Review on PQC standardization activities

Work Package 3

Beyond the Limits of PQC

31^{th} March, 2026

Table 1: List of Authors and Affiliated Organizations

Author	**Organization**
Sanish Gurung	University of Helsinki
Gizem Akman	University of Helsinki
Amy Sokhna Sidibé	University of Helsinki
Markku Kojo	University of Helsinki
Valtteri Niemi	University of Helsinki
Camilla Hollanti	Aalto University
Sini Ruohomaa	Ericsson
Jorma Kivelä	Jutel
Suvi Lampila	SSH
Markus Rautell	VTT
Mari Muurman	VTT
Outi-Marja Latvala	VTT
Visa Vallivaara	VTT
Kimmo Järvinen	Xiphera
Petri Jehkonen	Xiphera

Table 2: Abbreviations and Definitions

Abbreviation	Full Form
3GPP	3rd Generation Partnership Project
ACME	Automated Certificate Management Environment
ADDKE	Additional Key Exchange
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AMWA	Advanced Media Workflow Association
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface
ASIC	Application-Specific Integrated Circuit
ATIS	Alliance for Telecommunications Industry Solutions
BCrypt	Best Cryptography (API)
BIKE	Bit Flipping Key Encapsulation
BSI	Bundesamt für Sicherheit in der Informationstechnik
C2PA	Coalition for Content Provenance and Authenticity
CA	Certificate Authority
CBOR	Concise Binary Object Representation
CBOM / CBoM	Cryptographic Bill of Materials
CI/CD	Continuous Integration / Continuous Deployment
CIP	Common Industrial Protocol
CMP	Certificate Management Protocol
CNG	Cryptography API: Next Generation
COSE	CBOR Object Signing and Encryption
CRC-32	Cyclic Redundancy Check-32
CRQC	Cryptographically Relevant Quantum Computer
CSF	Cybersecurity Framework
DORA	Digital Operational Resilience Act
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EST	Enrollment over Secure Transport
ETSI	European Telecommunications Standards Institute
EUF-CMA	Existential Unforgeability under Chosen Message Attack
FFT	Fast Fourier Transform
FIPS	Federal Information Processing Standard
FN-DSA	Fast-Fourier Transform over NTRU-Lattice-Based DSA
FORS	Forest of Random Subsets
GPV	Gentry-Peikert-Vaikuntanathan
GSMA	Groupe Spécial Mobile Association
HNDL	Harvest Now, Decrypt Later
HQC	Hamming Quasi-Cyclic
HSM	Hardware Security Module
IACS	Industrial Automation and Control Systems
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange Protocol Version 2

Continued on next page

Table 2 – continued from previous page

Abbreviation	Full Form
IND-CCA2	Indistinguishability under Adaptive Chosen Ciphertext Attack
IoT	Internet of Things
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
KDF	Key Derivation Function
KEM	Key Encapsulation Mechanism
KEX	Key Exchange
KMS	Key Management Service
KPI	Key Performance Indicator
LWE	Learning With Errors
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key Encapsulation Mechanism
MLWE	Module Learning With Errors
MPC	Multi-Party Computation
MTI	Mandatory To Implement
MTU	Maximum Transmission Unit
MXL	Media eXchange Layer
NCSC	National Cyber Security Centre
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NMOS	Networked Media Open Specifications
NTT	Number Theoretic Transform
ORAN	Open Radio Access Network
OT	Operational Technology
PKI	Public Key Infrastructure
PMTU	Path Maximum Transmission Unit
PQC	Post-Quantum Cryptography
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
SA	Security Association
SCEP	Simple Certificate Enrollment Protocol
SCKA	Sparse Continuous Key Agreement
SDO	Standards Developing Organization
SHA	Secure Hash Algorithm
SHAKE	Secure Hash Algorithm Keccak
SIKE	Supersingular Isogeny Key Encapsulation
SIS	Short Integer Solution
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SP	Special Publication
SPQR	Signal Post-Quantum Ratchet
SSH	Secure Shell
TLS	Transport Layer Security
TNFL	Trust Now, Forge Later
TPM	Trusted Platform Module
VPN	Virtual Private Network
WOTS+	Winternitz One-Time Signature Plus
XMSS	eXtended Merkle Signature Scheme

Contents

1 Introduction

This report provides a high-level overview of Post-Quantum Cryptography (PQC) standardization activities. The purpose of the report is to serve as a comprehensive resource for anyone interested in the evolving landscape of PQC and related standards bodies, Standards Developing Organizations (SDOs), Industry consortia, and Trade associations, governing its implementation.

As of May 2026, most cryptographic primitives are largely reliant on the mathematical hardness of either integer factorization or computation of discrete logarithms. These primitives are vulnerable to quantum-enabled cryptanalysis using Shor's algorithm [192], which further propagates to invalidate the security of widely adopted cryptographic schemes, protocols, and frameworks. This report addresses the systematic challenge of migrating standards, and ultimately systems based on standards, to a quantum-safe state.

The report is structured to facilitate a granular transition from legacy architectures to quantum-resistant paradigms. It commences by describing the theoretical foundation regarding quantum computing, the quantum threat vector, and its cascading ramifications for current cryptographic primitives, schemes, and frameworks. Following this, probabilistic risks assessment of projected quantum threat timeline, emerging mandates for cryptographic agility and hybrid implementation strategies are discussed.

After discussing the conceptual baseline, the report gives a longitudinal survey of the standardization landscape. First, standardization activities are explored that aim to specifications of cryptographic algorithms. Most notably, National Institute of Standards and Technology (NIST) runs a programme based on open calls for proposed algorithms. Next, the report covers how security protocols are being updated in SDOs, such as IETF and 3GPP, to include full support for PQC algorithms. The report then culminates in an evaluation of PQC remediation strategies within critical industry domains.

2 General Background

This section covers technologies and concepts that have a major impact on PQC standardization.

2.1 Quantum Computing

Quantum computers leverage the fundamental principles of quantum mechanics which is a branch of physics that describes the behavior and interactions of sub-atomic particles. Unlike classical computers that rely on binary bits representing discrete values of 0 or 1, quantum systems utilize quantum bits (qubits).

The utility of quantum processor is derived from four main physical phenomena:

- **Superposition**: A qubit exists in a complex linear combination of its basis states ($|0\rangle$ and $|1\rangle$). This allows a quantum system to hold multiple values at once and perform complex computations parallelly.[128]
- **Entanglement**: A phenomenon that facilitates non-classical correlations between qubits. A primary example is the formation of **Bell States**, where the state of one qubit is intrinsically linked to another regardless of spatial separation. This implies that measuring one qubit immediately determines the state of its counterpart.
- **Interference**: This is the mechanism used by quantum algorithms to identify solutions by utilizing wave-like properties. Quantum systems employ **constructive interference** to amplify the probability of measuring the correct answer and **destructive interference** to cancel out incorrect measurement paths. This process is essential for solving complex problems such as integer factorization [192].
- **Decoherence**: The primary physical constraint where a system loses its quantum properties due to environmental noise. Maintaining stability against decoherence is the chief obstacle to building a computer capable of breaking current public-key encryption.[178]

By exploiting these quantum principles, quantum computers can efficiently solve certain computational problems that are intractable for classical systems. Through the use of superposition and entangled states, a quantum processor can manipulate vast amounts of data in a single operation. This capability allows for the execution of algorithms that directly threaten the mathematical foundations underlying many current public-key cryptographic schemes [122].

2.2 Quantum Threat

As mentioned in [122], there are two primary types of cryptography: symmetric and asymmetric. Symmetric cryptography uses a single secret key for both encryption and decryption. This is typically a sufficient mechanism to protect data at rest because encryption and decryption are typically performed by the same party, and nobody else needs to know the secret key. When protecting data in transit with symmetric cryptography, the secret key needs to be known by both the sender and the receiver of the data. The security of symmetric cryptography derives from the randomness of key generation and the repetition of scrambling, mixing, and substitution operations on the data using that key. Although Grover's algorithm [69] proposed a quadratic speedup for unstructured search, which can be applied to brute-force key search, symmetric cryptographic schemes can withstand from quantum attacks by appropriately increasing key sizes.

In contrast, asymmetric cryptography (aka. public key cryptography) relies on the use of a public–private key pair for encryption and decryption. This helps protecting data in transit because only the receiver of the data needs to know the private key. Unlike symmetric cryptography, asymmetric schemes are typically based on a few computationally (presumably) hard mathematical problems, such as integer factorization and the discrete logarithm problem. However, these two problems can be efficiently solved by sufficiently large quantum computers using Shor's algorithm [192], emphasizing that asymmetric schemes are more vulnerable and immediate measures should be taken.

2.3 Timeline and Risk Assessment

As of 2026, the quantum landscape has shifted from theoretical experimentation to commercial utility [204]. The increasing availability of superconducting quantum chips with high qubit counts suggests that the window for migration to PQC is narrowing. The urgency of the quantum threat is gauged by three intersecting factors: shelf-life[1], migration time[2], and the threat timeline[3]. To quantify this risk, Mosca Inequality established a framework for cryptographic readiness and suggested that to safeguard organizational assests, the combined duration of the migration time and the required shelf-life of the data cannot be longer than the quantum threat time. [134]

If the time required to migrate infrastructure plus the time the data must remain secret exceeds the time until a quantum computer is available, the data is already compromised by Harvest-Now-Decrypt-Later (HNDL) attacks. In such attack, adversaries intercept and archive encrypted data in transit with the intent to decrypt it once Cryptographically Relevant Quantum Computers (CRQCs) become available. Another major quantum era threat scenario, which is largely overlooked in public discussions, is Trust-Now-Forge-Later (TNFL) attack. One example of such threat is a setting where hardware in a device includes public keys by which digital signatures of data, e.g., for software updates, can be verified. Although such signatures can be currently trusted, the situation changes drastically when CRQCs become available [119] . It is critical to note that a hasty or incomplete transition may inadvertently introduce new vulnerabilities; therefore, structured migration must outpace the narrowing threat window.

Beyond theoretical risk, the European Commission has established a strategic roadmap to achieve quantum readiness, emphasizing that transition efforts must begin by 2025 to avoid critical security gaps [56]. The roadmap prioritizes high risk use cases, defined as data requiring confidentiality for ten years or more, which must be fully migrated to post-quantum standards by the end of 2030. Following this, the EU aims for a comprehensive transition across medium and low risk systems by 2035, aligning with international targets set by NIST and the UK NCSC. Adhering to this phased timeline is essential to prevent a chaotic migration that could inadvertently introduce new vulnerabilities through insufficiently tested solutions.

2.4 Crypto-Agility and PQC Migration

The difficulty of updating deployed cryptography has long been evident: the retirements of DES and SHA 1 proceeded slowly and remain incomplete in many environments due to structural inflexibility [24, 32, 9]. Incidents such as the MD5 based rogue certificate authority attack highlight how quickly security can fail when organizations cannot remove compromised primitives [202]. The post quantum transition magnifies these challenges,

[1] time in the future where adversary utilizes quantum computers to break into the system for malicious purposes
[2] approximate time practitioners require to enhance the security to safeguard data
[3] remaining time/duration data must be kept secure (in years)

as systems must interoperate across classical, hybrid, and post quantum mechanisms while NIST continues to standardize additional signature schemes and refine security assumptions [33, 140]. As noted in [129], architectures must anticipate that algorithms or parameters may require replacement as cryptanalysis evolves.

Cryptographic agility, more familiarly referred to as crypto agility, is the ability of systems, protocols, and applications to update, replace, or retire cryptographic mechanisms with minimal operational disruption. It relies on modularity, algorithm independence, and clear abstraction boundaries that support repeated transitions over a system's lifetime [125]. At the integration level, practical deployments show that upgrades must often be incremental and non disruptive, particularly across heterogeneous and globally distributed environments [152]. Current analyses emphasize that crypto agility remains an evolving discipline, with ongoing work to formalize requirements and engineering practices, especially in the context of long term PQC migration [118, 95].

2.4.1 Algorithm agility

Algorithm agility refers to the ability of systems or protocols to replace cryptographic algorithms without requiring fundamental redesign [80]. This capability depends on fungibility: algorithms must be swappable through extensible identifiers, well defined mechanisms for adding and removing options, and downgrade resistant selection processes that prevent adversaries from forcing weaker choices [129]. Strong integrity protections and a clean separation between protocol logic and cryptographic primitives further ensure that algorithm choice evolves independently of protocol semantics or application behavior [80].

A central mechanism enabling this is the mandatory to implement (MTI) algorithm set, which guarantees interoperability while guiding controlled evolution of algorithm portfolios. MTIs must be revised as algorithms weaken, and new MTIs introduced before older ones reach their security limits [24]. RFC7696 therefore recommends concurrent support for multiple algorithms during transitions and cautions that excessive backward compatibility can preserve obsolete mechanisms, underscoring the need for explicit deprecation strategies [80]. MTIs therefore function both as interoperability anchors and as governance tools for guiding controlled algorithm evolution.

Existing studies highlight the necessity of migration supporting metadata, such as format identifiers and provenance tags, to enable coexistence across algorithm generations during phased transitions [164]. As the PQC landscape introduces diverse candidates with heterogeneous performance profiles, algorithm agility increasingly functions as an ecosystem level readiness measure, since the ability of protocols, libraries, and infrastructures to support interchangeable algorithms determines whether large scale PQC substitution can occur reliably and without systemic fragility [212].

2.4.2 Crypto-agility in protocol design

Protocol agility refers to the ability of security protocols to incorporate new algorithms while maintaining interoperability and security. This requires modular design and authenticated negotiation mechanisms that allow new identifiers or cipher suites to be introduced without redesign [24]. Extensibility is essential, since protocols must evolve without coordinated global updates [129]. Standards bodies therefore recommend separating base protocol specifications from algorithm profiles so that MTI sets can be revised independently [24]. Protocols must also avoid fixed assumptions about key sizes, hash lengths, or signature formats, since rigid parameter dependencies can cause structural breakage when new algorithms are introduced [80]. In practice, this requires extensible identifiers, version based signaling, parameter agility, and downgrade resistant negotiation [24, 80], as protocols tied to fixed parameters tend to become brittle and costly to update [152].

Operational experience illustrates these principles. TLS 1.3 (see Section 5.1) exemplifies deliberately engineered agility by adopting a minimal modern MTI set, removing legacy constructions, and simplifying future replacement of key establishment and AEAD primitives [203, 184]. Its streamlined negotiation structure enables hybrid and post quantum key exchange mechanisms without redesign [200], while capability signaling, authenticated selection, and downgrade resistance further strengthen transition robustness [24, 80]. Excessive backward compatibility, however, can preserve insecure mechanisms and introduce what Millett terms "bugwards compatibility" pitfalls [129]. A comparable form of crypto agile design appears in the evolution of the Signal protocol (see Section 8), whose handshaking and ratcheting mechanisms have been restructured into modular, interchangeable cryptographic components that allow authenticated key exchange and continuous

key agreement stages to swap KEMs (see Section 3.2), signatures, and symmetric ratchets under both classical and post quantum assumptions [10, 78, 105].

2.4.3 Crypto-agility in hardware and firmware

Hardware and firmware components impose distinct constraints on cryptographic agility. Many devices, including routers, switches, IoT platforms, real time operating systems, TPMs, HSMs, and secure boot chains, embed cryptography in fixed function ASICs or tightly coupled firmware, making algorithm replacement dependent on vendor roadmaps and hardware refresh cycles rather than software updates [169, 32]. These limitations become especially acute during the PQC transition, where larger keys, signatures, and message artifacts stress accelerator designs, buffer architectures, and protocol message size boundaries such as MTU and PMTU [24]. Because many embedded systems remain in service for a decade or more, conservative algorithm selection and long term planning for secure boot, attestation, and firmware validation are essential [108]. Limited cryptographic transparency in proprietary hardware means organizations often cannot determine which primitives are embedded, complicating dependency mapping and PQC migration sequencing [108, 169].

These realities create structural barriers that exceed those found in software. Effective hardware agility therefore requires advance planning, explicit architectural support for substitution, and close coordination with vendors. It also demands visibility into hardware cryptographic inventories, longer deprecation timelines, and mechanisms for coexisting classical, hybrid, and post-quantum primitives during multi-year transition periods [169]. Research highlights several forward looking strategies, including unified cryptoprocessors that support multiple PQC schemes within shared arithmetic units [5], reconfigurable logic that loads and swaps cryptographic bitstreams at runtime [166], and algorithm level adaptations that map PQC workloads onto legacy co processors without modifying underlying silicon [30]. These approaches illustrate possible pathways for achieving greater agility at the silicon level, showing how adaptable cryptographic substrates, reconfigurable hardware, or algorithm level techniques could extend the useful lifetime of deployed devices during the PQC transition.

