public key, private key, and signature sizes.

ML-DSA-44 (Security Category 2) Offers a base level of security roughly equivalent to AES-128. It provides the fastest performance and is suitable for constrained environments including IoT and embedded systems. Public key size is 1312 bytes, private key size is 2528 bytes, and the signature size is 2420 bytes.

ML-DSA-65 (Security Category 3) Provides enhanced security roughly equivalent to AES-192. It strikes a balance between security and performance and is commonly recommended choice for most use cases. Public key size is 1952 bytes, private key size is 4032 bytes, and the signature size is 3309 bytes.

ML-DSA-87 (Security Category 5) Offers the highest level of security, roughly equivalent to AES-256. It is ideal for protecting highly sensitive information where maximum security is the priority despite higher computational overhead. Public key size is 2592 bytes, private key size is 4896 bytes, and the signature size is 4595 bytes.

2.2 Falcon

Fast Fourier Lattice-based Compact Signatures over NTRU (FALCON) is in the process of being specified as FIPS-206 [16]. NTRU is a family of lattice-based cryptographic constructions built on arithmetic over polynomial rings. FALCON-512 produces signatures of 666 bytes compared to ML-DSA-44's 2400 bytes — making it attractive for bandwidth and memory constrained environments such as UAS and IoT edge devices. However, FALCON requires Floating-point arithmetic and Gaussian sampling over lattices, making it computationally complex and difficult to implement.

2.3 SPHINCS+

Stateless Hash-Based Post-Quantum Signature (SPHINCS+) is a stateless, hash-based digital signature scheme standardized as SLH-DSA (Stateless Hash-Based Digital Signature Algorithm) in FIPS 205 [10]. It is a mathematically conservative alternative to lattice-based signatures. Its security relies on cryptographic hash functions rather than algebraic structures, making it highly robust against both classical and quantum attacks with minimal underlying assumptions. Unlike hash-based schemes, SPHINCS+ does not require maintaining signing state, which simplifies key management and avoids reuse risks. However, this strong security comes at a cost of significantly larger signatures, 7 KB to 30 KB, and slower performance compared to lattice-based schemes. As a result, it is best suited for applications where long-term security and cryptographic conservatism are essential, such as authenticating firmware updates, root certificates, or mission-critical command authorization.

2.4 ML-KEM

The Kyber public key is the pair (ρ, t), where $t = \mathbf{As} + \mathbf{e}$. $\mathbf{A}$ is a $k \times k$ matrix where each entry is a polynomial in $\mathbb{Z}_q[X]/(X^n + 1)$ with n=256, regenerated deterministically from the public seed ρ, $\mathbf{s}$ is the secret key vector of small polynomials, $\mathbf{e}$ is a vector of small random error polynomials added to masks. NIST specifies three parameter sets to balance security and performance for ML-KEM as well. As in Dilithium, the three parameter sets for Kyber differ primarily in module rank k (2, 3, and 4 respectively), which directly governs the size of $\mathbf{A}$, $\mathbf{s}$, and $\mathbf{t}$, and consequently the public key, ciphertext, and private key sizes.

ML-KEM-512 (Security Category 1) Offers a base level of security roughly equivalent to AES-128. It provides the fastest performance and targets constrained environments including IoT and embedded systems. Public key size is 800 bytes, ciphertext size is 768 bytes and the private key size is 1632 bytes.

ML-KEM-768 (Security Category 3) Provides enhanced security roughly equivalent to AES-192. It strikes a balance between security and performance, suitable for a wide range of applications. Public key size is 1184 bytes, ciphertext size is 1088 bytes and the private key size is 2400 bytes.

ML-KEM-1024 (Security Category 5) Offers the highest level of security, roughly equivalent to AES-256. It is ideal for protecting highly sensitive information where maximum security is the priority. Public key size is 1568 bytes, ciphertext size is also 1568 bytes and the private key size is 3168 bytes.

2.5 Key differences between ML-DSA and ML-KEM

The main differences between ML-DSA for digital signature and ML-KEM for key encapsulation are summarised in the following.

Underlying Problem Dilithium's security against signature forgery attacks relies on both Module Learning with Errors (MLWE) and the Module Short Integer Solution (MSIS) problem. Kyber's security against session key recovery attacks relies on the hardness of the MLWE problem, hardened via the Fujisaki-Okamoto trans-form.

Polynomial Ring Both operate over the polynomial ring Zq[X]/(Xn+1) with n=256, enabling ef-ficient computation via the Number Theoretic Transform (NTT), but with dif-ferent moduli: Kyber employs a 12-bit prime modulus (q=3329) suited to key encapsulation, while Dilithium uses a larger 23-bit prime (q=8380417) to support the arithmetic demands of signature generation.

Key Size Dilithium signatures are notably larger than Kyber ciphertexts at equivalent security levels. ML-DSA-65 produces 3,309-byte signatures versus ML-KEM-768's 1,088-byte ciphertext.

Others Other differences include 1) Dilithium starts with category 2 while Kyber starts with category 1. 2) The underlying matrix A is rectangular for Dilithium and square for Kyber. 3) Dilithium uses $\mathbf{s}_1$ and $\mathbf{s}_2$ while Kuber uses $\mathbf{s}$ and $\mathbf{e}$.