2.4.4 Crypto-agility in system design

System level agility refers to the ability of applications, operating systems, cryptographic libraries, middleware, and hardware modules to evolve their cryptography without disrupting dependent components. Abstraction layers and standardized cryptographic APIs decouple application logic from concrete implementations, enabling libraries or middleware to dispatch operations to appropriate providers or accelerators [24]. Prior work emphasizes that modular, well structured interfaces are essential for replacing vulnerable components rapidly and safely, and that systems must prepare for the possibility of cryptographic failure by ensuring that flawed components can be substituted without architectural disruption [129]. This perspective extends to application facing APIs: agility succeeds or fails at the interfaces developers actually use, where stable semantics, safe defaults, explicit deprecation paths, and versioned identifiers support iterative replacement of algorithms and parameters without disruptive rewrites [196]. These principles are especially relevant in end to end encrypted systems, where envelope formats, metadata protection, and multi device synchronization introduce additional agility requirements. Stable SDK contracts and versioned formats enable coexistence across algorithm generations [196].

Agility in system design also depends on disciplined interface layering. The cryptographic implementation interface, the application facing interface, and the configuration or policy interface must evolve independently so that transitions can occur through configuration changes or provider substitution rather than code modification [126]. This model supports library centric, service oriented, or hybrid architectures, each enabling organization wide enforcement of cryptographic policy while preserving extensibility [126]. Diverse execution environments reinforce these requirements: PQC mechanisms introduce larger parameters and heterogeneous performance profiles, complicating integration in constrained, embedded, or real time systems [32]. Many operating systems fix cryptographic primitives at build time, and embedded platforms often permit only limited post deployment modification, making replaceable components and long term planning for secure boot, attestation, and firmware validation essential [24, 108]. Migration oriented system design therefore benefits from identifying potential weakness points early and isolating components so they can be replaced with bounded impact, supporting parallel validation and staged deployment of new cryptography [164]. Across these environments, agile system design ensures that cryptographic transitions remain manageable, observable, and aligned

with evolving requirements.

2.4.5 Crypto-agility in enterprise and organizational contexts

At the organizational level, crypto agility is a governance and operational capability rather than a purely technical property [9]. It depends on enterprise wide visibility into deployed cryptography and on structured processes that can prioritize and coordinate change across heterogeneous systems [24]. In practice this requires comprehensive cryptographic inventories and machine readable Cryptographic Bill of Materials (CBoMs) that list algorithms, keys, certificates, libraries, hardware dependencies, and data flows [165, 164]. Standards such as CycloneDX support these structures and enable automated risk assessment, policy enforcement, and migration planning [44, 171]. Integrating inventories with CI/CD workflows turns cryptographic updates into a repeatable process and provides a consistent basis for regression validation, deprecation enforcement, and compliance monitoring [118, 126]. Organizations can then measure readiness using KPIs that capture inventory completeness, algorithm swap latency, and workforce preparedness, placing agility within the scope of accountable enterprise governance [20].

At the enterprise level, crypto agility is governed as a lifecycle managed service that relies on centralized oversight and coordinated policy. Enterprise level cryptographic agility frames cryptography as centrally managed providers that support controlled updates, rollbacks, and replacements across diverse environments [195]. Most organizations remain at early stages of this capability [79], which makes formal governance frameworks essential. DORA treats cryptographic lifecycle management and PQC migration as auditable resilience obligations that extend to ICT supply chains [183, 84]. NIST CSF 2.0 provides a similar structure by mapping PQC transition into governance, identification, protection, detection, response, and recovery processes [150]. Independent analyses highlight that enterprise agility must operate within an organization wide security program and cannot be delegated to isolated engineering teams [23].

Organizational readiness ultimately determines whether crypto agility succeeds in practice. Leadership engagement, dedicated resources, enterprise wide training, and structured governance processes form the core organizational capabilities identified as necessary for cryptographic agility [20]. Industry guidance stresses that agile organizations integrate cryptographic considerations into procurement processes [164], and that they maintain detailed documentation of deployed primitives and authenticated update mechanisms for long lived systems [168]. Strategic studies show that PQC migration is a large scale transformation that demands early planning and active executive stewardship, especially for organizations that rely on legacy systems or complex vendor ecosystems [123]. Governance must ensure that external policy or standards changes result in controlled and automatable updates for application teams by providing stable API contracts, explicit deprecation schedules, and compatibility affordances [196].

2.5 Hybrid Approach

Although postquantum cryptographic algorithms have been analyzed extensively in recent years, much bigger cumulative amount of cryptanalytic efforts have been devoted to breaking classical public-key cryptography, especially RSA and ECC. Because of these “test of time” guarantees it is sensible to try to combine a postquantum algorithm with a classical one. This approach is called “hybrid” in the postquantum context. Secure implementations of RSA and ECC already exist, and these are still useful as long as Shor’s algorithm cannot be efficiently used against these classical public-key solutions. The aim of the hybrid approach is to reach a security level that is the maximum of the two security levels: the level reached by the classical algorithm alone and the level reached by the postquantum algorithm alone. The most obvious drawback of the hybrid approach is that the performance cost is doubled because two algorithms must be run instead of a single one.

In general, two key separate key establishment protocols can be run between the same parties in order to create two independent shared keys. Assuming these two protocols are somehow securely tied to each other, another shared key can be created by simply concatenating the two keys. A key derivation function is further applied to the combined shared key before it is used for, e.g., a symmetric encryption algorithm, such as AES. If one of the individual shared keys can be obtained by the attacker, that still does not give any advantage in finding out the derived key.

For digital signatures, the hybrid approach means creating two independent signatures for the same message. Assuming that these two signatures are somehow securely tied to each other, the combine signature, also

called "dual" signature, is the pair of the two individual signatures. The dual signature is considered valid only if the two corresponding verification algorithms successfully verify both individual signatures in the pair. In addition to duplicating the computational cost, the length of the signatures is also doubled with this approach.

3 NIST PQC standardization

The National Institute of Standards and Technology (NIST) is an agency within the U.S. Department of Commerce [136] and serves as a leading standardization body for global cryptographic standards. Over the recent years and still in 2026, NIST spearheads the transition toward PQC by leading the development of standards to withstand quantum-enabled cryptanalysis. NIST governs the PQC algorithm selection process by evaluating candidate algorithms based on cryptographic strength, computational efficiency, and cross-platform implementability for both Key Encapsulation Mechanisms (KEMs) and Digital Signature Algorithms (DSAs).

The "Post-Quantum Cryptography Standardization" is the cornerstone of the NIST effort where researchers propose their algorithms under exhaustive peer-review. For meeting transparency and multi-stakeholder alignment, NIST has facilitated six workshops, as of May 2026 [151]. These fora are designed to foster interdisciplinary synergy between academic researchers, industry partners, and government stakeholders. These fora allow stakeholders to iteratively refine the PQC standards by facilitating community feedback and reviewing the results of rigorous cryptanalytic stress-testing.

3.1 NIST Selection Process

THE NIST's effort to PQC standards has undergone multi-stage competition to narrow a vast collection of global candidate algorithms into specialized suite of standardized primitives.

- **Phase 1: Initial Call (2016):** NIST issued a formal request for researchers to submit quantum-resistant primitives to cover new public key standards, focusing on KEMs and DSAs [133, 143] .
- **Phase 2: Evaluation Rounds (2017-2022):**
  - **Round 1 (2017):** Out of numerous proposals, NIST accepted 69 submissions [146]. By 2019, this field was narrowed to 26 algorithms that demonstrated sufficient security and efficiency to advance to the second round [141].
  - **Round 2 (2020):** From the 26 remaining candidates, NIST declared 7 finalists and 8 alternative algorithms to proceed to the third round [142]. The aim was to standardize at least one KEM and one DSA based on the finalist algorithms, while alternative algorithms were considered for potential standardization later.
  - **Round 3 (2022):** The NIST issued first major standardization announcement. NIST selected four primary algorithms for standardization:

    ML-KEM (CRYSTALS-Kyber) [22], ML-DSA (CRYSTALS-Dilithium) [116], FN-DSA (FALCON) [62] and SLH-DSA (SPHINCS+) [21].

    In addition, four candidate algorithms for KEM moved onto the fourth round. These algorithms are Supersingular Isogeny Key Encapsulation (SIKE) [91], Bit Flipping Key Encapsulation (BIKE) [16], Hamming Quasi-Cyclic (HQC) [65] and Classical McEliece [26]. As no candidate digital signature algorithms were kept in the competition, NIST issued an additional call for new digital signature schemes separately, preferably for algorithms relying on mathematical problems other than the lattice problem [137, 132].
  - **Round 4 (2022-May 2026):** Among the remaining four KEM algorithms from the previous round, SIKE team has officially withdrawn from the NIST competition because a major mathematical breakthrough rendered it completely insecure and easy to crack on a standard computer[206, 127]. The HQC algorithm became a winner as NIST decided to proceed it for standardization process in 2025 [138]. As of May 2026, this round is the final evaluation for the remaining KEM candidates and concurrently, there is an additional round in the call for new digital signature schemes [132].

- **Phase 3: Additional Signature Call (2022-May 2026)**: Parallel to finalizing the original competition, NIST accepted 40 signature algorithms as legitimate submissions in the first additional round for digital signatures in 2023 and subsequently, in October 2024, 14 of them moved forward to the second round of this additional call. Notably, 13 of these 14 algorithms are not based on lattice mathematical problems. In May 2026, NIST announced nine candidates that moved on to the third additional round for digital signatures. [145, 147, 148]

3.2 Key-Encapsulation Mechanisms

The Key Encapsulation Mechanism (KEM) is the method of securely establishing a shared secret key between two communication parties over a public channel. Conceptually, a KEM utilizes the properties of asymmetric cryptography to securely exchange a shared secret key that is subsequently used for symmetric cryptography, ensuring both confidentiality and data integrity.

The KEM Workflow: In a standard key exchange between two entities, Alice and Bob, the protocol typically proceeds as follows. While the roles of the initiator and responder can be swapped, the mechanism ensures that both participants arrive at an identical shared secret key.

- Alice first executes probabilistic "KeyGen" which allows Alice to create a pair of encapsulation/public (p_k) and decapsulation/private/secret (s_k) keys.
- Then, Alice gives her public key (p_k) to Bob.
- Bob runs probabilistic "Encapsulation" algorithm using Alice's public key (p_k) to get ciphertext (C) and shared secret key (K).
- Now, it is Bob's turn to give ciphertext (C) to Alice.
- Alice then runs deterministic "Decapsulation" algorithm, using her secret key (s_k) and C as inputs, to obtain shared secret key (K) as output.

Unlike traditional key exchange protocols (such as Diffie-Hellman), a basic KEM is inherently unidirectional, i.e., the ciphertext of the shared secret (C) is transmitted by the sender and recovered by the receiver to obtain the shared secret key (K). Notably, standard KEMs do not inherently provide mutual authentication or a key confirmation step to verify that both parties possess the correct key. Such verification, if required, must be handled by higher-level protocols. NIST published in September 2025 recommendations about how KEM can and should be used in various contexts, e.g., for authenticated key establishment or for key confirmation [144]. In the same document, NIST provides extensive guidelines about how KEMs should be implemented.

As of May 2026, NIST has selected two PQC algorithms for standard KEMs. They are listed below:

- **ML-KEM**: Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) is a KEM based on the CRYSTALS-Kyber algorithm. It was selected by NIST in July 2022 and was standardized under Federal Information Processing Standard (FIPS) 203 in August 2024. It is designed to achieve Indistinguishability under Adaptive Chosen Ciphertext Attack (IND-CCA2)[4] security. The security of ML-KEM is primarily based on computational difficulty of Module Learning with Errors (MLWE) problem [111], which is a generalization of the Learning with Error (LWE) problem [182]. In an LWE problem, a system of linear equations is noised with small errors, which makes solving them intractable with known methods like Gaussian elimination. MLWE adds another layer of security by employing module lattices, where equations are constructed using polynomial rings rather than simple integers. ML-KEM employs a variant of Fujisaki-Okamoto transform in both encapsulation and decapsulation algorithms [158, 157]. Furthermore, it utilizes the Number Theoretic Transform (NTT) to perform rapid polynomial multiplications. Lastly, NIST provided three parameter sets for ML-KEM.[131, 137]
- **HQC-KEM**: Hamming Quasi-Cyclic Key Encapsulation Mechanism (HQC-KEM) is a code-based KEM and is considered as a backup to ML-KEM. It is designed to achieve IND-CCA2 security. This level of security is

[4] a property where an adversary cannot distinguish a shared secret from randomly sampled key, even with access to a decryption oracle for other ciphertexts

achieved by applying a salted version of the Fujisaki-Okamoto transform to the underlying HQC Public Key Encryption (HQC-PKE) scheme. Its security depends on the computational hardness of the Quasi-Cyclic Syndrome Decoding (QCSD) problem, which is a variant of the Syndrome Decoding (SD) problem proven to be NP-complete with respect to the Hamming Distance [25]. Furthermore, it utilizes a concatenation of Reed-Muller and Reed-Solomon (RMRS) [17] codes for error correction to ensure a low Decoding Failure Rate (DFR). Note that, unlike is the case with traditional algorithms RSA and ECC, both ML-KEM and HQC-KEM include a small chance for decryption errors.[66]

Although HQC has been selected as a reserve standard in 2025, it is not yet included in FIPS. NIST plans to release an initial draft for **FIPS 207** standard incorporating HQC later in the year 2026.

3.3 Digital Signature Algorithms

A Digital Signature Algorithm (DSA) is a mathematical scheme which is used to demonstrate the authenticity of digital messages or documents. A valid digital signature gives a recipient/verifier reason to believe that the message was created by known sender/signer. That means it provides authentication of the origin, and guarantees that the message was not altered in transit, i.e., it ensures integrity.

DSA Workflow: In a standard communication between a signer (Alice) and a verifier (Bob), the protocol ensures authenticity and integrity. The Digital Signature process is divided into the operations performed by the signer (Alice) and the verifier (Bob).

Signer Side (Alice):

- **Setup:** Alice first executes a probabilistic "KeyGen" algorithm to produce a key pair consisting of a private signing key (s_k) and a public verification key (p_k). One key pair can be used in signing of many messages.
- **Hashing:** When Alice wants to sign a message (M), she first processes M through a deterministic "Hash" function to obtain a fixed-length message digest (H).
- **Signing:** Then, Alice runs probabilistic "Signing" algorithm using her private key (s_k) and the digest (H) to produce a digital signature (σ).
- **Sending:** Finally, Alice sends both the original message (M) and the digital signature (σ) to Bob.

Verifier Side (Bob):

- **Message Processing:** After receiving the original message (M) and the digital signature (σ), Bob independently runs the same deterministic "Hash" function on M to obtain H'.
- **Verification:** Bob executes a deterministic "Verification" algorithm using Alice's public key (p_k), signature (σ), and the computed digest H'.
- **Validation:** The verification algorithm returns a boolean result; i.e., if the result is True, Bob accepts the signature as authentic; otherwise, the message is rejected.

As of May 2026, NIST has selected three post-quantum DSAs. They are listed below:

- **ML-DSA**: Module-Lattice-Based Digital Signature Algorithm (ML-DSA) is the NIST standardized and refined version of the CRYSTALS-Dilithium scheme [116]. It was selected by NIST in July 2022 and formally was published in August 2024 under FIPS 204. ML-DSA is designed to have Strong Existential Unforgeability under Chosen Message Attack (SUF-CMA)[5]. The security of ML-DSA is inherent from MLWE problem [111] and the nonstandard variant of Module Short Integer Solution (MSIS) problem called SelfTargetMSIS [103]. In addition, ML-DSA employs "Fiat-Shamir with Aborts" framework which uses a rejection sampling check to ensure the generated signature does not leak sensitive information about the private key[114, 115]. Furthermore, it utilizes the Number Theoretic Transform (NTT) to perform rapid polynomial multiplications. Lastly, NIST provided three parameter sets for ML-DSA. [139]

[5] property where adversary cannot produce a new valid signature, even for a message that has already been signed by the known signer

- **SLH-DSA**: Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) is the standardized version based on the SPHINCS+ scheme[27, 198]. It was selected in July 2022 and was formally published in August 2024 under FIPS 205. Although based on hash functions, it is still a stateless scheme[6], meaning it does not require the signer to maintain and update a record of previously used signatures. Its security is designed for EUF-CMA and relies on the presumed difficulty of finding preimages and collisions for the underlying hash functions. The algorithm is constructed using a multi-layered framework that includes Winternitz One-Time Signature Plus (WOTS+) [36], the Forest of Random Subsets (FORS) few-time signature scheme, and a hypertree of eXtended Merkle Signature Scheme (XMSS) instances [81]. The WOTS+ and XMSS components in SLH-DSA are specially modified versions that differ from the original specifications in RFC 8391 [81] and SP 800-208 [36]. Furthermore, NIST approved twelve parameter sets for SLH-DSA, categorized by their use of SHA-2 or SHAKE hash functions across different security levels. [149]

- **FN-DSA**: Fast-Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA) is the standardized version of Falcon scheme. It was selected in July 2022; however, NIST has not disclosed a formal document under FIPS 206 as of May 2026. It is a lattice-based signature scheme based on hash-and-sign paradigm. Its design is built upon the theoretical Gentry-Peikert-Vaikuntanathan (GPV) framework [67] and is proved to be secure in the random oracle model based on NTRU-SIS. It also uses randomized trapdoor sampler called Fast Fourier sampling [42]. This scheme also relies on FFT for private key operations and NTT for rapid polynomial multiplication during verification. To prevent potential security issues from duplicate signatures, FN-DSA adopts hash randomization by prepending a 320-bit salt to the message before hashing with SHAKE-256.[63]

NIST is also hosting an on-ramp signature competition in order to get more variety into the underlying hard mathematical problems of standardized digital signature algorithms. The additional algorithms include lattice-based, isogeny-based, MPC-in-the-head, symmetric-based, and multivariate algorithms. As of May 2026, the competition is currently in its third round with 9 schemes still under consideration. [148]

The security strength of NIST PQC algorithms is broadly grouped into the following five levels, and to each of the PQC security levels, the corresponding traditional and post-quantum algorithms can be mapped:

Level 1: At least as hard as breaking AES-128 (key search on block cipher) , PQC-Algorithm: ML-KEM-512, FN-DSA-512, SLH-DSA-SHA2/SHAKE-128f/s

Level 2: At least as hard as breaking SHA-256/SHA3-256 (collision search on a 256-bit hash function), PQC-Algorithm: ML-DSA-44

Level 3: At least as hard as breaking AES-192 (key search on block cipher), PQC-Algorithm: ML-KEM-768, ML-DSA-65, SLH-DSA-SHA2/SHAKE-192f/s

Level 4: At least as hard as breaking SHA-384/SHA3-384 (collision search on a 256-bit hash function), PQC-Algorithm: No algorithm yet at this level

Level 5: At least as hard as breaking AES-256 (key search on block cipher), PQC-Algorithm: ML-KEM-1024, FN-DSA-1024, ML-DSA-87, SLH-DSA-SHA2/SHAKE-256f/s

4 PQC in ISO/IEC

International Organization for Standardization (ISO) is a global organization formed by a network of national standards organizations where each national standards organization represents its respective country [86]. ISO follows a consensus-based approach to developing and publishing standards across various industries, including post-quantum cryptography. Complementing this, International Electrotechnical Commission (IEC) is an organization that supports and fosters in formalizing international standards for all electronical, eletronics and related technologies, covering many technologies such as batteries and fibre optics [13]. For information technology and cybersecurity, including post-quantum cryptography, ISO and IEC collaborate through a Joint Technical Committee (ISO/IEC JTC 1) to ensure a unified global approach.

Some algorithms that have NOT been selected by NIST have been proposed for standardization in other standardization bodies, most notably in the ISO. As of May 2026, FrodoKEM [205] and Classic McEliece [26]

[6] property where signer does not need to keep track of state, e.g., counter of previously signed messages, which is different from other hash-based schemes XMSS and LMS

are potential candidates for standardization within ISO/IEC JTC 1/SC 27, which is responsible for IT security techniques (ICS 35.030) [68, 113].

- **Classic McEliece:** It is a KEM based on the hardness of syndrome decoding problem in binary Goppa codes. It is IND-CCA2 secure and and is based on the difficulty of decoding a randomly corrupted code without the secret structure, a problem that has resisted many attacks for over four decades. Unlike traditional public-key schemes based on integer factorization or discrete logarithms, McEliece does not rely on number-theoretic assumptions and is therefore considered resistant to quantum attacks. Modern constructions such as Classic McEliece use Niederreiter's formulation to provide an IND-CCA2-secure key encapsulation mechanism with strong security margins against both classical and quantum adversaries.[26]
- **FrodoKEM:** It is a post-quantum KEM built on the LWE problem over algebraically unstructured lattices. It is IND-CCA2 secure and offers twelve parameters sets for three security levels (matching AES-128,192, and 256). It features two main variants: a standard version for unrestricted key reuse and an ephemeral variant (eFrodoKEM) for fresh key generation. It also provides flexibility through AES or SHAKE variants, allowing for optimized performance based on a system's hardware acceleration capabilities. It remains highly trusted and is recommended by the German BSI [59], Netherland's NLNCSA and AIVD [11], and France's ANSSI[14]. [113, 205]
- **NTRU:** It is a post quantum KEM which is based on the hardness of Ring-LWE and SIS problems over polynomial rings, i.e., on hardness of finding short vectors in a specific type of lattice. It offers five parameter sets for three different NIST security levels. It is IND-CCA secure and is currently progressing through the ISO/IEC standardization pipeline under JTC 1/SC 27. Within this process, it is being evaluated for integration into the ISO/IEC 29192-4 standard, which targets on building lightweight cryptographic solutions designed for constrained and portable environments [37].

5 PQC in Internet standards (IETF)

Internet Engineering Task Force (IETF) is the premier standards organization that improves the Internet's functionality through the development of high-quality technical specifications known as Request for Comments (RFCs). IETF does not operate in a membership structure, meaning that it relies on a global community of individual volunteers who drive progress through "rough consensus" and practical implementation ("running code"). In IETF, the primary work occurs within specialized "Working Groups", which refine initial Internet-Drafts into the foundational protocols that support global digital communication [88]. A repository of PQC-related Internet-drafts is maintained by the Post-Quantum Use In Protocols (PQUIP) working group [211].

5.1 TLS

Transport Layer Security (TLS) [184] is a cryptographic protocol, standardized by the IETF, that provides a secure communication between two parties, ensuring the authentication, confidentiality, and integrity. The protocol is divieded into two main components: the Handshake protocol, which negotiates cryptographic parameters and establishes shared keys, and the Record Protocol, which secures the subsequent data traffic using those keys.

The primary algorithms currently used in TLS 1.3 for key exchange are Ephemeral Diffie–Hellman (DHE) and Elliptic Curve Diffie–Hellman (ECDHE), specifically curves such as X25519, NIST P-256, and NIST P-384. For digital signatures, the protocol relies on RSA, the Elliptic Curve Digital Signature Algorithm (ECDSA), and the Edwards-curve Digital Signature Algorithm (EdDSA). [184]

The primary focus of the PQC transition in TLS 1.3 is securing the key exchange against "harvest-now-decrypt-later" attacks. Current internet-drafts [200, 106] specify hybrid key exchange for TLS 1.3 by treating combinations of classical ECDH and post-quantum ML-KEM—such as X25519MLKEM768—as single named entities. This hybrid approach is preferred because it ensures the session remains secure even if one underlying algorithm is compromised; however, it necessitates significant updates to underlying cryptographic libraries and introduces practical challenges regarding message size [179]. Specifically, since hybrid key shares are computed by concatenating independent outputs via a Key Derivation Function (KDF), the resulting `ClientHello`

may exceed the Path Maximum Transmission Unit (Path MTU), potentially leading to packet fragmentation and thereby increased risk of additional retransmissions and latency [179, 200].

The internet-draft draft-reddy-emu-pqc-eap-tls-02 [180] proposes enhancing EAP-TLS and EAP-TTLS with post-quantum algorithms. To mitigate the risk of session failures caused by significantly larger PQC certificates, it suggests leveraging Enrollment over Secure Transport (EST) to pre-retrieve and cache intermediate certificate chains, thereby reducing handshake overhead.

Datagram TLS (DTLS) [185] is a protocol whose aim is to provide security guarantees equivalent to those of TLS, for communications run on top of connectionless protocols such as User Datagram Protocol (UDP), instead of Transmission Control Protocol (TCP). The post-quantum migration path for DTLS is expected to follow the one of TLS. The internet draft [179] also addresses the DTLS-specific PQC migration challenges. The first challenge is having many ClientHello messages-caused by exceeding MTU-lead to increase in latency and delaying in handshake in lossy network. The second challenge concerns DTLS deployment where IP/UDP (ClientHello) messages are not properly handled by middlebox. [179]

5.2 IPsec

Internet Protocol Security (IPsec) [100, 98, 99] is a network protocol suite that helps to establish mutual authentication, negotiate cryptographic keys, and encrypt data packets for a secure channel operating at the IP layer between individual hosts, entire networks, or security gateways.

The Internet Key Exchange Protocol Version 2 (IKEv2) is a core component for the IPsec suite used to establish and maintain Security Associations (SAs) through mutual authentication and the negotiation of cryptographic keys [97]. IKEv2 relies on DH or ECDH for key exchange and RSA or ECDSA signatures for peer authentication. [97]

RFC 9370 [207] facilitates the transition to post-quantum cryptography (PQC) by modifying how IKEv2 negotiates and executes key exchanges. RFC 9370 redefines “Transform Type 4” from “Diffie-Hellman Group” to the broader “Key Exchange Method”, allowing the protocol to support non-discrete-logarithm-based algorithms. It introduces seven new transform types (ADDKE1 through ADDKE7), enabling the negotiation of multiple additional key exchanges that can be combined with a classical exchange to create a hybrid shared secret.

As of May 2026, an active Internet-Draft, draft-ietf-ipsecme-ikev2-pqc-auth-06 [181], is undergoing IETF review. It proposes integrating post-quantum cryptographic signature algorithms, specifically ML-DSA and SLH-DSA, into the IKEv2 authentication process to update existing standards.

Another active Internet-Draft, draft-wang-ipsecme-kem-auth-ikev2-03 [210], proposes a post-quantum authentication method for IKEv2 that replaces traditional digital signatures with Key Encapsulation Mechanisms (KEM) like ML-KEM. This approach specifically modifies the IKE_AUTH exchange by using the KEM to establish a shared key that proves the responder’s identity, thereby reducing the large message overhead and computational strain typically associated with post-quantum signature schemes.

5.3 Secure Shell

Secure Shell Protocol (SSH) is a cryptographic network protocol that provides secured terminal, file transfer and application tunneling services over untrusted network. The first version of SSH was invented by Tatu Ylönen in 1995, to replace protocols such as rlogin, TELNET, rsh, rcp and FTP which failed to ensure strong authentication and confidentiality. The protocol was completely redesigned as SSH-2 to address security vulnerabilities such as the design flaw with Cyclic Redundancy Check-32 (CRC-32) checks. The SSH-2 protocol was later standardized by the IETF in 2006 [214].

The protocol follows a client-server model where SSH-2 establishes a secure channel via a negotiated Key Exchange (KEX) mechanism. Server identity is verified through public-key host keys, while symmetric encryption and hashing algorithms ensure confidentiality and data integrity [199]. User identity is typically verified using public-key credentials or certificates. By negotiating cryptographic suites for KEX, ciphers, and signatures, SSH-2 provides a modular framework for algorithm agility. This flexibility allows for the seamless adoption of new cryptographic standards, such as post-quantum algorithms, without breaking backward compatibility.

As of May 2026, the two hybrid KEM proposals: draft-ietf-sshm-ntruprime-ssh-06 [64] and draft-ietf-sshm-mlkem-hybrid-kex-10 [96] have been submitted to the Internet Engineering Steering Group (IESG) for publica-

tion as RFCs. The document draft-ietf-sshm-ntruprime-ssh-06 [64] has transitioned to the AUTH48 state and is designated to be published as RFC 9941 [121].

Informal internet-drafts for the use of the PQC ML-DSA signature algorithm such as draft-sfluhrer-ssh-mldsa-05 [61] exist. However, PQC for secure shell authentication use cases have not yet been widely implemented, nor are there any internet-drafts yet in the publication track to become published as RFCs.

5.4 JSON/CBOR Signing and Encryption

Data object security is primarily governed by two parallel frameworks: JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE). JOSE, established through a suite of specifications, including RFC 7515 [93] for signatures and RFC 7516 [94] for encryption, represents secured content using JSON-based data structures, requiring Base64URL encoding for binary components. Conversely, COSE protocol, defined in RFC 9052 [188], serves as a binary-optimized alternative specifically designed for constrained nodes and the Internet of Things (IoT). By utilizing CBOR for serialization, COSE achieves a small message size and reduced code size, minimizing the processing overhead critical for resource-limited environments.

As defined in RFC 7515 [93] and RFC 7516 [94], the JOSE suite uses the JSON Web Algorithms (JWA) [92] registry, managed by RFC 7518, to select specific primitives such as RSASSA-PKCS1-v1_5 for signatures or RSAES-OAEP and ECDH-ES for encryption. Similarly, RFC 9052 and RFC 9053 set up the algorithm lists for COSE, which include similar options like ECDSA and EdDSA.

The specific mathematical operations used by these structures are centralized in JSON Web Algorithms (JWA) defined in RFC 7518 [92]. RFC 7518 [92] serves as a registry for the cryptographic foundations of the framework, including digital signature algorithms such as RSASA-PKCS1-v1_5, and ECDSA, as well as encryption methods such as AES-GCM and key management schemes such as RSA-OAEP.

In terms of PQ transition in JOSE and COSE, there are three main Internet Drafts: i) draft-ietf-cose-dilithium-11 [175], ii) draft-ietf-cose-falcon-04 [176], and iii) draft-ietf-cose-sphincs-plus-07 [177]. These drafts provide technical specifications and integration of PQ DSA within JOSE and COSE frameworks. All of these specifications are based on Algorithm Key Pair (AKP) type to standardize key handling. Furthermore, draft-ietf-cose-sphincs-plus-07 and draft-ietf-cose-falcon-04 restrict usage to the pure mode of algorithms and not the pre-hash variant to minimize the implementation complexity. Additionally, for draft-ietf-cose-sphincs-plus-07 and draft-ietf-cose-falcon-04, to defend against physical attacks, these drafts mandate that implementations of these signature schemes should strictly follow side-channel resistant practice, such as constant-time operations and uniform memory access patterns. Lastly, draft-ietf-cose-sphincs-plus-07 and draft-ietf-cose-falcon-04 require mandatory public key validation before signing or verification occurs. [175, 177, 176]

5.5 Email protection S/MIME and Cryptographic Message Syntax: CMS

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for securing electronic messages by adding cryptographic protections to MIME data. It provides authentication, message integrity, and non-repudiation through digital signatures, as well as confidentiality via encryption, and can optionally compress messages. While primarily designed for traditional email clients, S/MIME can be applied to any transport protocol that carries MIME-formatted data, such as HTTP or SIP. It also supports automated systems, enabling secure signing and encryption of machine-generated messages without user intervention. [189]

While S/MIME provides the framework for protecting MIME data, its actual cryptographic operations and the transition to post-quantum resilience are defined by the underlying Cryptographic Message Syntax (CMS).

CMS is at the core of a family of standards that allow encryption and signing of arbitrary files in a way that can make use of PKI built from X.509 certificates. S/MIME, most well known from encrypted email, builds in turn on PKCS#7, the original Cryptographic Message Syntax developed by RSA laboratories. CMS in its current form is defined in RFC 5652.

To send encrypted and signed email in the classical setting, the sender signs the message with its own private key, and to encrypt it generates a symmetric key, encrypts the message with that key, and then encrypts the symmetric key with the public key of each recipient. Recipients can then read the message by using their own private key to decrypt the symmetric key, and then use the latter key to decrypt the message, as well as validate signatures by using the public verification key of the sender. When using a PKI based on a certificate authority that both parties trust, the needed public keys can be distributed by email.

The CMS format is cryptographically agile and can support PQC signatures, but it received a separate update in RFC 9629 to provide a new way of working for encryption using KEM algorithms. This was a necessary extension: while RSA keys can encrypt a single symmetric key multiple times to different recipient public keys, a KEM algorithm such as ML-KEM can only establish an individual key with each public ML-KEM key, and this becomes a challenge, for example, when sending email to multiple recipients.

In order to work around this issue, an additional symmetric key is introduced to allow upgrading CMS encryption from using RSA to using instead a PQC algorithm like ML-KEM. This symmetric key is generated first and the message contents, e.g., email, are encrypted with it. Then ML-KEM is used to agree on an individual key[7] against each recipient's public ML-KEM key, and that individual key is used to encrypt the common key for that recipient.

In the past, it has been quite common to see a single RSA key certificate used for both mail encryption and signing for easier manageability in email clients; instead of explicitly sharing certificates, users have been technically able to deliver their individual certificate as a side effect of signing the email, and several mail clients have automatically discovered the user's certificate this way. However, key reuse between encryption and signature is a known security weakness. With the new PQC KEM algorithms, which simply cannot be used to sign messages, it also becomes technically necessary to separate signature keys from encryption keys.

6 Signature and Certificate standards

This section explains how various signature and certificate standards are affected by the introduction of post-quantum signature algorithms explained in Section 3.3.

6.1 CMP and other certificate management protocols

There are multiple certificate management protocols in use. Certificate Management Protocol (CMP) is a versatile standard which can be used for managing both trust anchors and enrolling end entity certificates. Entities communicating with the Certificate Authority (CA) can be authenticated by multiple different mechanisms, including cryptographically by using a certificate from another PKI.

Automated Certificate Management Environment (ACME) and Simple Certificate Enrolment Protocol (SCEP), as well as Enrollment over Secure Transport (EST) which builds on SCEP, are more focused on settings that are specific to the webPKI use case. For example, in ACME, enrolment requests can be authenticated by demonstrating control of a DNS name. However, the expectation is that end entities would not have an identity from another PKI they could authenticate with. Furthermore, there is no globally trusted registration authority that could identify the certificate requestor reliably to the CA. SCEP is inherently tied to RSA and how it functions. EST is an extension of SCEP.