3 Applying PQC to 5G and 6G

The standardization of post-quantum cryptographic algorithms by NIST has initiated urgent activity for PQC integration across the telecommunications sector. The deployment horizon of cryptographically relevant quantum computers (CRQCs), estimated by NSA and others at 10–15 years, intersects dangerously with the long operational lifespans of cellular infrastructure and the sensitivity of data transiting these networks. The "harvest now, decrypt later" (HNDL) threat is particularly acute for telecom networks, where adversaries may already be archiving encrypted traffic for future decryption. Long-lived subscriber credentials, network function certificates, and inter-operator signaling data are all at risk and motivates immediate PQC migration. The NSA's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) [17] mandates transition to PQC algorithms for national security systems by 2030. NSA's CNSA 2.0 advisory directly influences the adoption of PQC in 5G and emerging 6G networks, particularly in defense, government, and mission-critical communication infrastructures.

3.1 Standards

The 3GPP Security Working Group SA3 has been evaluating PQC integration since NIST's draft FIPS publications. 3GPP Release 18 and Release 19 contain working items addressing quantum-safe cryptography for the 5G Core (5GC) and air interface. The primary focus areas include: 1) Replacement of Elliptic Curve Integrated Encryption Scheme (ECIES) in the SUCI/SUPI subscriber identity protection mechanism with ML-KEM or hybrid X25519/ML-KEM constructions; 2) PQC-enhanced authentication frameworks as alternatives to or extensions of 5G-AKA; 3) Quantum-safe certificate management for network function authentication within the service-based architecture (SBA).

Unlike 5G, 6G standardization provides an opportunity to incorporate quantum resistance and to be PQC ready by design. The standards landscape for PQC in 6G is converging around a few key principles: 1) Cryptoagility is mandatory; 2) Hybrid PQC/classical is the transition model; 3) Transport-layer migration precedes native 6G security redesign; 4) Interoperability across ecosystems (IETF, ETSI, GSMA) is critical.

3GPP SA3 6G Activities Summary TR 33.703 (Release 20 Study) [32] is the central 3GPP document for PQC transition. Hybrid key exchange utilizing PQC with existing procedures without completely replacing them and identification of interfaces that are most vulnerable to harvest now decrypt later (HNDL) attack are the focus. SA3 is working security architecture evolution towards 6G in the following areas: a) Next generation of AKA beyond 5G-AKA and EAP-AKA'; b) Integration of PQC digital signatures and key encapsulation; c) PQC impact on the service based architecture (SBA), IPsec, Roaming Security. 3GPP SA3's emerging work for 6G identity shifts from a centralized, subscription-bound model in 5G toward a decentralized, credential-based, and zero-trust-based framework. This evolution introduces new dependencies on post-quantum secure signatures and raises open challenges in scalability, interoperability, and trust governance.

Relevant work in other standards 1) IETF: a) use of PQC algorithms in X.509 PKI, by enabling ML-KEM-based key establishment and ML-DSA-based signatures within certificates, certification revocation lists (CRLs), and related structures ([19], [20]) ; b) TLS 1.3 hybrid key exchange [21], c) IPsec with hybrid PQC [23]; 2) ETSI: Focus on migration strategies provide operation guidance for telecom deployment and influences device and SIM ecosystem; 3) GSMA: Its focus on roaming, interconnect security, and deployment guidelines contributes to real-world operator requirements ([24], [25], [26], [27], [28]).

3.2 Challenges

Applying PQC to the cellular networks, 5G now and 6G in the future, is a highly complex system wide problem. The 3GPP-specific work, TR 33.703, is still a Release 20 study and specifications are not yet available for implementing PQC in the cellular networks. The major challenging areas are listed below.

Architectural heterogeneity 5G uses a large set of security procedures across domains – AKA, TLS, HTTP/2, IPsec/IKE (Internet Key Exchange), JSON Object Signing and Encryption protcols -JOSE/JWS/JWE, Non Access Stratum (NAS), Packet Data Convergence Protocol (PDCP), and other interface-specific protections. Each of them has to be addressed separately for PQC integration.

Size of keys and cyphertext PQC algorithms use significantly larger keys and signatures than their classical counterparts which is challenging for their use in 3GPP air interface protocols where message sizes have to be specified tightly. ML-KEM-768 public keys are 1,184 bytes compared to 64 bytes for ECDH (Elliptic Curve Diffie-Hellman), and ML-DSA-65 signatures are around 3,309 bytes versus 64 bytes for ECDSA (Elliptic Curve Digital Signature Algorithm).

Redesign of identity and authentication The IMSI and the home network public key are physically provisioned onto SIM cards at manufacturing time. Using PQC will require re-provisioning or replacing of existing SIMs globally. Note that the eSIM/eUICC (Embedded Universal Integrated Circuit Card) is an important enabler of a manageable PQC migration path for subscriber identity protection.

Symmetric Vs. Asymmetric Keys The cellular authentication and key management e.g., 5G-AKA, is based on symmetric pre-shared keys. PQC establishes shared secrets over insecure channels using public keys and asymmetric key exchange. This creates a challenge for a natural insertion point for PQC into 5G-AKA.

Resource constrained cellular end devices Resource-constrained 5G and 6G devices, including IoT nodes and UAS/drones, face significant challenges in adopting PQC due to increased computational complexity, memory requirements, and energy consumption, in addition to communication overhead.

Dynamic RF channels The inherently dynamic nature of the RF interface presents a distinct set of challenges for PQC integration in cellular networks. Unlike wired environments where communication channels are assumed reliable, radio channels fluctuate continuously due to fading, shadowing, interference, and mobility.

3.3 Current approaches

The near term approach is hybrid migration inside existing security protocols rather than a redesign of cellular security protocols. There is work in progress in IETF on hybrid TLS design where multiple key exchange algorithms are combined so the resulting shared secret remains secure as long as one component remains unbroken ([21], [22], [29], [30]). A domain by domain integration of PQC into the cellular security procedures rather than the whole network has emerged as a practical approach. Network interface such as N32 for roaming are seen as high priority for PQC hardening. ATIS separates a first stage focused on HNDL-exposed interfaces from a later stage focused on signatures and authentication, and maps these priorities across Device/UE, RAN/Core, Core Network, and Interconnect Network [31].

Integrating PQC into 5G and emerging 6G systems is a comprehensive transformation of the trust infrastructure, including public key infrastructure (PKI), certificates, and application-layer security objects. While early efforts focused on replacing classical key exchange mechanisms (e.g., ECDHE) with post-quantum key encapsulation mechanisms (KEMs), recent guidance from standards bodies emphasizes that identity, authorization, and control-plane security must also transition to quantum-resistant primitives.

Equally important is the need for coexistence between classical and PQC-based trust anchors during a phased transition period. Both GSMA and ATIS emphasize that telecom operators must support parallel validation of legacy (RSA/ECDSA) and PQC (e.g., ML-DSA) certificates, along with cross-signing strategies and hybrid trust chains, to maintain interoperability across multi-operator environments ([24], [31]). Beyond PKI, PQC migration must extend to application-layer security objects, particularly in the 5G SBA. Core network functions rely heavily on signed artifacts such as JSON Web Signatures (JWS), JSON Web Tokens (JWT), and OAuth-based authorization tokens for inter-service authentication and authorization. These mechanisms currently depend on classical digital signatures and are therefore vulnerable to quantum attacks. ATIS recommends that these control-plane security objects adopt PQC-compliant signature schemes, ensuring that identity assertions and authorization decisions remain trustworthy in a post-quantum context [31].

This approach must be tightly coupled with transport layer migration, rather than treated independently. Secure communication protocols such as TLS (including mutual TLS) and IKE/IPsec depend on both key establishment and certificate based authentication. As a result, a consistent PQC deployment requires the combined use of ML-KEM for session key establishment and ML-DSA for certificate validation and message signing. Hybrid deployment models, combining classical and PQC algorithms, are widely recommended during the transition phase to ensure backward compatibility and resilience against both classical and quantum adversaries ([24], [31]).

In summary, current industry and standards efforts converge on a staged, multi-layered migration strategy in which PQC is introduced across PKI, transport protocols, and application-layer security mechanisms. This approach recognizes that securing future 5G and 6G networks requires not only protecting data in transit but also ensuring the long-term integrity and authenticity of the trust relationships that underpin network operation.

4 NextG use case

In this section, we consider a specific use case to focus our discussions of PQC integration into the NextG. Using the phased approach of PQC integration, we discuss how PQC can be applied to secure the data transfer for this scenario instead of applying it to each phase of the cellular connection.

4.1 Drone Operation with Integrated Ground & Space Coverage

Let us consider secure drone communication with its ground control station (GCS) as a representative Advanced Mobile System (AMS) (see figure 1). The primary wireless link is provided by a 5G cellular network with RF coverage from the ground. When a drone swarm is used, Wi-Fi links enable intra-swarm communication among the drones. When the drone swarm is in an area where ground based RF coverage is not available, it connects to a LEO satellite which