CMP has support for PQC algorithms. The relevant standards are the previous version RFC 4210 (CMPv2) now obsoleted by CMPv3, RFC 9483 (2023) for CMP Lightweight Profile, and RFC 9480 (2023) describing CMP Updates that addressed, for example, improvements in cryptographic agility. CMPv3 is specified in RFC 9810, published in 2025. It combines RFC 4210 and RFC 9480 into a self-contained document, and adds support for requesting certificates for KEM keys, where proof of possession cannot be performed by a signature mechanism. Transport protocol issues are delegated to a separate document RFC 6712.

6.2 PKIX and X.509 certificates

X.509 is the name of an ITU-T standard on certificates, which connect a private key to relevant metadata. This metadata includes representation of an identity, and it describes ways to identify the key holder through a public key certificate signed with a certificate authority. A certificate can, for example, identify the key holding entity's email address, DNS name, IP address, given name, surname and title, or LDAP resource pointer. Additionally, a certificate can specify what it is allowed to be used for. For example, possible uses are digital signatures in general or specifically signing other certificates or signing certificate revocation lists, the latter in the case of a certificate authority's own certificate. The IETF's Public-Key Infrastructure (X.509) (PKIX) working group has

[7] Technically, what is agreed on is secret input used to derive the symmetric key. Additional inputs are allowed.

adapted the standard definition, and usually when speaking of X.509 the standard discussed is, in fact, RFC 5280 and not the ITU standard.

X.509 certificates can be issued for both PQC signature algorithms and KEM algorithms. There are a few different proposals for hybrid certificates, varying in goals. Some focus on backward compatibility, ensuring that a certificate is able to introduce an additional PQC signature, while an old implementation is still able to ignore the new parts that it does not understand. In practice, this kind of approach may not add security against the quantum threat. Other initiatives focus on introducing algorithms into the certificate's algorithm identifier, public key and signature fields that contain in fact two algorithms in once. For example, there could be a concatenated ECC and ML-DSA key, signature and an identifier pointing out which combination it is the bits should be interpreted as.

Hybrid X.509 certificates and their use is still at a draft stage, but standalone PQC algorithms can be considered ready for production use in X.509 certificates, as in May 2026.

6.3 OpenPGP

Open Pretty Good Privacy (OpenPGP), described in RFC 9580 [213], is the standard for encrypting and signing data. OpenPGP is designed to provide data confidentiality and integrity for messages and data files. RFC 9580 specifies a range of public key algorithms for encryption and digital signatures, including RSA, Elgamal and modern ECC schemes. OpenPGP establishes Ed25519 and X25519 as the mandatory primitives for digital signature and key exchange, respectively. [213]

In the recent Internet Draft, draft-ietf-openpgp-pqc-17, the protocol integrates several NIST-standardized post-quantum algorithms into its decentralized architecture. For key encapsulation, the draft focuses on ML-KEM , specifically variants like ML-KEM-768 and ML-KEM-1024, to provide quantum-resistant encryption. Regarding digital signatures, it establishes support for ML-DSA (variants 65 and 87) and includes SLH-DSA for high-assurance, hash-based security. These primitives are implemented using a hybrid model, where a post-quantum algorithm is paired with a classical elliptic curve such as Curve25519 or Curve448. [104]

7 PQC in wireless standards

Wireless communications are particularly vulnerable to eavesdropping, or even active attacks, because of radio interfaces. Therefore, encryption and integrity protection mechanisms are already applied in the radio layers, while higher communication layers may be protected by methods discussed in Section 5.

7.1 3GPP

The 3rd Generation Partnership Project (3GPP) is a global organization, set up by regional SDOs, that defines standards for global telecommunications. Each release from 3GPP contains a full and stable set of technical specifications that allow manufacturers and operators to build networks and devices that actually are able to communicate with each other.

In September 2025, 3GPP announced that Release 19 is being finalized until December 2025 [1]. Rel-19 included specifications related to 5G. Plans for Rel-20 include 5G Advanced track and immediate commercial needs for 5G, which will function as a bridge towards 6G. The timeline for 6G and Rel-21 will be decided in June 2026.

Regarding PQC, 3GPP is currently working on Technical Report *TR 33.703 V0.4.0* with the title "Study on Transitioning to Post Quantum Cryptography (PQC) in 3GPP" [2]. In this document, they

- Study on the impact of using hybrid and standalone PQC algorithms in 3GPP procedures,e.g., existing security protocols used by 5G specifications,
- Studies the suitability of classes of post-quantum signature algorithms (e.g., lattice-based, hash-based) to 3GPP procedures.
- Study on migration of security protocols including COSE, IKEv2, JWE, JWS, MIKEY-SAKKE, SUCI, TLS 1.2, TLS 1.3.

Table 3: Where Post-Quantum Cryptography Matters in Mobile Networks

Area	Description	Classical Crypto Used	PQC Relevance
AKA Protocol (Subscriber authentication)	Mutual authentication between UE and network using SIM-based credentials	MILENAGE (symmetric), EAP-AKA', SHA-2	Not an immediate PQ risk (symmetric crypto is quantum-resistant)
5GC Network Functions	Service communication between 5G Core NFs (e.g., AMF, SMF) uses HTTPS	ECC-based TLS, RSA certs, SHA-2	High relevance: Core signaling and API comms must migrate to PQ-safe TLS
eSIM and SIM Credential Provisioning	Secure credential provisioning over-the-air to embedded SIMs	RSA, ECC (e.g., 2048-bit RSA, P-256 ECC)	Critical long-term key confidentiality risk — must move to PQC for provisioning flows
VPN in Core and RAN	Used in backhaul and intra-network tunnels (esp. for small cells, MEC)	IPsec, IKEv2 with RSA/ECC, AES, SHA-2	Migration to hybrid or PQC-safe IKE needed; ML-KEM key exchange under consideration
Roaming and Interconnection	GRX and IPX networks depend heavily on TLS and IPsec (long persistence tunnels between operators)	ECC-based TLS, IPsec	High relevance: Migration to PQ-safe TLS is necessary

3GPP is considering PQC update of protocols under two titles: by 3GPP and by other Standards Development Organizations (SDOs), e.g., IETF.

7.2 ETSI

European Telecommunications Standard Institute (ETSI) is a non-profit organization that has more than 900 member organizations worldwide. ETSI develops globally recognized technical standards for information and communications technology, including 5G, network function virtualization and SIM cards.

In 2020, they published a technical report ETSI TR 103 619 [50] that establishes migration strategies to quantum safe schemes and related recommendations. They introduce 3 stages in this approach: (1) inventory compilation, (2) preparation of the migration plan, and (3) migration execution, as well as describe the activities that fulfill these stages.

After establishing migration strategies, several technical reports have appeared focusing on quantum-safe key exchanges, signatures, public key operations, and hybrid schemes. Then, ETSI published the first PQC-related standard TS 104 015 V1.1.1 [48], which has the title "Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies". The standard is designed to guarantee the protection of critical data and communications in the quantum-enabled future. Another standard TS 103 744 V1.2.2 [52] is published with the title "Quantum-safe Hybrid Key Establishment". This document includes a framework for hybrid key establishment that combines classical cryptographic methods with post-quantum algorithms.

The full list of PQC-relevant technical standards and technical reports published by ETSI is as follows:

- **GR QSC 001 V1.1.1 (2016) [51]**: Quantum-safe algorithmic framework
- **TR 103 570 V1.1.1 (2017) [53]**: Quantum-Safe Key Exchanges
- **TR 103 616 V1.1.1 (2021) [55]**: Quantum-Safe Signatures
- **TR 103 619 V1.1.1 (2020) [50]**: Migration strategies and recommendations to Quantum Safe schemes
- **TS 103 744 V1.2.2 (2026) [52]**: Quantum-safe Hybrid Key Establishment

- **TR 103 823 V1.1.2 (2021) [54]**: Quantum-Safe Public-Key Encryption and Key Encapsulation
- **TR 103 966 V1.1.1 (2024) [47]**: Deployment Considerations for Hybrid Schemes
- **TR 104 005 V1.2.1 (2026) [49]**: Impacts of the post-quantum cryptography on ETSI TC Secure Element Technologies (SET) specifications
- **ETSI TS 104 015 V1.1.1 (2025) [48]**: Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies

7.3 GSMA

The Global System for Mobile Communications Association (GSMA) is a global organization that represents the interests of mobile network operators and the mobile ecosystem. GSMA participates in establishing technical standards for mobile networks and devices, e.g., 5G and SIM cards, and advocating policy and regulations for mobile innovations. GSMA gathers a list of countries and their PQC activities, especially in the Telco sector [75]. This list includes, for each country, the PQC algorithms they consider, the name of the published guidance, and their timeline for PQC transfer.

GSMA also plays an important role in determining the impact of post-quantum cryptography in telecommunication networks, managing risks related to the PQC environment, defining use cases, and developing quantum-safe/post-quantum cryptography for different use cases, e.g., 4G/5G roaming, IoT ecosystems, and non-terrestrial networks. The full list of PQC related documents published in GSMA is as follows:

- **PQ.01 (2023) [76]**: Post Quantum Telco Network – Impact Assessment
- **PQ.02 (2023) [70]**: Guidelines for Quantum Risk Management for Telco
- **PQ.03 (2024) [71]**: Guidelines for Telecom Use Cases
- **PQ.04 (2025) [74]**: Post Quantum Cryptography in IoT Ecosystem
- **PQ.05 (2025) [77]**: Quantum-safe Cryptography for 4G and 5G Roaming
- **PQ.07 (2026) [72]**: Post Quantum Cryptography for Non-Terrestrial Networks.

7.4 ATIS

The Alliance for Telecommunications Industry Solutions (ATIS) is a standards organization for the North American ICT industry that identifies and proposes technical solutions. ATIS views the emerging quantum computer as a significant threat to current encryption; thus, ATIS has formulated a research and implementation strategy focused on PQC transition. [8]

The core of ATIS's mission lies in the development of the Open Quantum Safe - Test Framework (OQS-TF) which is an open-source project aimed at estimating PQ algorithms' effectiveness in realistic conditions. As PQ algorithms tend to be more resource-heavy than the classical ones, there is a potential risk of existing telecom hardware causing system failures. A central component of the OQS-TF is the Qujata Project which is a specialized testbed for benchmarking and analyzing the performance metrics including CPU and memory usage, connection establishment time, and post-connection download speeds, on different hardware, virtualized infrastructures, and operating systems. [7, 83]

ATIS leads the Quantum Safe Communications and Information Initiative (QSCII) Working Group and coordinates with the main technology stakeholders, including AWS, Cisco, IBM, and Microsoft, to form a unified transition strategy. By establishing this strategic initiative, ATIS ensures that cryptographic updates across various cloud and hardware vendors remain interoperable, preventing network fragmentation during the migration process. [83, 7]

To resolve the complexity of the PQC transition, ATIS advocates the use of a Cryptographic Bill of Materials (CBOM). Although general-purpose CBOM schemas typically catalog high-level application cryptography (such as TLS/SSL), they often lack the granularity to document domain-specific protocols such as 5G-AKA, PRINS, and MILENAGE. Furthermore, ATIS's initiative extends the CycloneDX foundation to account for cryptographic operations offloaded to specialized hardware, including Hardware Security Modules (HSMs) and Trusted Platform Modules (TPMs). [6]

7.5 ITU-T

International Telecommunication Union Standardization Sector (ITU-T) has established a work item whose aim is to produce a technical report "Guidance on use of advanced cryptography based on Post Quantum Cryptography (PQC)"[90]. The report is scheduled to be finished by June 2026. As the title suggests, the report provides guidance on the construction and implementation of PQC-based cryptography in emerging environments such as Beyond 5G.

7.6 ORAN Alliance

The Open Radio Access Network Alliance (O-RAN Alliance) represents a worldwide community of mobile network operators, vendors and academia. Their work strives to create an open environment enabling network elements to integrate easily and effectively, which will improve overall efficiency and innovation in the Radio Access Network (RAN). [159]

In addition, O-RAN Alliance's next Generation Research Group (nGRG) is conducting surveys in order to assess the state of quantum security in the industry and prepare for 6G networks. In the process, they have noticed that majority of the existing protocols and interfaces make use of certificate-based authentication and key agreement based on classical public-key algorithms. Their research suggests the necessity of transitioning to quantum-safe technologies in regard to O-RAN interfaces such as C/U/S and M-Plane, A1, O1, O2, R1, and E2. This is because the security for all mentioned interfaces relies on mTLS, IPsec and 802.1X certificate-based authentication that allow for establishing a secure communication between the Service Management and Orchestration (SMO) layer, the Radio Intelligent Controllers (RIC), and other network elements. [18]

Moreover, O-RAN Alliance also focus on automated management frameworks and software lifecycle procedures that depend on public key infrastructures. They mention protocols such as SZTP, BRSKI, and ACME, as well as software signing and the enrollment of xApps/rApps. Furthermore, they emphasize the potential for cryptographic agility and the use of hybrid X.509 certificates that integrate classical and quantum resistant algorithms to transition towards quantum-safe systems. [18]

8 PQC in Messaging

This section delves into the Signal Protocol, which is the industry leader in secure messaging and its integration into PQC. The Signal Protocol [194] is a cryptographic framework that provides end-to-end encryption for platforms such as WhatsApp, Google Messages, Facebook Messenger, and Skype. It was originally developed by Open Whisper Systems in 2013 and has now evolved to include a hybrid PQC approach. The first element of this upgrade is Post-Quantum Extended Diffie-Hellman (PQXDH), which is a hybrid handshake designed for asynchronous settings. PQXDH derives a shared secret by combining classical ECDH (using either Curve25519 or Curve448) with the PQ CRYSTALS-KYBER-1024 algorithm. The design of the protocol requires both components to work flawlessly, essentially creating a "logical AND" design. For an adversary to compromise the resulting secret key, breaching both the classical Gap Diffie-Hellman and the MLWE problems is a prerequisite [105].

Despite maintaining forward secrecy in the upgraded protocol, PQXDH yet relies on the XEdDSA signature scheme and the discrete logarithm problem (DLP) for mutual authentication and identity binding. For this reason, its PQ security is IND-CCA. Furthermore, the encryption of the initial message employs an AEAD scheme that meets the requirements of both IND-CPA and INT-CTXT. For maintaining forward secrecy even while a recipient is offline, it utilizes **one-time pqkem prekeys** that are published to a server and deleted immediately after a session is established. In the worst case, when a server runs out of these one-time keys, it uses a **Last-Resort pqkem prekey**, which is a reusable PQ key that ensures that the session can still be established with quantum resistance, albeit with reduced forward secrecy for that specific handshake [105].

To keep the conversation secure after the first connection is made, Signal introduced the Sparse Post-Quantum Ratchet (SPQR), which evolves the system into a Triple Ratchet. This architecture functions by combining the existing symmetric Hash Ratchet and classical Diffie-Hellman Ratchet with the new SPQR component, mixing their respective outputs through a hybrid Key Derivation Function (KDF). While the classical Double Ratchet provides healing through elliptic curves, SPQR guarantees quantum resistant Forward Secrecy and Post Compromise Security by mixing ML-KEM secrets into the key stream. SPQR utilizes the ML-KEM Braid protocol to

mitigate latency caused by the larger size of PQ keys [190]. This protocol functions as a Sparse Continuous Key Agreement (SCKA) for breaking high bandwidth cryptographic material into smaller chunks using erasure coding. By treating the communication channel as a stream of capacity, the protocol braids these fragments into regular outgoing messages over time. In this way, the recipient can reconstruct the full PQ key once any necessary subset of chunks is received, regardless of message loss or reordering. [193]

Technically, the Braid protocol leverages an incremental interface to transmit the encapsulation key vector and the ciphertext in parallel, which helps to significantly reduce the time needed for a session to heal from potential compromise. To ensure integrity during this gradual exchange, the protocol includes an internal ratcheted authenticator that provides standalone authenticity for every epoch. [193]

9 Role of PQC in OT standards

There is a trend for increased synergy between operational technology (OT) and information technology (IT), especially due to addition of Internet access to various machines and OT systems.

The most important affected standards on this domain are listed in the following:

1. ISA/IEC 62443– Industrial Automation and Control Systems Security for industries like manufacturing, energy, and transportation [46, 87].

   Scope: Comprehensive security for industrial automation and control systems (IACS), covering asset owners, system integrators, and component/product suppliers.

   Key components: Identification and authentication, use control, system integrity, data confidentiality, and timely response to events.

   PQC Impact: IEC 62443 does not inherently include PQC algorithms. Organizations need to transition to PQC to ensure that their systems remain secure against future quantum attacks, e.g., migrate from RSA and ECC to PQC-safe algorithms.

2. IEEE 802.1X [109] / IEEE 802.1AR [110]– Device Authentication and Identity.

   Scope: IEEE 802.1X aims to provide compatible authentication, authorization, and cryptographic key agreement mechanisms to support secure communication between devices connected by IEEE 802 Local Area Networks (LANs), specifying a general method for the provision of port-based network access control. IEEE 802.1AR specifies Secure Device Identifiers (DevIDs) for use with IEEE 802.1X and other industry standards and protocols that authenticate, provision, and authorize communicating devices.