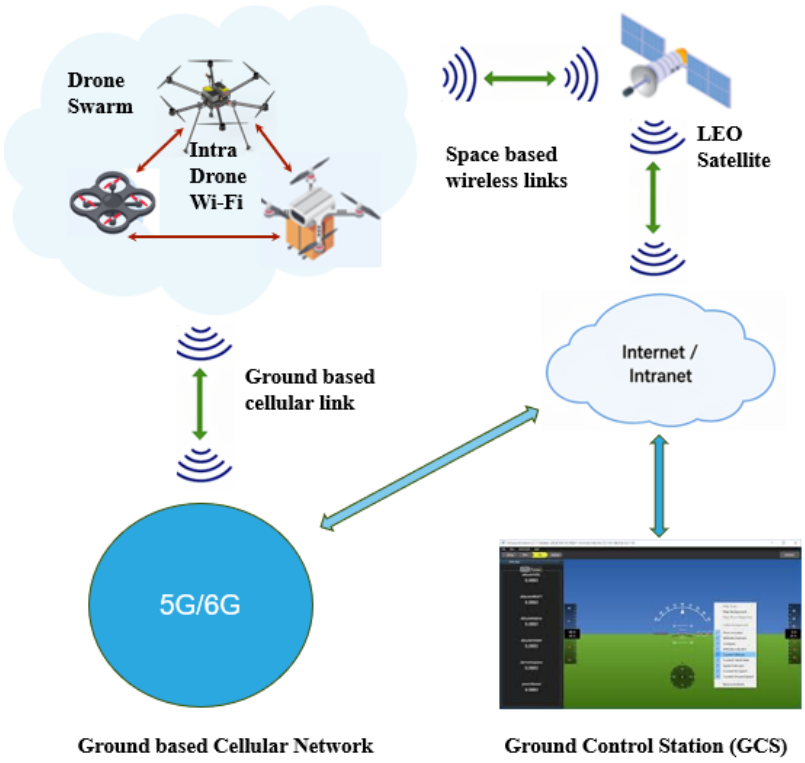


Fig. 1. An example of AMS composed of drones and satellite along with ground based wireless network and other AMS components including the drone GCS.

provides a transport pipe either to a ground based 5G base station or directly to the GCS through the LEO's ground network.

Utilizing NIST's PQC portfolio in this AMS use case presents several challenges including constraints on computing resources and communication bandwidth as well as dynamic RF channel which the AMS wireless links use. 1) Computational limitation: PQC adds overheads for CPU and RAM that challenge the requirements for SWaP (Size-Weight-Power) e.g., for UAS and SATCOM. 2) Key and signature size: Much larger PQC keys and signatures challenge the communication bandwidth e.g., for SATCOM. 3) Communication latency: Delayed PQC handshakes required for mission start is a challenge for low latency requirements for advanced mobility systems in general. 4) Communication link changes: Transition of the communication links between networks requires reconfiguring PQC components. Vulnerability to cyber-attacks: The open nature of wireless communications enables adversaries to easily monitor communications over RF and launch attacks not only on the RF inter-face over the air; but also on any part of the end to end connection.

To apply PQC to the data exchange between the drone/UAS and its ground control system, the following tasks have to be completed. 1) Determination of available resources and RF channel characteristics: This task has to compute resources such as CPU cycles and usable RAM at the drone/UAS. It has to also determine the communication capability such as available data throughput and capacity based on the current RF channel conditions. 2) PQC selection with policy enforcement: The optimal PQC algorithm has to be selected based on available bandwidth, throughput, latency, and compute resources. 3) Key and certificate generation: The PQC certificates and key pairs (e.g., Kyber/Dilithium) have to be generated and configured and all certificate and key transactions have to be logged. 4) Monitoring of wireless connectivity: As RF conditions change over time or an attack is detected, PQC has to be reconfigured as necessary.

4.2 PQC selection with an AI Agentic Solution

An agentic AI framework offers a compelling approach for PQC algorithm selection in resource-constrained 5G/6G edge devices, such as drones and IoT nodes, operating over highly variable RF channels. Unlike static or rule-based methods that rely on predefined thresholds (e.g., signal quality, latency, or battery level), an agentic system can continuously learn and adapt to multidimensional context, including channel conditions, mission priorities, device energy state, and adversarial risk. This enables real-time selection or switching between PQC schemes (e.g., ML-KEM parameter sets or hybrid modes) to optimize trade-offs between security strength, computational overhead, and communication efficiency.

In addition, in the presence of active threats such as RF jamming, spoofing, or selective interference, a distributed set of AI agents - spanning the end device, base station (gNB), and 5G core—can collaboratively build a richer, network-wide situational awareness that goes well beyond local signal metrics. By correlating observations across neighboring cells, handover patterns, interference signatures, and control-plane anomalies, these agents can distinguish between benign channel degradation and adversarial activity. A coordinating agent can then trigger adaptive responses such as switching to more robust PQC parameter sets, enabling hybrid or redundant key establishment paths, prioritizing low-latency secure re-keying, or even orchestrating mobility decisions to less-contested cells. This coordinated, threat-aware adaptation provides resilience that any rule-based systems are not likely to achieve, since static rules typically lack the ability to fuse multi-layer intelligence or respond dynamically to evolving attack strategies.

4.3 PQC Selection Results

This section presents the results of PQC selection for a selected set of simulated scenarios of variable RF channel conditions and resource constraints at the drone with an agentic solution described in the appendix (see section A).

In the following scenarios, channel conditions range from very strong (SNR $\geq$ 5 dB) to very poor SNR of -5 dB. Two cases of compute resources at the drone are considered in these scenarios. The Constrained tier (128 MB RAM, 70% CPU) models a resource-limited embedded processor under moderate load. The Critical tier (64 MB RAM, 90% CPU) represents a severely resource-constrained micro-controller processor operating near capacity, as encountered during battery depletion, thermal throttling, or concurrent processing. Note that the CPU load denotes the proportion of total processing capacity already consumed by non-PQC tasks, a higher load leaves less headroom for PQC operations.