   Key components: Public Key Infrastructure (PKI) such as RSA and ECC, X.509 certificate.

   PQC Impact: 802.1AR and 802.1X do not inherently include PQC algorithms. Organizations need to transition to PQC to ensure that their systems remain secure against future quantum attacks, e.g., migrate from RSA and ECC to PQ-safe algorithms.

3. NIST SP 800-82 (Guide to Operational Technology (OT) Security) [201].

   Scope: The purpose of this document is to provide guidance for establishing secure operational technology (OT) while addressing OT's unique performance, reliability, and safety requirements.

   OT encompasses a broad range of programmable systems and devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems (ICS), building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

   Key components: NIST supported digital signature schemes, DSA, ECDSA, and RSA, public key infrastructure for key exchange, VPN protocols supported by TLS, SSH, and IPsec.

   PQC Impact: NIST SP 800-82 does not inherently include PQC algorithms. However, the standard suggests NIST-supported signature schemes and public key infrastructures, which rank PQC readiness higher.

4. IEC 62351 (Security for Power System Communications) [89, 85]

   Scope: IEC 62351 is the current standard for security in energy management systems and on associated data exchange. The series addresses system architecture and describes measures that can be applied to commonly used protocols to comply with the four major requirements for secure data communications/data processing: confidentiality, data integrity, authentication, and non-repudiation.

   Key components: TLS, PKI (signatures, key generation), X-509, VPN

   PQC Impact: IEC 62351 does not inherently include PQC algorithms. Organizations need to transition to PQC to ensure that their systems remain secure against future quantum attacks, e.g., migrate from ECC to PQ-safe algorithms.

5. NERC CIP (Critical Infrastructure Protection)

   Scope: The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards is a set of regulatory cybersecurity requirements designed to secure the assets critical to the reliability of the North American bulk electric system (BES).

   Key components: The standards require implementation of confidentiality and integrity protections (including encryption). However, the standards do not specify protocols or cryptography primitives. This gives flexibility to adopt industry-accepted cryptography (e.g., TLS, IPsec, PKI).

   PQC Impact: NERC CIP does not inherently include PQC algorithms. Organizations need to transition to PQC to ensure that their systems remain secure against future quantum attacks, e.g., migrate from ECC to PQ-safe algorithms.

6. TLS and SSH Use in OT Protocols: OPC UA (Unified Architecture) [162], Modbus Security Protocol [130], and DNP3 [41].

   Scope: The **OPC** Unified Architecture (UA) is a platform independent service-oriented architecture that integrates all the functionality of the individual OPC Classic specifications into one extensible framework. This multi-layered approach accomplishes the original design specification goals of functional equivalence, platform independence, security, extensiblity, and comprehensive information modeling.

   The **Modbus/TCP** Security protocol provides protection through the blending of Transport Layer Security (TLS) with the traditional Modbus protocol. TLS encapsulates Modbus packets to provide authentication and message-integrity protection. The new protocol also leverages X.509v3 digital certificates for authentication of the Server and Client. The new Modbus Security protocol uses port 802.

   The **DNP3** aims to achieve open, standards-based Interoperability between substation computers, RTUs, IEDs (Intelligent Electronic Devices) and master stations (except inter-master station communications) for the electric utility industry.

   Key components: TLS and SSH are widely used in these protocols. So, PKI encryption, symmetric encryption, digital signatures, and certificates.

   PQC Impact: These protocols will require updates to their underlying cryptographic libraries to incorporate PQ-safe algorithms.

7. Open DeviceNet Vendors Association (ODVA) [160] is a standards development organization and membership association gathering leading industrial automation companies.

   Scope: ODVA is mainly focusing on Common Industrial Protocol (CIP) and CIP Security defines the security related requirements and capabilities of CIP devices [161].

   Key components: CIP Security ensures the security of their devices by using IETF-defined TLS and DTLS protocols. End point authentication is ensured via X.509 certificates or pre-shared keys.

   PQC Impact: ODVA does not inherently include PQC algorithms. However, the use of TLS and X.509 would indirectly ensure their transition to PQC.

8. PROFIBUS & PROFINET International (PI) [173] is providing a networking environment for the companies and experts in the field of industrial communication, so that the collaboration of the member companies would become standards, which leads to innovative products and automation solutions.

Scope: IEC 62443 standard for industry security is the basis of PI's security [174]. For wireless transmission, IEEE 802.11 provides the security measures for ProfiSAFE networks [172], where PROFIsafe is an International Standard IEC 61784-3-3.

Key components: Identification and authentication, use control, system integrity, data confidentiality, and timely response to events.

PQC Impact: PI does not include PQC algorithms in their systems currently. Organizations need to transition to PQC to ensure that their systems remain secure against future quantum attacks, e.g., migrate from ECC to PQ-safe algorithms.

Table 4: Operational Technology (OT) Standards and Post-Quantum Cryptography

Specifications/ Protocols	**Use in OT**	**Current Crypto Algorithms / Security Protocols**	**PQC Replacements (NIST Candidates)**
IEC 62443	ICS security, secure device communications	RSA, ECC (ECDSA, ECDH), AES	ML-KEM (key exchange), ML-DSA (signatures), AES (unchanged)
IEEE 802.1AR / 802.1X	Secure device identity, Port-based network access control	RSA signatures, ECDSA, X.509 certificates	ML-DSA (certificate signatures), ML-KEM (key exchange)
NIST SP 800-82	Establishing secure OT	TLS (RSA/ECC digital signatures and key exchange), SSH, VPN, IPsec protocols	ML-KEM (key exchange), ML-DSA (signatures), Hybrid TLS
IEC 62351	Secure energy management systems, secure data exchange	PKI (digital signatures and key exchange), TLS, VPN, X.509 certificates	ML-KEM (key exchange), ML-DSA (signatures), Hybrid TLS
NERC CIP	Critical infrastructure protection (Bulk Electric System (BES))	TLS, SSH, VPNs, digital signing	ML-KEM (VPN/TLS), ML-DSA (code signing)
OPC UA	Platform independent service-oriented architecture	TLS (RSA/ECC digital signatures, key exchange), SHA-2	ML-DSA (certs), ML-KEM (session keys), SHA-3 (hashes)
Modbus Security	Security protocol that blends TLS with the traditional Modbus protocol	TLS (RSA/ECC digital signatures, key exchange), SHA-2	ML-DSA (certs), ML-KEM (session keys), SHA-3 (hashes)
Secure DNP3	Interoperability between electric utility industry	TLS (RSA/ECC digital signatures, key exchange), SHA-2	ML-DSA (certs), ML-KEM (session keys), SHA-3 (hashes)

10 Other Sectors Impacted by Post-Quantum Cryptography (PQC)

Table 5: Sectors Beyond IT, Wireless, and OT That Should Care About PQC

Sector	Why PQC Matters	At-Risk Assets	Recommended PQC Actions
Finance and Banking	Secure transactions, digital signatures, and long-term confidentiality	TLS certificates [45], smart-cards [28]	Adopt hybrid key exchange, implement small PQ signature scheme [28]
Cloud and Data Storage	Long-term confidentiality of stored and in-transit data	Encrypted backups [43], KMS keys, Secret Manager secrets, TLS session keys[12]	Upgrade TLS [43], Deploy hybrid PQC, FIPS-validated libraries that include PQC [12]
Healthcare and Medical Devices	Protection of PHI, secure diagnostics, and device firmware	EHR access [4]	Combine blockchain with PQC[4]
Space and Satellite Communications	Long mission lifetimes with limited update capabilities	Telemetry, control signals[29], firmware integrity	Adopt PQC algorithms, Incorporate PQC into satellite communication standards (ETSI, CCSDS)
Automotive and Transportation	Secure connected vehicle communication, OTA updates, and digital keys	V2X/V2V/V2I communications[15], EV Charging[101]	Integrate PQC algorithms in connected vehicle communication[15], and OTA update security [31]
Military and National Security	Decades-long confidentiality and integrity of sensitive data	Classified comms, secure boot, battlefield systems	Coordinate PQC Migration Across Allied Militaries[167],
Legal, Archival, and Notarial Systems	Validity of digital signatures and timestamps, trust services[107]	Intellectual property filings, Strong authentication[107]	Adopt PQC-safe signature standards as a recommended practice.
Blockchain and Cryptocurrencies	Protection of wallets, transaction signatures, and consensus	ECC keys, smart contracts [117], concensus mechanism	Use PTPKH, PQC-friendly protocol forks[117]
Industrial IoT (Beyond OT)	Secure communication and device identity in lightweight devices	Sensors, actuators[112], firmware signatures [154]	Integrate PQ algorithms (Dilithium5, Falcon1024)[154],Optimize PQC for performance, memory, energy[112]

- PHI – Protected Health Information
- V2I – Vehicle-to-Infrastructure
- OTA – Over-The-Air
- PTPKH/P2PKH - Pay-To-Public-Key-Hash
- CCSDS - Consultative Committee for Space Data Systems

10.1 Finance and Banking

The modern fintech landscape relies on asymmetric cryptography like RSA and ECC, to verify authenticity of the card. Since offline transactions are dependent on traditional public-key cryptography, these transactions are at risk. The quantum adversary could obtain private keys to create digital duplicates that local terminals cannot detect. The authors of [28] proposed migrating to hybrid protocols which can provide a "safety net" against the immaturity of post-quantum algorithms. The empirical results showed the huge performance drop when using the post-quantum digital signatures and certificates, since they are too large for the 256-byte limit of standard banking commands, and have heavy computational power and memory consumption. To overcome this challenge and maintain Europay, Mastercard, and Visa (EMV) reliability, the authors of [28] redesigned a protocol such that heavy signature schemes are replaced with KEM such as CRYSTALS-Kyber or NTRU.

While these technical redesigns offer a path forward for physical hardware, the broader banking industry remains hesitant to commit to a full-scale migration. According to a survey conducted by the Bank of Finland in 2025, roughly 30 respondents saw the rise of quantum technology as a marginal point to refine the risk assessment and investment opportunities. Nearly half of the respondents hope that quantum technology could enhance fraud detection, model risks simulations and portofolio optimizations. Interestingly, only one-third of the respondents planned to incorporate post-quantum cryptography in the upcoming 3 years, while another one-third of respondents think it would take roughly 5 years or more, and rest of respondents have not planned for migration at all.[197]

This lack of industry-wide urgency is particularly concerning when contrasted with the immediate operational pressures facing banking infrastructure. The Venafi research highlights a critical readiness gap in the financial services regarding three major shifts in digital security. First, introducing 90-day TLS certificate lifespans is creating operational crisis because most banks rely on manual updates and renewing these security IDs five times more often seems to be a bottleneck. The second challenge is the volatile Certificate Authority (CA) market. When major providers like Entrust become suddenly distrusted, thousands of certificates needs to be replaced by banks on short notice and this task has already caused security incidents for 38% of firms. Last, there is the looming threat of quantum computing where 69% of the firms admit that they do not have the inventory of their own encryption keys needed to migrate safely. The proposed solution for three major shifts is the adoption of machine identity automation. This would imply that PQC alone is not enough and without an automated system to manage these identities, even the strongest quantum-resistant cryptography cannot be deployed fast enough to protect a bank. Automation acts as the essential bridge which can provide the crypto-agility required to handle the high volume of 90-day renewals today while ensuring the organization can swap out old encryption for a quantum-safe future.[45, 209]

10.2 Cloud and Data Storage

As of 2026, the intersection of cloud infrastructure and data storage has become the primary battlefield for quantum-readiness. While Cryptographically Relevant Quantum Computers (CRQCs) capable of executing Shor's algorithm are projected for the early 2030s, the threat to existing data assets is immediate. The risk of HNDL attacks is particularly sensitive for cloud-hosted archives, financial records, government assets, and healthcare data, which often carry confidentiality requirements spanning decades. Therefore, the cloud industry, with Cloud Service Providers (CSPs), is shifting from theoretical planning to the active deployment of PQC, motivated by the finalization of NIST standards such as FIPS 203 [131] and FIPS 204 [139]. This transition aims to replace or augment vulnerable RSA and ECC systems with lattice-based and hash-based primitives, ensuring that modern Enterprise-IT data remains resilient against both classical and future quantum adversaries.

To future-proof their data infrastructure, CSPs are executing PQC migration plans, which involve a systematic review of existing assets and data sensitivity to establish a clear, risk-based hierarchy for cryptographic migration. Therefore, among their axes of priorities are divided between data protection: **data at rest**, **data in transit**; **security infrastructure**: **hardware security modules (HSMs)** (e.g., Google Cloud KMS, AWS KMS), **cryptographic libraries**, etc.

Data at rest, such as backups and archives stored on SSDs or cloud drives, face significant risk if it lacks robust encryption like AES-256, which is currently considered quantum-resistant. Meanwhile, data in transit are highly vulnerable, as many standard communication protocols rely on RSA for key exchange; a quantum computer could compromise TLS channels, putting remote access and real-time transfers at risk. Data in use must also be protected to prevent exposure during active processing. As regards Identity and Access Management (IAM), CSPs are gradually migrating their "Root of Trust" and CAs to use ML-DSA for signing tokens and identity certificates.

Finally, with performance considerations introduced by PQC algorithms (i.e., larger key and signature sizes, computational resource requirements), TLS handshakes and cryptographic operations may experience modest increases in latency and CPU utilization. These costs might influence pricing models for managed cryptographic services such as Cloud KMS. In the following, we will focus on key functional migration steps of major cloud stakeholders with regards to standardized PQC algorithms.

10.2.1 Google Cloud

Google has deployed ML-KEM (FIPS 203) in parts of its infrastructure. Network Encryption (Data in Transit): Internal Google traffic and Google Cloud network encryption now use ML-KEM for key exchange. Google services and Google Cloud-native services are protected by default when traffic uses Google Cloud's internal networking encryption layer [170].

In Cloud KMS, ML-DSA (FIPS 204) and SLH-DSA (FIPS 205) [149] are available in Public Preview for software-backed keys. Integration with Cloud HSM is underway, with Google's collaboration with hardware vendors to support these algorithms in FIPS 140-3 validated hardware modules. Furthermore, Google is migrating public API endpoints to hybrid TLS (1.3) key exchange that incorporates ML-KEM (FIPS 203), to protect client-to-cloud communications against HNDL attacks. Google is working to integrate ML-DSA into its internal PKI infrastructure.

Google Chrome Desktop started experimenting with hybrid post-quantum key exchange. It emphasizes Hybrid Cryptography as the 'safer' appoach for the transition period. It deploys hybrid cryptography combining classical algorithms (such as RSA or ECDSA) with PQ algorithms. Their hybrid constructions are designed so that the system remains secure as long as at least one of the algorithms remains secure.

Finally, Google promotes Crypto-Agility through its open-source tools: Tink (to provide HPKE), BoringCrypto Module (BCM) an open-source FIPS-validated crypto library (FIPS 140-3 CAVP [8], 3 validated assets) [156, 208].

10.2.2 Amazon Web Service (AWS)

Through the AWS Shared Responsibility Model for cloud security, the transition to PQC is a shared effort between AWS and customers [124]. AWS will deliver PQC to hardware, software, networking, and other facilities that run AWS Cloud services. Meanwhile, IaaS instances are under the responsibility of customers, and hence any PQC migration is the sole responsibility of the client. Such responsibility covers, among other things, customer control of their data encryption schemes, using appropriate IAM tools for permissions, etc.

Since 2019, AWS has been deploying different NIST standardized versions of PQC algorithms. It was conducted in their open-source libraries as well as other security-critical services to gradually allow customers for performance testing, e.g., AWS KMS, AWS Secrets Manager, AWS Certificate Manager (ACM) [124]. They defined PQC migration priorities based on customer needs. In their plan, they focus more on encryption for data in transit and less for data at rest. As of today, data at rest in AWS is encrypted using 256-bit symmetric cryptography, which is not at risk for CRQC. Therefore, they do not plan to change their encryption scheme.

Moreover, they advocate for the adoption of the hybrid approach, i.e., Hybrid post-quantum key agreement (combination of ECDH with ML-KEM to encrypt traffic). PQC algorithms are gradually being integrated to public AWS endpoints for customer data encryption. Thus, customers are strongly mandated to migrate to TLS 1.3 as part of their software lifecycle maintenance and vulnerability assessment.

[8] Cryptographic Algorithm Validation Program

Among other tools, their open-source cryptographic libraries are key features that contribute to their roadmap. As of January 2026, AWS has 32 validations of AWS libcrypto (AWS-LC) implementations (FIPS-140-3) including ML-KEM, and ML-DSA [CAVP-AWS]. Their update on s2n-tls implementation depends on IETF standards on TLS adoption of PQC. It will be deployed for use in AWS public endpoints, which include services such as AWS SDK, AWS CLI, SFTP endpoints, server-side TLS termination of workloads (Amazon API Gateway, ELB, etc.).

Another migration strategy of the firm is to provide PQC-based Root of Trust to secure customer software, firmware, and document signing. For instance, AWS KMS integrates ML-DSA to provide long-lived root of trust for code and document signing. In 2026, AWS KMS transitioned to **FIPS 140-3 Level 3** validated HSMs to maintain systems' security throughout their lifetime (i.e., security maintained even in offline systems).