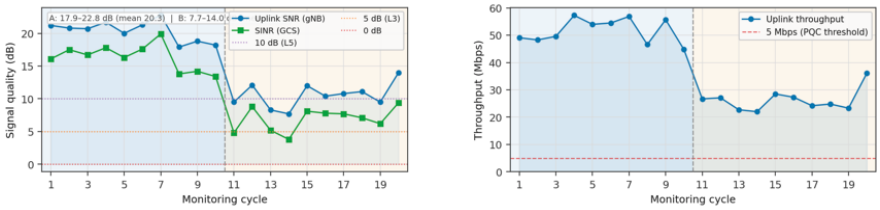
Scenario 1 : In this scenario, the drone's compute resources are "Constrained" and the uplink RF channel at the drone remains strong. SNR is approximately 20 dB during the first 10 monitoring cycle, dropping to approximately 10 dB for the next 10 cycles (see fig. 2(a)). The PQC algorithms ML-KEM-768 and ML-DSA-65 are consistently selected for the entire duration. The PQC selection for this scenario is driven by the compute resources even though the RF channel is capable of high data throughput to support higher levels of the PQC algorithms e.g., ML-KEM-1024 and ML-DSA-87.

Scenario 2 : In this scenario, the drone's compute resources are still "Constrained" but with the uplink RF channel not as strong as in scenario 1 (see fig. 2(b)). With the throughput reducing to below 5 Mbps, FALCON-512's 666-byte signature is selected along with ML-KEM-512 as the lowest-bandwidth options. The PQC selection for this scenario is driven by the RF channel conditions at the drone.

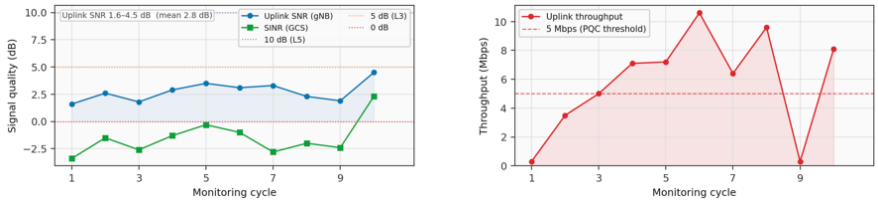
Scenario 3 : Keeping the drone's compute resources as "Constrained", PQC is now determined when the RF channel deteriorates further resulting in very low throughput (see fig. 2(c)). The selected PQC algorithms remain the same with ML-KEM-512 and FALCON-512 as in the previous scenario of low throughput.

Scenario 4 : In this scenario, the drone's compute resources are "Critical" or severely constrained. Although the RF channel condition varies over the monitoring cycles, the channel remains strong resulting in high throughput for most of the time (see fig. 2(d)).

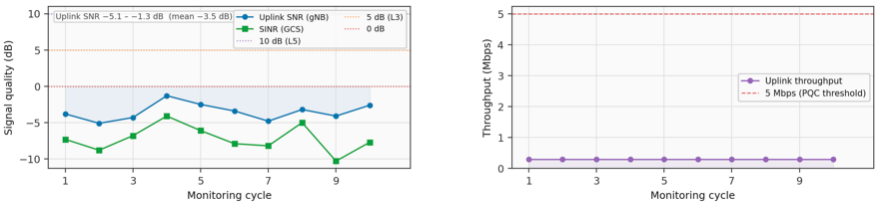
Scenario 5 : In this final scenario, the drone's compute resources are still "Critical" or severely constrained. Along with it, the RF channel is also the weakest ((see fig. 2(e)). This combination forces the selection of SPHINCS+-SHA2-128s for Digital Signature along with ML-KEM-512 for key encapsulation.



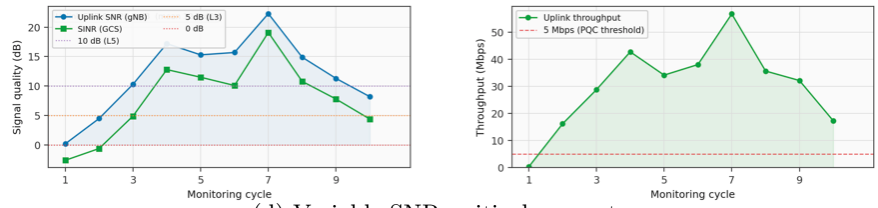
(a) High SNR, constrained compute



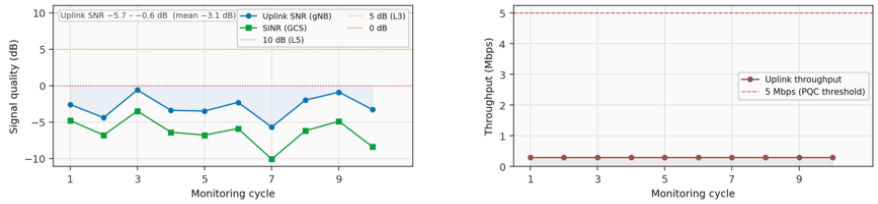
(b) Low SNR, constrained compute



(c) Very low SNR, constrained compute



(d) Variable SNR, critical compute



(e) Very poor SNR, critical compute

Fig. 2. Simulation results for constrained and critical compute scenarios. Each subfigure shows SNR (left) and data throughput at the drone (right).

The PQC selection results for the simulated scenarios are summarized in Table 1.

Table 1. Summary of PQC Selection.