10.2.3 Microsoft Azure

Despite a clear migration strategy, PQC is not yet fully default in Microsoft services. In its migration strategy, Microsoft is taking a hybrid approach combining classical algorithms (e.g., ECDHE) with quantum-safe PQC mechanisms. PQC algorithms (i.e., ML-KEM, ML-DSA) are already available in Windows Server 2025, Windows 11 clients. Moreover, the algorithms are integrated in .NET 10 through the Cryptography API: Next Generation (CNG) libraries and certificate functions (e.g. BCrypt). As of 2026, the company aims for PQC availability in Active Directory Certificate Services (ADCS). SymCrypt open-source crypto library includes OpenSSL implementation with hybrid schemes as per IETF standardization.

10.2.4 Oracle Cloud

Oracle Cloud Infrastructure (OCI) has a large offering of services in government and defense, especially in the US, UK, and Australia [163, 191]. Oracle Cloud aims to provide "Quantum-Safe" architectures by integrating PQC to its core infrastructures. Therefore, they proposed different approaches for *data at rest* and *data in transit* encryptions. For data at rest, AES-256 remains the encryption mechanism for all database features, offering strong protection against both classical and quantum threats. However, future releases will support PQC in database client drivers mainly for developer tools (e.g., SQL with JDBC, SQLcl, ODP.NET, etc.).

Meanwhile, for encrypting data in transit, the goal is to adopt either hybrid key-exchange or full PQC key-exchange. Since 2025, Oracle AI Database 26ai integrates PQC algorithms: ML-KEM for key exchange in TLS 1.3 for both client and server; ML-DSA for signing and verification [187].

As a cryptographic provider, Oracle has ML-KEM and ML-DSA validated implementations through FIPS 140-3 used in their cloud services- Furthermore, its PQC contribution to OpenSSL 3.5, FIPS validated, will be supported in different instances of Oracle Linux running databases and softwares (e.g., servers, cloud infrastructure, and enterprise workloads).

10.3 Healthcare and Medical Devices

Ngwenya et al. [153] published a review paper in February 2026 on post-quantum cryptography for healthcare data protection. In this paper, it is shown that there has been a good deal of study on keeping healthcare-related data secure, the importance of PQC in healthcare, and how to realize the transition to PQC safely and effectively. However, Ngwenya et al. also claim that even though the lattice-based PQC schemes have great promise, deployment readiness remains largely at the conceptual and experimental stage. Real-world implementation validation in a healthcare setting has not been achieved. Similarly, Saberikamarposhti et al. [186] summarize the challenges that post-quantum would bring to healthcare and present a roadmap on how to overcome these challenges along the way.

The latest "HIPAA Privacy Rule To Support Reproductive Health Care Privacy" [38] document published in 2024 by the Department of Health and Human Services (HHS) in the US requires that personal health information needs to be encrypted. Otherwise, the document does not include any information regarding PQC. Regarding security, the latest document on the HHS website, "Omnibus HIPAA Final Rule" [39], was published in 2013 and is still in effect.

In EU, there is also no specific information regarding PQC in healthcare systems. Similarly, GDPR does not mention post-quantum either. However, the NIS cooperation group published an EU roadmap [155] for transitioning to PQC. Since GDPR is intertwined with EU security regulations, it could be expected that PQC would

be brought into line with GDPR. As one of the high-risk use cases, healthcare systems would have an indirect impact.

10.4 Security on Space and Satellite Communications

For decades, space has been considered a safe zone for the operation of scientific instruments, earth observation, and naturally as a communication channel. Safety and security on the space has been mostly focusing on maximizing the success of failure free satellite missions (no break-downs). The second major interest for space mission has been the reliability of electric components in heavy ionizing radiation conditions.

The landscape has changed. This can be seen, for example, by the executive orders already issued in the US [57, 58]. These executive orders set the minimum approval level for computing platforms for systems sold and used on ground and in space. Similar measures are set by European Commission regulations, such as the European Cyber Resilience Act (CRA).

The aforementioned binding guidelines have led to the development of new security schemes, security architectures, security protocols, and semiconductor-products to achieve security goals. Notably, the security goals require protection against quantum computers or benefits from quantum technologies. Protection schemes must include the adoption and deployment of PQC. These requirements are equally needed on ground stations and satellites.

The first pillar to achieve goals is to establish trust in the computing platforms. As the first step, boot-sequences need to be protected with PQC digital signatures. Furthermore, any system update, or upload of external software is required to be verified for integrity and authenticity.

The communication between ground station and satellite and between satellites (Inter Satellite Communications) have been partly protected with cryptographic algorithms. The Consultative Committee for Space Data Systems (CCSDS)[9] produces data-transfer protocols such as SDLS (Space Data Link System) [35]. The series of CCSDS documents describe complete system, intended use, protocol details, lifetime management, etc. Another example of the data-transfer protocol is Bulk Security Standard for Spacecraft Communication [135]. It appears that the CCSDS standardization is widely adopted among space organizations and covers more than end-to-end real-time protocols, for example, BPsec which is a kind of hop-to-hop letter-box protocol. In addition of the space specific protocols, standard data-transfer protocols such as MACsec and IPsec are used in satellite-to-satellite communications and occasionally also between ground-station and satellite.

However, adding PQC support to satellite protocols is a challenge. There are two sides in this challenge: legacy systems, which cannot be updated, and existing or new systems, which can be updated. Naturally, the latter ones are of specific interest. CCSDS is currently updating the SDLS protocol to support PQC algorithms. The transmission of PQC signatures is a challenge because they may not fit in data-transfer frames and some protocols do not support the fragmentation of signature information. Some future satellite constellations may also offer multitenancy, and key-exchange events are more likely to take place for each tenant. For Low Earth Orbit (LEO) satellites, the communication window is approximately 7 minutes between a satellite and a specific ground station, whereas communication windows between satellites may alter from a few seconds to several hours.

A specific ongoing activity is to enable PQC key encapsulation mechanisms for space communication; see, for example, [82]. The new protocol CCSDS is not public and cannot be referenced yet. Quite notably, the CCSDS protocols seem to be the way how space agencies collaborate in the future. In the long run, the SDLS and its future versions will be required by agencies and also system architectures such as SAVOIR.

10.5 Automotive and Transportation

5G Automotive Association (5GAA) has a cooperation agreement with GSMA Post-Quantum Telco Networks (PQTN) Task Force for investigating the impact of quantum computing and migrating to post-quantum cryptography, and they published a statement of intent in March 2025 [3]. Even though there are no standards or specifications yet, the collaboration between the telco and automotive industries aims to strengthen future connected automotive security through PQC and crypto-agility. Quantum threat would cause road user safety issues, such as

[9] https://ccsds.org

- vehicle damage, e.g., overwriting braking software,
- financial damage, e.g., removing theft protection,
- privacy issues, e.g., remote monitoring, and
- operational damage, e.g., deleting software.

These attacks are possible because operations are controlled over the air, relying on traditional cryptography and digital signatures. Especially since vehicle lifetimes are rather long and updating the system is difficult, the use of quantum-vulnerable cryptographic algorithms should be limited in vehicles.

10.6 Military and National Security

According to Parker from RAND Corporation [167] military and national security systems are especially vulnerable to HNDL attacks due to the nature of information exchanged in such systems. On the other hand, lifetime of such systems is typically long, some devices may be in use for decades. Therefore, the U.S. National Security Agency has set exact timelines for PQC transition, with the year 2035 as the last milestone, by when all systems must be quantum-resistant. Interoperability of communication systems between allies is critical. NATO countries France and U.K. have publicly set similar timeline objectives but transition plans are less clear in many European countries.

NSA has clearly stated preference of PQC approach against quantum-based hardware solutions such as Quantum Key Distribution (QKD). An explicitly stated reason is that QKD is anyway just a partial solution against the quantum threat. Other countries, most notably People's Republic of China (PRC) has invested a lot in QKD infrastructure but they advance PQC as well.

10.7 Media Production

As media production transitions toward network-based and cloud-based environments, new standards have emerged for device control, media transmission between devices, and verification of media authenticity. These standards need to be evaluated from the perspective of PQC as they are not directly PQC-oriented

Below is a summary of relevant standards and their associated challenges For media transmission over IP networks, traditional standardized methods have been used, including streaming protocols such as RTP, SRT, RIST, RTSP, HLS, XRTC, and WebRTC, and file transfer protocols such as FTP and HTTP. The SMPTE organization has introduced the ST 2110 standard family for professional audio and video media transport. For Media transfers, exact timing is important and the PTP v2 is generally used in Media production environments.

More and more media production is done in Containerised Cloud environments where media transfer delays play important role. In order to avoid delays, new architectures with Common Memory Sharing have been developed. An example of this is the MXL. MXL refers to the Media eXchange Layer of the EBU (European Broadcasting Union) Dynamic Media Facility (DMF) reference architecture.

Media Device Control typically relies on TCP/IP-based protocols or protocols operating over HTTPS, such as Ember+, which is used for media control, or MQ message queue applications. Advanced Media Workflow Association (AMWA) has developed the Networked Media Open Specifications (NMOS). NMOS is an open-source set of protocols and associated software for discovery, registration, connection, and management of ST 2110 networks. To address the issue of Media Authenticity, the C2PA initiative has been introduced. The Coalition for Content Provenance and Authenticity (C2PA) is a project of the Joint Development Foundation.

10.8 Legal, Archival, and Notarial Systems

One desired property of digital signatures is non-repudiation. Although an overwhelming majority of digital signatures are used for the purpose of authentication only, non-repudiation is still important from a legal point of view. The relevance of authenticity in communication is typically limited in time. After the communication has ended, the attacker cannot interfere with it anymore. The setting is different with documents and files. In many cases, it is important to verify authenticity and integrity of a document years after the document was created. This fact emphasizes the urgency of PQC transition in archival and notarial systems.

In 2024, the EU has published regulation for Electronic Identification, Authentication, and Trust Services 2.0 (eIDAS 2.0). One of the main components of eIDAS is a reusable digital identity that could be used in many different services and digital platforms. Verification of such identities is based on the concept of digital signatures. Another main component of eIDAS is the establishment of trust services. One goal of these trust services is to enable digital signatures that provide a legal equivalent to traditional handwritten signatures [107].

10.9 Blockchain and Cryptocurrencies

According to [19], Google has found out that the elliptic curve protected bitcoin and other cryptocurrencies can be broken, just with less than 500 000 qubits. Quantum attacks in the blockchain and cryptocurrencies field are mainly classified into three categories: on-spend, at-rest and on-setup attacks.

On-spend attack targets the "mempool" where attacker derives a private key and replaces the original transaction with fraudulent one before the actual transaction commit happens. The average block time for Bitcoin is 10 minutes, whereas Google has found that the cracking could take roughly nine minutes. If the cracking is done in parallel, the cracking will be well below the average block time of the Bitcoin. As per CoinDesk [34], attacker will able to perform such attack with nearly 41 % success rate. While Ethereum's and Solana's block time is extremely short, Google claims that cracking them will mostly depend on utilizing faster hardware.

At-rest attack refers to targeting the public keys that are revealed on the blockchain. Since the public keys are stationary, quantum adversary has ample time to derive the private keys by running Shor's algorithm, meaning that dormant wallets and reused addresses are at risk. The third type of attack, on-setup attack is about exploiting a weakness in the protocol to find the "master backdoor". Success in this last type of attack would allow attacker to forge proof or digital signature. [19, 120, 34]

10.10 Industrial IoT (Beyond OT)

The shift toward a quantum-capable era creates a massive surface area for potential exploitation in interconnected industrial systems. The Industrial IoT ecosystem is defined by its diversity, comprising a massive number of interconnected devices across critical sectors like automation, transportation, agriculture, and healthcare. This complexity, combined with the rise of 5G/6G networks and distributed computing, enables unique threats of quantum-capable attackers such as HDNL, or computation hijacking to disrupt critical infrastructures [73].

In order for the IIoT ecosystem to be resilient against the upcoming quantum threats security must be embedded across its entire stack. For instance, the edge device layer requires identity protection, through authentication mechanisms with algorithms such as ML-DSA and SLH-DSA. At the network layer, encryption is necessary for the data in transit. This will be enabled by using PQC-ready gateways, PLCs, and fog devices to encrypt data moving across wireless and wired protocols. In data collection points, it is crucial to ensure databases and cloud repositories utilize quantum-resistant encryption (e.g., ML-KEM) for long-term storage of data at rest.

The transition to PQC presents a barrier for IIoT due to the large increase in public key and ciphertext sizes. Unlike classical cryptography, these larger data structures directly impact bandwidth, storage, and memory usage resources that are scarce in constrained IoT environments.

Meanwhile, the current landscape of PQC standardization reveals a significant gap for IIoT systems. The focus of NIST PQC selection remains primarily on the high-performance requirements for domains like government agencies and tech giants [40, 60]. This top-down approach often overlooks the unique constraints of IIoT, where standardization must prioritize lightweight, resource-efficient options to prevent smaller devices from being excluded from a quantum-safe future. Widespread adoption of PQC in IIoT will require a dual focus on software and hardware optimization, including the integration of GPU acceleration for PQC algorithms to handle the increased computational load without impacting system responsiveness [40].

Many industrial devices have lifecycles spanning many years (often decades) [102]. Therefore, the urgency for PQC migration is critical; a device deployed today without quantum-resistant capabilities might become a point of failure during its operational life in the future. Addressing these performance implications is essential to maintaining the integrity of long-term industrial infrastructure against quantum threats.

11 Summary and Conclusions

This report covers state of PQC standardization in many fronts. After first providing general background on quantum computing, quantum threat and related risks, we discussed crypto-agility and migration strategies, including hybrid approach that combines good properties from classical algorithms and PQC algorithms with the cost of increased complexity. The core of PQC standardization is in NIST competition calls, whose state was covered next. They have been able to produce new standards roughly in the anticipated schedule, although some final specifications have been delayed. Selected algorithms have bias towards security based on hardness of structured lattice problems, which is why NIST is still looking for new standard signature algorithms. Other SDOs, especially ISO and IETF, have also been active in standardizing PQC algorithms.

Algorithms can seldom be used as such; instead, they act as cornerstones for larger systems. We discuss activities in IETF on bringing popular security protocols, such as TLS and IPsec, to the quantum-resistant era. Then we cover standards devoted for signature systems, followed by wireless systems and OT systems, studying the state of PQC activities in each sector. Finally, state of PQC migration in several other critical industry sectors, such as cloud or finance, is discussed. The key learning is that PQC migration contains much more than just simple replacement of old algorithms with new ones.

Disclaimer

Generative AI has been used in the creation of author tables 1, abbreviations 2 and summary tables 3, 4, 5 in this document and to refine the linguistic precision. All content has been reviewed and edited by experts.

References

[1] 3GPP. "Plenary progress on Rel-19 freeze". In: *3GPP News* (2025). Last Accessed: 2026-03-05. URL: https://www.3gpp.org/news-events/3gpp-news/plenary109.

[2] 3GPP. *Study on Transitioning to Post Quantum Cryptography (PQC) in 3GPP*. Technical Report TR 33.703 V0.4.0. 3GPP, 2026.

[3] 5G Automotive Association. *Statement of Intent on the Quantum Threat and Mitigation Strategies for the Automotive Industry*. Joint Statement. Munich, Germany: 5GAA Automotive Association, 2025.

[4] Seun Adeoye. "Blockchain-Enabled, Post-Quantum Cryptographic Framework for Securing Electronic Health Records: A Next-Generation Approach to Healthcare Data Protection". In: *Cognizance Journal of Multidisciplinary Studies* 5 (Apr. 2025), pp. 77–104. DOI: 10.47760/cognizance.2025.v05i04.006.

[5] Aikata Aikata, Ahmet Can Mert, David Jacquemin, Amitabh Das, Donald Matthews, Santosh Ghosh, et al. "A unified cryptoprocessor for lattice-based signature and key-exchange". In: *IEEE Transactions on Computers* 72.6 (2022), pp. 1568–1580. DOI: 10.1109/TC.2022.3215064.

[6] Alliance for Telecommunications Industry Solutions. *Preparing Telecom for the Quantum-Safe Future: Why a Telecom-Specific CBOM Matters*. https://atis.org/preparing-telecom-for-the-quantum-safe-future-why-a-telecom-specific-cbom-matters/. Last Accessed: 2026-03-25.

[7] Alliance for Telecommunications Industry Solutions. *QSCII Open Source PQC Test Framework*. https://atis.org/initiatives/quantum/qscii-open-source-pqc-test-framework/. Last Accessed: 2026-03-25.

[8] Alliance for Telecommunications Industry Solutions. *Quantum*. https://atis.org/initiatives/quantum/. Last Accessed: 2026-03-25.

[9] Nouri Alnahawi, Nicolai Schmitt, Alexander Wiesmaier, Andreas Heinemann, and Tobias Graßmeyer. "On the state of crypto agility". In: *Tagungsband zum* 18 (2022). Last Accessed: 2026-01-12, pp. 103–126.