Scenario	Selected KEM	Selected DS	Rationale
Scenario 1: constrained compute, high throughput	ML-KEM-768	ML-DSA-65	Category 3 algorithms are selected due to compute constraints.
Scenario 2: constrained compute, medium throughput	ML-KEM-512	FALCON-512	Smaller signatures are selected to reduce throughput overhead.
Scenario 3: constrained compute, low throughput	ML-KEM-512	FALCON-512	The same selection is retained under further throughput reduction.
Scenario 4: critical compute, high throughput	ML-KEM-512	ML-DSA-44	Lowest-level ML-KEM and ML-DSA options minimize CPU and memory footprint.
Scenario 5: critical compute, low throughput	ML-KEM-512	SPHINCS+	Hash-based signatures provide a fallback when compute resources and RF conditions are severely constrained.

Acknowledgments. We acknowledge Prof. Syed Hussain and his Ph.D. student Yilu Ding in Pennsylvania State University and Thanh Tong for their contributions to our work with NIST PQC algorithms.

Page limit is 18 pages excluding references and appendices, and a total page limit of 24 pages (including references and appendices).

A Agentic Solution

We present the agentic simulation used in this paper.

A.1 AI Agentic Architecture

Figure 3 shows the architecture diagram of a representative AI agentic solution that can be applied to the AMS used case for effectively select the appropriate PQC algorithms under changing operating conditions.

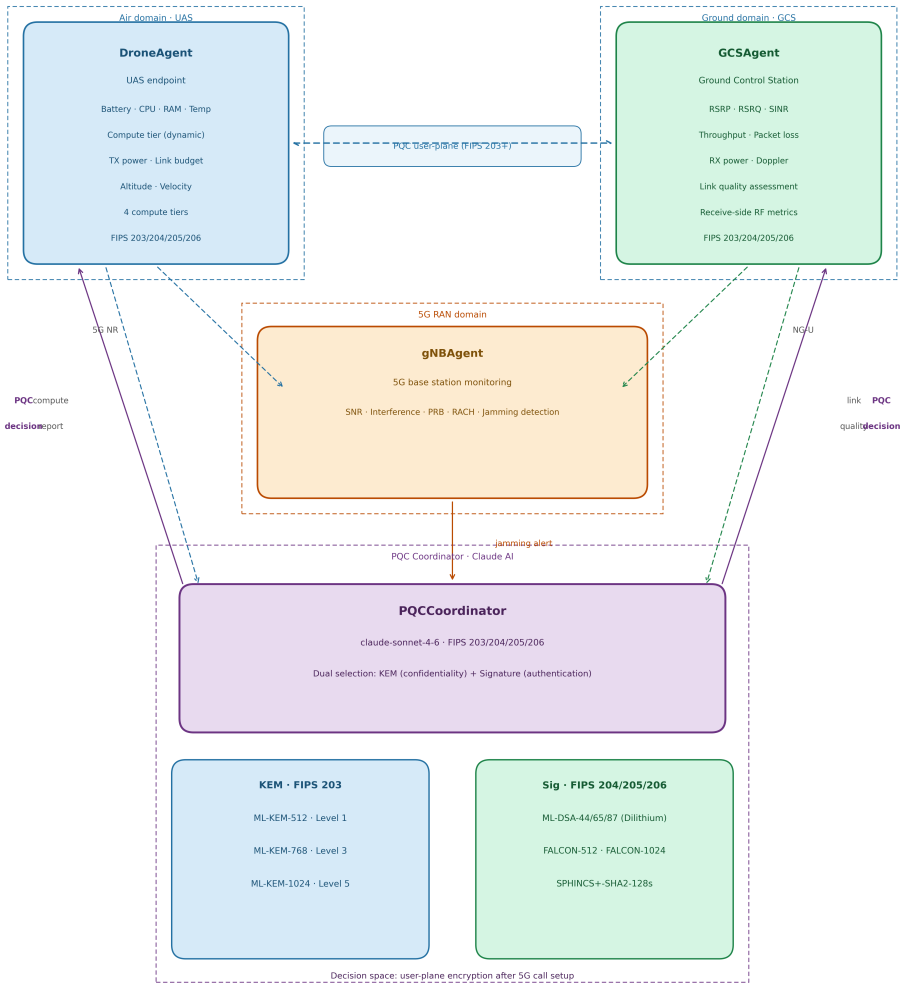


Fig. 3. Architecture diagram for AI agentic solution used for dynamic PQC selection.

A.2 Summary of Agents

Describe what each agent does.