[10] Joël Alwen, Sandro Coretti, and Yevgeniy Dodis. "The double ratchet: security notions, proofs, and modularization for the signal protocol". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2019, pp. 129–158. DOI: 10.1007/978-3-030-17653-2_5.

[11] Alessandro Amadori, Thomas Attema, Maxime Bombar, João Diogo Duarte, Vincent Dunning, Simona Etinski, et al. *The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography*. Technical Report. TNO, CWI, and AIVD, Dec. 2024.

[12] Amazon Web Services. *Post-Quantum Cryptography*. Last Accessed: 2025-09-08. URL: https://aws.amazon.com/security/post-quantum-cryptography/.

[13] Analog Devices. *IEC (International Electrotechnical Commission)*. https://www.analog.com/en/resources/glossary/iec.html. Last Accessed: 2026-03-22.

[14] ANSSI. *ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)*. Technical Report. Agence nationale de la sécurité des systèmes d'information (ANSSI), Dec. 2023. URL: https://messervices.cyber.gouv.fr/guides/en-follow-position-paper-post-quantum-cryptography.

[15] Apriorit. *Post-Quantum Cryptography in Automotive*. Last Accessed: 2025-09-08. URL: https://www.apriorit.com/dev-blog/post-quantum-cryptography-in-automotive.

[16] Nicolas Aragon, Paulo L. Barreto, Slim Bettaieb, Loı c Bidoux, Olivier Blazy, Jean-Christophe Deneuville, et al. *BIKE: Bit Flipping Key Encapsulation*. Last Accessed: 2026-02-20. URL: https://bikesuite.org/.

[17] Nicolas Aragon, Philippe Gaborit, and Gilles Zémor. *HQC-RMRS, an instantiation of the HQC encryption framework with a more efficient auxiliary error-correcting code*. 2020. arXiv: 2005.10741 [cs.CR]. URL: https://arxiv.org/abs/2005.10741.

[18] Swaminathan Arunachalam, Alex Reznik, Aritra Banerjee, Clifton Fernandes, Prabhu K, Raghavendran Ramiya, et al. *Research Report on Quantum Security*. Research Report RR-2023-04. Version 1.1. O-RAN next Generation Research Group (nGRG), Sept. 2023. URL: https://mediastorage.o-ran.org/ngrg-rr/nGRG-RR-2023-04-Quantum-Security-v1_1.pdf.

[19] Forbes Digital Assets. *Google Finds Quantum Computers Could Break Bitcoin Sooner Than Expected*. Last Accessed: 2026-04-01. Mar. 2026. URL: https://www.forbes.com/sites/digital-assets/2026/03/31/google-finds-quantum-computers-could-break-bitcoin-sooner-than-expected/.

[20] ATIS. *Strategic Framework for Crypto Agility and Quantum Risk Assessment*. Tech. rep. Last Accessed: 2025-12-30. Alliance for Telecommunications Industry Solutions, 2024. URL: https://atis.org/resources/strategic-framework-for-crypto-agility-and-quantum-risk-assessment/.

[21] Jean-Philippe Aumasson, Daniel J. Bernstein, Ward Beullens, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, et al. *SPHINCS+: Stateless Hash-Based Digital Signature Scheme*. Last Accessed: 2026-02-20. URL: https://sphincs.org/.

[22] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, et al. *CRYSTALS-Kyber: A Post-Quantum KEM*. Last Accessed: 2026-02-20. URL: https://pq-crystals.org/kyber/.

[23] Abdullah Aydeger, Engin Zeydan, Awaneesh Kumar Yadav, Kasun T. Hemachandra, and Madhusanka Liyanage. "Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography". In: *IEEE Xplore* (2024). DOI: 10.1109/NoF62948.2024.10741441.

[24] Elaine Barker, Lily Chen, David Cooper, Dustin Moody, Andrew Regenscheid, Murugiah Souppaya, et al. "Considerations for Achieving Crypto Agility: Strategies and Practices". In: (2025). DOI: 10.6028/NIST.CSWP.39.ipd.

[25] E. Berlekamp, R. McEliece, and H. van Tilborg. "On the inherent intractability of certain coding problems (Corresp.)" In: *IEEE Transactions on Information Theory* 24.3 (1978), pp. 384–386. DOI: 10.1109/TIT.1978.1055873.

[26] Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, et al. *Classic McEliece*. https://classic.mceliece.org/. Last Accessed: 2026-02-20.

[27] Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. "The SPHINCS+ Signature Framework". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS '19. London, United Kingdom: Association for Computing Machinery, 2019, pp. 2129–2146. ISBN: 9781450367479. DOI: 10.1145/3319535.3363229. URL: https://doi.org/10.1145/3319535.3363229.

[28] Luk Bettale, Marco De Oliveira, and Emmanuelle Dottax. "Post-Quantum Protocols for Banking Applications". In: *Smart Card Research and Advanced Applications*. Ed. by Ileana Buhan and Tobias Schneider. Cham: Springer International Publishing, 2023, pp. 271–289. ISBN: 978-3-031-25319-5.

[29] BIS Research. *Cybersecurity in Orbit Empowering the Future of Space and Satellites Security*. Last Accessed: 2025-09-08. May 2025. URL: https://bisresearch.com/insights/cybersecurity-in-orbit-empowering-the-future-of-space-and-satellites-security.

[30] Joppe W. Bos, Joost Renes, and Christine van Vredendaal. "Post-Quantum Cryptography with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen & Nussbaumer". In: *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, Aug. 2022, pp. 3683–3697. ISBN: 978-1-939133-31-1. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/bos.

[31] Abel C. H. Chen and Bon-Yeh Lin. "Hybrid Scheme of Post-Quantum Cryptography and Elliptic-Curve Cryptography for Certificates A Case Study of Security Credential Management System in Vehicle-to-Everything Communications". In: *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)*. Vol. 1. 2024, pp. 426–430. DOI: 10.1109/ICCPCT61902.2024.10673280.

[32] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, et al. *Report on Post-Quantum Cryptography*. NIST Internal Report (NISTIR) 8105. National Institute of Standards and Technology (NIST), Apr. 2016. DOI: 10.6028/NIST.IR.8105. URL: http://dx.doi.org/10.6028/NIST.IR.8105.

[33] NSA CISA. *NIST, "Quantum-readiness: Migration to post-quantum cryptography,"* tech. rep. CISA, Tech. Rep, 2023. URL: https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography.

[34] CoinDesk. *Breaking Bitcoin with quantum may be easier than thought, Google Says*. Last Accessed: 2026-04-01. Mar. 2026. URL: https://www.coindesk.com/markets/2026/03/31/bitcoin-s-taproot-could-make-quantum-attacks-easier-than-expected-new-google-research-says.

[35] Consultative Committee for Space Data Systems. *Space Data Link Security Protocol*. Recommended Standard (Blue Book) CCSDS 355.0-B-2. Consultative Committee for Space Data Systems (CCSDS), July 2022. URL: https://ccsds.org/Pubs/355x0b2.pdf.

[36] David A. Cooper, Daniel C. Apon, Quynh H. Dang, Michael S. Davidson, Morris J. Dworkin, and Carl A. Miller. *Recommendation for Stateful Hash-Based Signature Schemes*. NIST Special Publication (SP) 800-208. Gaithersburg, MD: National Institute of Standards and Technology (NIST), Oct. 2020. DOI: 10.6028/NIST.SP.800-208.

[37] NTT Corporation. *NTRU: Post-Quantum Cryptography*. Last Accessed: 2026-01-14. URL: https://info.isl.ntt.co.jp/crypt/ntru/index.html.

[38] Department of Health and Human Services. *HIPAA Privacy Rule To Support Reproductive Health Care Privacy*. Tech. rep. 45 CFR Parts 160 and 164. 2024.

[39] Department of Health and Human Services. *The Security Rule*. Last Accessed: 2026-03-13. 2022. URL: https://www.hhs.gov/hipaa/for-professionals/security/index.html.

[40] Derek Atkins. *Requirements for Post-Quantum Cryptography on Embedded Devices in the IoT*. Tech. rep. Last Accessed: 2026-03-25. NIST, 2021. URL: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/atkins-requirements-pqc-iot-pqc2021.pdf.

[41] DNP Users Group. *Overview of DNP3 Protocol*. URL: https://www.dnp.org/About/Overview-of-DNP3-Protocol.

[42] Léo Ducas and Thomas Prest. "Fast Fourier Orthogonalization". In: *Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*. ISSAC '16. Waterloo, ON, Canada: Association for Computing Machinery, 2016, pp. 191–198. ISBN: 9781450343800. DOI: 10.1145/2930889.2930923. URL: https://doi.org/10.1145/2930889.2930923.

[43] Sandra Dunbar. *The Post Quantum Cryptography countdown: Why your data's safety net is fraying*. https://www.netapp.com/blog/post-quantum-cryptography-storage-layer/.

[44] *ECMA-424: CycloneDX Bill of Materials Specification*. Defines the CycloneDX v1.7 specification and includes the Cryptography Bill of Materials (CBOM) capability. Ecma International, Dec. 2025. URL: https://ecma-tc54.github.io/ECMA-424/.

[45] Editorial Team. "Financial services not ready for TLS changes and post-quantum crypto". In: *Bobsguide* (2024). Accessed on August 14, 2025. URL: https://www.bobsguide.com/financial-services-not-ready-for-tls-changes-and-post-quantum-crypto/.

[46] Editorial Team of IEC. *Understanding IEC 62443*. 2021.

[47] ETSI. *Deployment Considerations for Hybrid Schemes*. Technical Report ETSI TR 103 966 V1.1.1. ETSI, 2024.

[48] ETSI. *Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies*. Technical Specification ETSI TS 104 015 V1.1.1. France: ETSI, 2025.

[49] ETSI. *Impacts of the post-quantum cryptography on ETSI TC Secure Element Technologies (SET) specifications*. Technical Report ETSI TR 104 005 V1.2.1. ETSI, 2026.

[50] ETSI. *Migration strategies and recommendations to Quantum Safe schemes*. Technical Report ETSI TR 103 619 V1.1.1. ETSI, 2020.

[51] ETSI. *Quantum-safe algorithmic framework*. Group Report ETSI GR QSC 001 V1.1.1. ETSI, 2016.

[52] ETSI. *Quantum-safe Hybrid Key Establishment*. Technical Specification ETSI TS 103 744 V1.2.2. ETSI, 2026.

[53] ETSI. *Quantum-Safe Key Exchanges*. Technical Report ETSI TR 103 570 V1.1.1. ETSI, 2017.

[54] ETSI. *Quantum-Safe Public-Key Encryption and Key Encapsulation*. Technical Report ETSI TR 103 823 V1.1.2. ETSI, 2021.

[55] ETSI. *Quantum-Safe Signatures*. Technical Report ETSI TR 103 616 V1.1.1. ETSI, 2021.

[56] European Commission. *Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. Library Document. Last Accessed: 2026-02-12. European Commission, Directorate-General for Communications Networks, Content and Technology, 2024. URL: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[57] Executive Office of the President. *Strengthening and Promoting Innovation in the Nation's Cybersecurity*. Federal Register. Executive Order 14144, signed January 16, 2025. Jan. 2025. URL: https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity.

[58] Executive Office of the President. *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144*. The White House, Presidential Actions. Executive Order 14306. June 2025. URL: https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/.

[59] Federal Office for Information Security (BSI). *BSI Technical Guideline TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths*. Technical Guideline. Version 2026-01. Bonn, Germany: Federal Office for Information Security (BSI), Jan. 2026. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=7.

[60] Tiago M. Fernández-Caramés. "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things". In: *IEEE Internet of Things Journal* 7.7 (2020), pp. 6457–6480. DOI: 10.1109/JIOT.2019.2958788.

[61] Scott Fluhrer and Ryan Appel. *draft-sfluhrer-ssh-mldsa-05: SSH Support of ML-DSA*. Last Accessed: 2026-03-06. 2026. URL: https://datatracker.ietf.org/doc/draft-sfluhrer-ssh-mldsa/.

[62] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, et al. *Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU*. https://falcon-sign.info/. Last Accessed: 2026-02-20.

[63] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, et al. *Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU*. Last Accessed: 2026-03-25. URL: https://falcon-sign.info/falcon.pdf.

[64] Markus Friedl, Jan Mojzis, and Simon Josefsson. *draft-ietf-sshm-ntruprime-ssh-06: Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512*. Last Accessed: 2026-03-06. URL: https://datatracker.ietf.org/doc/draft-ietf-sshm-ntruprime-ssh/.

[65] Philippe Gaborit, Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loı c Bidoux, Olivier Blazy, et al. *HQC: Hamming Quasi-Cyclic*. Last Accessed: 2026-02-20. URL: https://pqc-hqc.org/.

[66] Philippe Gaborit, Carlos Aguilar-Melchor, Nicolas Aragon, Slim Bettaieb, Loı c Bidoux, Olivier Blazy, et al. *Hamming Quasi-Cyclic HQC*. Tech. rep. Aug. 2025. URL: https://pqc-hqc.org/doc/hqc_specifications_2025_08_22.pdf.

[67] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions". In: *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*. STOC '08. Victoria, British Columbia, Canada: Association for Computing Machinery, 2008, pp. 197–206. ISBN: 9781605580470. DOI: 10.1145/1374376.1374407. URL: https://doi.org/10.1145/1374376.1374407.

[68] Lewis Glabush, Patrick Longa, Michael Naehrig, Chris Peikert, Douglas Stebila, and Fernando Virdia. "FrodoKEM: A CCA-Secure Learning With Errors Key Encapsulation Mechanism". In: *IACR Communications in Cryptology* 2.3 (Oct. 6, 2025). DOI: 10.62056/ayivom2hd.

[69] Lov K. Grover. "A fast quantum mechanical algorithm for database search". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 212–219. ISBN: 0897917855. DOI: 10.1145/237814.237866. URL: https://doi.org/10.1145/237814.237866.

[70] GSMA. *Guidelines for Quantum Risk Management for Telco*. Tech. rep. GSMA-PQ.02. GSM Association, 2023.

[71] GSMA. *Post Quantum Cryptography – Guidelines for Telecom Use Cases*. Tech. rep. GSMA-PQ.03. GSM Association, 2024.

[72] GSMA. *Post Quantum Cryptography for Non-Terrestrial Networks*. Tech. rep. GSMA-PQ.07. GSM Association, 2026.

[73] GSMA. *Post Quantum Cryptography in IoT*. Executive Summary. Feb. 2025. URL: https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2025/02/Post-Quantum-Cryptography-Executice-Summary-Feb-2025-1.pdf.

[74] GSMA. *Post Quantum Cryptography in IoT Ecosystem*. Tech. rep. GSMA-PQ.04. GSM Association, 2025.

[75] GSMA. *Post Quantum Government Initiatives by Country and Region*. Last Accessed: 2026-03-28. 2026. URL: https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/.

[76] GSMA. *Post Quantum Telco Network Impact Assessment Whitepaper*. Tech. rep. GSMA-PQ.01. GSM Association, 2023.

[77] GSMA. *Quantum-safe Cryptography for 4G and 5G Roaming*. Tech. rep. GSMA-PQ.05. GSM Association, 2025.

[78] Keitaro Hashimoto, Shuichi Katsumata, Kris Kwiatkowski, and Thomas Prest. "An Efficient and Generic Construction for Signal's Handshake (X3DH): Post-quantum, State Leakage Secure, and Deniable". In: *J. Cryptol.* 35.3 (July 2022). ISSN: 0933-2790. DOI: 10.1007/s00145-022-09427-1. URL: https://doi.org/10.1007/s00145-022-09427-1.

[79] Julian Hohm, Andreas Heinemann, and Alexander Wiesmaier. "Towards a Maturity Model for Crypto-Agility Assessment". In: *Foundations and Practice of Security*. Ed. by Guy-Vincent Jourdan, Laurent Mounier, Carlisle Adams, Florence Sèdes, and Joaquin Garcia-Alfaro. Cham: Springer Nature Switzerland, 2023, pp. 104–119. ISBN: 978-3-031-30122-3.

[80] Russ Housley. *Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms*. Nov. 2015. DOI: 10.17487/RFC7696.

[81] Andreas Huelsing, Denis Butin, Stefan-Lukas Gazdag, Joost Rijneveld, and Aziz Mohaisen. *XMSS: eXtended Merkle Signature Scheme*. RFC 8391. May 2018. DOI: 10.17487/RFC8391. URL: https://www.rfc-editor.org/info/rfc8391.

[82] Andreas Hülsing, Tanja Lange, and Fiona Johanna Weber. "A Key-Update Mechanism for the Space Data Link Security Protocol". In: *Cryptology and Network Security – CANS 2025*. Vol. 16351. Lecture Notes in Computer Science. Springer, 2026, pp. 602–611. DOI: 10.1007/978-981-95-4434-9_29.

[83] Ian Deakin and Carroll Gray-Preston. *Navigating the Quantum Leap: PQC Migration and What It Means for the ICT Industry – ATIS*. Last Accessed: 2025-12-09. URL: https://atis.org/navigating-the-quantum-leap-pqc-migration-and-what-it-means-for-the-ict-industry/.