References

1. 3GPP: 5G; Security architecture and procedures for 5G System. ETSI TS 133 501 V19.6.0 / 3GPP TS 33.501 Release 19. ETSI, Sophia Antipolis Cedex, France (2026). https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/19.06.00_60/ts_133501v190600p.pdf, last accessed 2026/04/26
2. 3GPP: Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture. ETSI TS 133 401 V19.2.0 / 3GPP TS 33.401 Release 19. ETSI, Sophia Antipolis Cedex, France (2026). https://www.etsi.org/deliver/etsi_ts/133400_133499/133401/19.02.00_60/ts_133401v190200p.pdf, last accessed 2026/04/26
3. 3GPP: Release 20. 3GPP Work Plan SP-260360, TSG SA#111, March 2026. 3GPP, Sophia Antipolis Cedex, France (2026). https://www.3gpp.org/specifications-technologies/releases/release-20, last accessed 2026/05/01
4. 3GPP: Technical Report 22.870: Study on 6G Use Cases and Service Requirements; Stage 1 (Release 20). 3GPP TR 22.870 V20.0.0, approved at TSG SA#111, Fukuoka, Japan, March 2026. 3GPP, Sophia Antipolis Cedex, France (2026). https://www.3gpp.org/ftp/Specs/archive/22_series/22.870/, last accessed 2026/05/03
5. 3GPP: Technical Report 33.801-01: Study on Security for the 6G System (Release 20). Draft V0.4.0, 3GPP SA WG3 (SA3). 3GPP, Sophia Antipolis Cedex, France (April 2026). https://www.3gpp.org/ftp/Specs/archive/33_series/33.801-01/33801-01-040.zip, last accessed 2026/05/03
6. National Institute of Standards and Technology (NIST): Post-Quantum Cryptography. Computer Security Resource Center. https://csrc.nist.gov/projects/post-quantum-cryptography, last accessed 2025/12/06
7. National Institute of Standards and Technology (NIST): Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography. Computer Security Resource Center (2024). https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved, last accessed 2025/12/06
8. National Institute of Standards and Technology: FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. Federal Information Processing Standard. NIST, Gaithersburg, MD (2024). https://doi.org/10.6028/NIST.FIPS.203
9. National Institute of Standards and Technology: FIPS 204: Module-Lattice-Based Digital Signature Standard. Federal Information Processing Standard. NIST, Gaithersburg, MD (2024). https://doi.org/10.6028/NIST.FIPS.204
10. National Institute of Standards and Technology: FIPS 205: Stateless Hash-Based Digital Signature Standard. Federal Information Processing Standard. NIST, Gaithersburg, MD (2024). https://doi.org/10.6028/NIST.FIPS.205
11. Barker, E., Chen, L., Davis, R.: Recommendation for Key-Derivation Methods in Key-Establishment Schemes. NIST SP 800-56C Rev. 2. National Institute of Standards and Technology, Gaithersburg, MD (2020). https://doi.org/10.6028/NIST.SP.800-56Cr2
12. Barker, E., Roginsky, A.: Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST SP 800-131A Rev. 2. National Institute of Standards and Technology, Gaithersburg, MD (2019). https://doi.org/10.6028/NIST.SP.800-131Ar2
13. Cooper, D., Apon, D., Dang, Q., Davidson, M., Dworkin, M., Miller, C.: Recommendation for Stateful Hash-Based Signature Schemes. NIST SP 800-208.

National Institute of Standards and Technology, Gaithersburg, MD (2020). https://doi.org/10.6028/NIST.SP.800-208
14. Barker, E., Barker, W.: Recommendation for Key Management: Part 1 – General. NIST SP 800-57 Part 1 Rev. 6 (Initial Public Draft). National Institute of Standards and Technology, Gaithersburg, MD (2025). https://doi.org/10.6028/NIST.SP.800-57pt1r6.ipd
15. Moody, D., Perlner, R., Regenscheid, A., Robinson, A., Cooper, D.: Transition to Post-Quantum Cryptography Standards. NIST IR 8547 (Initial Public Draft). National Institute of Standards and Technology, Gaithersburg, MD (2024). https://doi.org/10.6028/NIST.IR.8547.ipd
16. Perlner, R.: FIPS 206: FN-DSA (Falcon). NIST Computer Security Resource Center Presentation. NIST, Gaithersburg, MD (2025). https://csrc.nist.gov/presentations/2025/fips-206-fn-dsa-falcon
17. National Security Agency (NSA): Commercial National Security Algorithm (CNSA) Suite 2.0 Advisory Memorandum. September 2022. https://media.defense.gov/2022/Sep/07/2003071835/-1/-1/0/CNSA%202.0%20ADVISORY%20MEMO.PDF
18. 3GPP: TR 33.703: Study on transitioning to Post Quantum Cryptography (PQC) in 3GPP. Draft technical report, Release 20, portal entry. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4422, last accessed 2026/04/14
19. Turner, S., Kampanakis, P., Massimo, J., Westerbaan, B.E.: Internet X.509 Public Key Infrastructure – Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM). RFC 9935. RFC Editor (2026). https://doi.org/10.17487/RFC9935
20. Massimo, J., Kampanakis, P., Turner, S., Westerbaan, B.E.: Internet X.509 Public Key Infrastructure – Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA). RFC 9881. RFC Editor (2025). https://doi.org/10.17487/RFC9881
21. Stebila, D., et al.: Hybrid key exchange in TLS 1.3. IETF Internet-Draft, draft-ietf-tls-hybrid-design (work in progress), 2024. Available at: https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design
22. Stebila, D., Fluhrer, S., Gueron, S.: Hybrid key exchange in TLS 1.3. IETF Internet-Draft draft-ietf-tls-hybrid-design-16 (2025). https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/, last accessed 2026/04/14
23. Fluhrer, S., Kampanakis, P., McGrew, D., Nir, Y.: Hybrid Key Exchange in IKEv2 for Post-Quantum Security. RFC 9370, Internet Engineering Task Force (IETF), 2023. Available at: https://www.rfc-editor.org/rfc/rfc9370
24. GSMA: FS.41 Quantum Security Guidelines: Recommendations for Migration to Quantum-Safe Cryptography. Version 1.0, 2023. https://www.gsma.com/security/resources/quantum-security-guidelines-fs-41/
25. GSM Association: Post-Quantum Cryptography Documents. https://www.gsma.com/solutions-and-impact/technologies/security/post-quantum-cryptography-documents/, last accessed 2026/04/14
26. GSM Association: Post Quantum Cryptography – Guidelines for Telecom Use Cases. PQ.03 Version 2.0 (2024). https://www.gsma.com/newsroom/wp-content/uploads/PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-Cases-v2.0-2.pdf, last accessed 2026/04/14

27. GSM Association: Quantum-safe Cryptography for 4G and 5G Roaming. PQ.05 Version 1.0 (2025). https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2019/03/PQ.05-Post-Quantum-Cryptography-for-5G-Roaming-use-case-1.pdf, last accessed 2026/04/14
28. GSM Association: Post Quantum Cryptography for Non-Terrestrial Networks (PQ.07) (2026). https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/post-quantum-cryptography-for-non-terrestrial-networks-pq-07/, last accessed 2026/04/14
29. Kwiatkowski, K., Kampanakis, P., Westerbaan, B.E., Stebila, D.: Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3. IETF Internet-Draft draft-ietf-tls-ecdhe-mlkem-04 (2026). https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/, last accessed 2026/04/14
30. Connolly, D.: ML-KEM Post-Quantum Key Agreement for TLS 1.3. IETF Internet-Draft draft-ietf-tls-mlkem-07 (2026). https://datatracker.ietf.org/doc/draft-ietf-tls-mlkem/, last accessed 2026/04/14
31. Alliance for Telecommunications Industry Solutions (ATIS): Preparing 5G for the Quantum Era: An Analysis of 3GPP Architecture and the Transition to Quantum-Resistant Cryptography. ATIS-I-0000101. ATIS, Washington, DC (2025). https://cdn.atis.org/atis.org/2025/02/25152429/Preparing-5G-for-the-Quantum-Era-WP-V9.pdf, last accessed 2026/04/14
32. 3GPP: Study on Security for the 6G System (FS_6G_SEC). Study Item UID 1090044, approved in SP-251233, SA3#123. 3GPP, Sophia Antipolis Cedex, France (2025). https://www.3gpp.org/ftp/Specs/archive/33_series/33.700/, last accessed 2026/05/01
33. ITU-R: Recommendation ITU-R M.2160-0 – Framework and Overall Objectives of the Future Development of IMT for 2030 and Beyond. ITU-R, Geneva, Switzerland (2023). https://www.itu.int/rec/R-REC-M.2160/en, last accessed 2026/05/01
34. ITU-R: Report ITU-R M.2516 – Future Technology Trends of Terrestrial International Mobile Telecommunications Systems Towards 2030 and Beyond. ITU-R, Geneva, Switzerland (2022). https://www.itu.int/pub/R-REP-M.2516, last accessed 2026/05/01
35. 3rd Generation Partnership Project (3GPP), "TR 33.801-01: Study on Security for the 6G system," Release 20, Draft, Version 0.4.0, Apr. 2026.
36. European Telecommunications Standards Institute (ETSI): Secure Element Technologies (SET); Technical Report on impacts of the post-quantum cryptography on ETSI TC SET specifications. ETSI TR 104 005 V1.2.1. ETSI, Sophia Antipolis Cedex, France (2026). https://www.etsi.org/deliver/etsi_tr/104000_104099/104005/01.02.01_60/tr_104005v010201p.pdf, last accessed 2026/04/14
37. 3GPP: Specification series: 35 series. Includes the MILENAGE-256 and 256-bit 5G confidentiality, integrity, and authenticated-encryption algorithm specifications. https://3gpp.org/DynaReport/35-series.htm, last accessed 2026/04/14
38. Turnip, T.N., Andersen, B., Vargas-Rosales, C.: Towards 6G Authentication and Key Agreement Protocol: A Survey on Hybrid Post Quantum Cryptography. IEEE Communications Surveys & Tutorials **28**, 3311–3345 (2025). https://doi.org/10.1109/COMST.2025.3567439
39. 3GPP: LTE; 5G; Security of the Mission Critical (MC) service. ETSI TS 133 180 V19.4.0 / 3GPP TS 33.180 Release 19. ETSI, Sophia Antipolis Cedex, France (2026). https://www.etsi.org/deliver/etsi_ts/133100_133199/133180/19.04.00_60/ts_133180v190400p.pdf, last accessed 2026/04/26

40. 3GPP: LTE; 5G; Mission Critical Services Common Requirements (MCCoRe); Stage 1. ETSI TS 122 280 V19.7.0 / 3GPP TS 22.280 Release 19. ETSI, Sophia Antipolis Cedex, France (2026). https://www.etsi.org/deliver/etsi_ts/122200_122299/122280/19.07.00_60/ts_122280v190700p.pdf, last accessed 2026/04/26
41. 3GPP: Study on Security for the 6G system. 3GPP TR 33.801-01, Version 0.4.0, Release 20, Draft. 3GPP, Sophia Antipolis Cedex, France (2026). https://www.3gpp.org/ftp/Specs/archive/33_series/33.801-01/33801-01-040.zip, last accessed 2026/05/01