[84] IBM. *DORA and Your Quantum-Safe Cryptography Migration*. 2024. URL: https://www.ibm.com/think/insights/dora-quantum-safe-cryptography-migration.

[85] IEC Editorial Team. *Cyber security: understanding IEC 62351*. 2023. URL: https://www.iec.ch/blog/cyber-security-understanding-iec-62351.

[86] International Organization for Standardization. *Members*. https://www.iso.org/about/members. Last Accessed: Accessed: 2026-01-14.

[87] International Society of Automation (ISA). *ISA/IEC 62443 Series of Standards - ISA*. 2025. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[88] Internet Engineering Task Force. *Introduction to the IETF*. https://www.ietf.org/about/introduction/. Last Accessed: 2026-03-30.

[89] IPCOMM. *IEC 62351*. 2025. URL: https://www.ipcomm.de/protocol/IEC62351/en/sheet.html.

[90] ITU-T Study Group 17. *Guidance on use of advanced cryptography based on Post Quantum Cryptography (PQC)*. Technical Report XSTR.ac-pqc. The International Telecommunication Union (ITU-T), 2026.

[91] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, et al. *SIKE: Supersingular Isogeny Key Encapsulation*. Last Accessed: 2026-02-20. URL: https://sike.org/.

[92] M. Jones. *JSON Web Algorithms (JWA)*. RFC 7518. May 2015. DOI: 10.17487/RFC7518. URL: https://www.rfc-editor.org/info/rfc7518.

[93] M. Jones, J. Bradley, and N. Sakimura. *JSON Web Signature (JWS)*. RFC 7515. May 2015. DOI: 10.17487/RFC7515. URL: https://www.rfc-editor.org/info/rfc7515.

[94] M. Jones and J. Hildebrand. *JSON Web Encryption (JWE)*. RFC 7516. May 2015. DOI: 10.17487/RFC7516. URL: https://www.rfc-editor.org/info/rfc7516.

[95] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, et al. "Transitioning organizations to post-quantum cryptography". In: *Nature* 605.7909 (2022), pp. 237–243.

[96] Panos Kampanakis, Douglas Stebila, and Torben Hansen. *draft-ietf-sshm-mlkem-hybrid-kex-10: PQ/T Hybrid Key Exchange with ML-KEM in SSH*. Last Accessed: 2026-03-06. URL: https://datatracker.ietf.org/doc/draft-ietf-sshm-mlkem-hybrid-kex/.

[97] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen. *Internet Key Exchange Protocol Version 2 (IKEv2)*. RFC 7296. Oct. 2014. DOI: 10.17487/RFC7296. URL: https://datatracker.ietf.org/doc/html/rfc7296.

[98] S. Kent. *IP Authentication Header*. RFC 4302. Dec. 2005. DOI: 10.17487/RFC4302. URL: https://www.rfc-editor.org/info/rfc4302.

[99] S. Kent. *IP Encapsulating Security Payload (ESP)*. RFC 4303. Dec. 2005. DOI: 10.17487/RFC4303. URL: https://www.rfc-editor.org/info/rfc4303.

[100] S. Kent and K. Seo. *Security Architecture for the Internet Protocol*. RFC 4301. Dec. 2005. DOI: 10.17487/RFC4301. URL: https://www.rfc-editor.org/info/rfc4301.

[101] Dustin Kern, Christoph Krauß, Timm Lauser, Nouri Alnahawi, Alexander Wiesmaier, and Ruben Niederhagen. "QuantumCharge: Post-Quantum Cryptography for Electric Vehicle Charging". In: *Applied Cryptography and Network Security*. Ed. by Mehdi Tibouchi and XiaoFeng Wang. Cham: Springer Nature Switzerland, 2023, pp. 85–111.

[102] W.Z. Khan, M.H. Rehman, H.M. Zangoti, M.K. Afzal, N. Armi, and K. Salah. "Industrial internet of things: Recent advances, enabling technologies and open challenges". In: *Computers & Electrical Engineering* 81 (2020), p. 106522. DOI: https://doi.org/10.1016/j.compeleceng.2019.106522.

[103] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. "A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model". In: *Advances in Cryptology – EUROCRYPT 2018*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Cham: Springer International Publishing, 2018, pp. 552–586. ISBN: 978-3-319-78372-7.

[104] Stavros Kousidis, Johannes Roth, Falko Strenzke, and Aron Wussler. *Post-Quantum Cryptography in OpenPGP*. Internet-Draft draft-ietf-openpgp-pqc-17. Internet Engineering Task Force. URL: https://datatracker.ietf.org/doc/draft-ietf-openpgp-pqc/17/.

[105] Ehren Kret and Rolfe Schmidt. *The PQXDH Key Agreement Protocol*. Signal Messenger. Last Accessed: 2026-03-23. URL: https://signal.org/docs/specifications/pqxdh/.

[106] Kris Kwiatkowski, Panos Kampanakis, Bas Westerbaan, and Douglas Stebila. *Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLS 1.3 (draft-ietf-tls-ecdhe-mlkem-01)*. Internet Draft, IETF. Feb. 2025. URL: https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/.

[107] Dock Labs. *eIDAS 2.0: A Beginner's Guide*. Last Accessed: 2025-09-09. Sept. 2025. URL: https://www.dock.io/post/eidas-2.

[108] Brian LaMacchia. "The long road ahead to transition to post-quantum cryptography". In: *Communications of the ACM* 65.1 (2021), pp. 28–30.

[109] LAN/MAN Standards Committee. *Port-Based Network Access Control*. Standard IEEE 802.1X-2020. IEEE, 2020.

[110] LAN/MAN Standards Committee. *Secure Device Identity*. Standard IEEE 802.1AR-2018. IEEE, 2018.

[111] Adeline Langlois and Damien Stehlé. "Worst-case to average-case reductions for module lattices". In: *Designs, Codes and Cryptography* 75.3 (2015), pp. 565–599. DOI: 10.1007/s10623-014-9938-4.

[112] Tao Liu, Gowri Ramachandran, and Raja Jurdak. "Post-quantum cryptography for internet of things: a survey on performance and optimization". In: *arXiv preprint arXiv:2401.17538* (2024).

[113] Patrick Longa. *FrodoKEM: A conservative quantum-safe cryptographic algorithm*. Last Accessed: 2026-01-14. Microsoft Research. May 2025. URL: https://www.microsoft.com/en-us/research/blog/frodokem-a-conservative-quantum-safe-cryptographic-algorithm/.

[114] Vadim Lyubashevsky. "Fiat-Shamir With Aborts: Applications to Lattice and Discrete-Log Based Signatures". In: *Advances in Cryptology – EUROCRYPT 2009*. Ed. by Christophe Antoine. Vol. 5479. Lecture Notes in Computer Science. Springer, 2009, pp. 598–616. DOI: 10.1007/978-3-642-10366-7_35. URL: https://doi.org/10.1007/978-3-642-10366-7_35.

[115] Vadim Lyubashevsky. "Lattice Signatures without Trapdoors". In: *Advances in Cryptology – EUROCRYPT 2012*. Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 738–755. DOI: 10.1007/978-3-642-29011-4_43.

[116] Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, et al. *CRYSTALS-Dilithium: A Post-Quantum Digital Signature Scheme*. https://pq-crystals.org/dilithium/. Last Accessed: 2026-02-20. 2024.

[117] Nikos Makriyannis. *How Blockchains Will Evolve for the Quantum Era*. Last Accessed: 2025-09-08. 2025. URL: https://www.fireblocks.com/blog/how-blockchains-will-evolve-for-the-quantum-era/.

[118] Lodovica Marchesi, Michele Marchesi, and Roberto Tonelli. "Reviewing crypto-agility and quantum resistance in the light of agile practices". In: *International Conference on Agile Software Development*. Springer. 2022, pp. 213–221. DOI: 10.1007/978-3-031-48550-3_21.

[119] Marin Ivezic. *Trust Now, Forge Later (TNFL) - The Overlooked Quantum Threat*. https://postquantum.com/post-quantum/trust-now-forge-later/. Last Accessed: 2026-04-02.

[120] Sinisa Markovic. *Crypto industry may be running out of time to prepare for quantum attacks*. Last Accessed: 2026-04-01. URL: https://www.helpnetsecurity.com/2026/03/31/quantum-computers-cryptocurrency-risks-google-research/.

[121] Friedl Markus, Jan Mojžíš, and Simon Josefsson. *Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512*. RFC 9941. Apr. 2026. DOI: 10.17487/RFC9941.

[122] Jillian Mascelli and Megan Rodden. *"Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks*. Finance and Economics Discussion Series 2025-093. Washington, DC: Board of Governors of the Federal Reserve System, 2025. DOI: 10.17016/FEDS.2025.093.

[123] Atefeh Mashatan and Douglas Heintzman. "The complex path to quantum resistance: Is your organization prepared?" In: *Queue* 19.2 (2021), pp. 65–92.

[124] Melanie Goldsborough Matthew Campagna and Peter O'Donnell. *AWS post-quantum cryptography migration plan*. Last Accessed: 2026-03-04. Amazon Web Services. 2024. URL: https://aws.amazon.com/blogs/security/aws-post-quantum-cryptography-migration-plan/.

[125] Hassane Aissaoui Mehrez and Othmane El Omri. "The crypto-agility properties". In: *The 12th International Conference on Society, Cybernetics and Informatics*. 2018, pp. 99–103.

[126] Guillaume Michel. "Road to Cryptographic Agility". Diploma Project (Master's Thesis). École Polytechnique Fédérale de Lausanne (EPFL), 2021. URL: https://guillaume.michel.id/docs/road-to-cryptographic-agility.pdf.

[127] Microsoft. *SIKE Cryptographic Challenge*. Microsoft Security Response Center (MSRC). Last Accessed: 2026-02-19. URL: https://www.microsoft.com/en-us/msrc/sike-cryptographic-challenge.

[128] Microsoft. *Superposition*. https://quantum.microsoft.com/en-us/insights/education/concepts/superposition. Last Accessed: 2025-10-22.

[129] Lynette I Millett and Anne Frances Johnson. *Cryptographic Agility and Interoperability: Proceedings of a Workshop*. National Academies Press, 2017.

[130] Modbus. *Specifications and Implementation Guides for Modbus Protocol*. 2025. URL: https://www.modbus.org/modbus-specifications.

[131] *Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203)*. Federal Information Processing Standard Publication 203. National Institute of Standards and Technology, Aug. 2024. DOI: 10.6028/NIST.FIPS.203.

[132] Dustin Moody. *NIST PQC: The Road Ahead*. Presentation at Real World Crypto (RWC) / NIST PQC Workshop. Last Accessed: 2025-05-22. National Institute of Standards and Technology (NIST), Mar. 2025. URL: https://csrc.nist.gov/csrc/media/Presentations/2025/nist-pqc-the-road-ahead/images-media/rwcpqc-march2025-moody.pdf.

[133] Dustin Moody. *Post-Quantum Cryptography: NIST's Plan for the Future*. Presentation at PQCrypto 2016, Fukuoka, Japan. National Institute of Standards and Technology (NIST). Feb. 2016. URL: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/pqcrypto-2016-presentation.pdf.

[134] Michele Mosca and Marco Piani. *Quantum Threat Timeline Report 2025*. Tech. rep. Co-authored by evolutionQ Inc. Global Risk Institute, Mar. 2026. URL: https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/.

[135] NASA Goddard Space Flight Center. *Bulk Security Standard for Spacecraft Communication*. NASA Technical Standard GSFC-STD-8012. National Aeronautics and Space Administration (NASA), Aug. 2024. URL: https://standards.nasa.gov/sites/default/files/standards/GSFC/Baseline/0/GSFC-STD-8012_Approved.pdf.

[136] National Institute of Standards and Technology. *About NIST*. Last Accessed: 2025-08-21. n.d. URL: https://www.nist.gov/about-nist.

[137] National Institute of Standards and Technology. *Announcing PQC Candidates to be Standardized, Plus Fourth Round Candidates*. https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4. Last Accessed: 2026-02-20. July 2022.

[138] National Institute of Standards and Technology. *HQC Announced as a 4th Round Selection*. https://csrc.nist.gov/news/2025/hqc-announced-as-a-4th-round-selection. Last Accessed: 2026-02-20. Mar. 2025.

[139] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard*. Tech. rep. Federal Information Processing Standards (FIPS) 204. Gaithersburg, MD: U.S. Department of Commerce, Aug. 2024. DOI: 10.6028/NIST.FIPS.204.

[140] National Institute of Standards and Technology. *Post-Quantum Cryptography: Additional Digital Signature Schemes*. https://csrc.nist.gov/projects/pqc-dig-sig. Ongoing NIST post-quantum cryptography standardization effort. 2022–.

[141] National Institute of Standards and Technology. *PQC Standardization Process: Second Round Candidate Announcement*. https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates. Last Accessed: 2026-02-20. Jan. 2019.

[142] National Institute of Standards and Technology. *PQC Third Round Candidate Announcement*. https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement. Last Accessed: 2026-02-20. July 2020.

[143] National Institute of Standards and Technology. *Public-Key Post-Quantum Cryptographic Algorithms: Nominations*. https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms. Last Accessed: 2026-02-20. Dec. 2016.

[144] National Institute of Standards and Technology. *Recommendations for Key-Encapsulation Mechanisms*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-227.pdf. Last Accessed: 2026-04-08. Sept. 2025.

[145] National Institute of Standards and Technology. *Round 1 Additional Signatures - Post-Quantum Cryptography*. https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures. Last Accessed: 2026-02-20. July 2023.

[146] National Institute of Standards and Technology. *Round 1 Submissions - Post-Quantum Cryptography Standardization*. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions. Last Accessed: 2026-02-20. 2017.

[147] National Institute of Standards and Technology. *Round 2 Additional Signatures - Post-Quantum Cryptography*. https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures. Last Accessed: 2026-02-20. Oct. 2024.

[148] National Institute of Standards and Technology. *Round 3 Additional Signatures - Post-Quantum Cryptography*. https://csrc.nist.gov/Projects/pqc-dig-sig/round-3-additional-signatures. Last Accessed: 2026-05-19. May 2026.

[149] National Institute of Standards and Technology. *Stateless Hash-Based Digital Signature Standard*. Tech. rep. Federal Information Processing Standards (FIPS) 205. Gaithersburg, MD: U.S. Department of Commerce, Aug. 2024. DOI: 10.6028/NIST.FIPS.205. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf.

[150] National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.CSWP.29.

[151] National Institute of Standards and Technology. *Workshops and Timeline - Post-Quantum Cryptography*. https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline. Last Accessed: 2026-02-20.

[152] David Nelson. *Crypto-Agility Requirements for Remote Authentication Dial-In User Service (RADIUS)*. Tech. rep. Last Accessed: 2026-01-05. URL: https://www.rfc-editor.org/rfc/rfc6421.

[153] Taboka Ngwenya and Belinda Ndlovu. "A Systematic Review of Post-Quantum Cryptography for Healthcare Data Protection: Performance, Readiness, and Deployment Challenges". In: *Journal of Applied Informatics and Computing (JAIC)* 10.1 (2026), pp. 134–149.

[154] Mads Villum Nielsen, Magnus Raagaard Kjeldsen, Togu Turnip, and Birger Andersen. "Post-Quantum Digital Signature Algorithms on IoT: Evaluating Performance on LoRa ESP32 Microcontroller". In: *22nd International Conference on Security and Cryptography*. SCITEPRESS Digital Library. 2025, pp. 592–600.

[155] NIS Cooperation Group. *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. Tech. rep. Part 1, Version: 1.1, EU PQC Workstream. 2025, p. 17.

[156] NIST. *Cryptographic Algorithm Validation Program*. Last Accessed: 2026-03-02. Google Cloud. URL: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation-search?searchMode=implementation&vendor=Google&productType=-1&algorithm=180&ipp=50.

[157] NIST PQC-Forum. *Discussion about Kyber's tweaked FO transform*. Last Accessed: 2025-10-20. URL: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/WFRDl8DqYQ4.

[158] NIST PQC-Forum. *Kyber decisions, part 2: FO transform*. Last Accessed: 2026-03-25. URL: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/C0D3W1KoINY/m/99kIvydoAwAJ.

[159] O-RAN ALLIANCE. *About O-RAN ALLIANCE*. Last Accessed: 2026-03-18. URL: https://www.o-ran.org/about.

[160] ODVA Technologies. *About*. en-US. 2026. URL: https://www.odva.org (visited on 05/12/2026).

[161] ODVA Technologies. *CIP Security*. en-US. 2026. URL: https://www.odva.org/technology-standards/distinct-cip-services/cip-security/ (visited on 04/17/2026).

[162] OPC Foundation. *Unified Architecture*. 2025. URL: https://opcfoundation.org/about/opc-technologies/opc-ua/.

[163] Oracle. *Service Availability in all Cloud Regions*. Last Accessed: 2026-04-02. 2026. URL: https://www.oracle.com/cloud/distributed-cloud/service-availability/.

[164] David Ott, Christopher Peikert, et al. "Identifying research challenges in post quantum cryptography migration and cryptographic agility". In: *arXiv preprint* (2019). DOI: https://doi.org/10.48550/arXiv.1909.07353.

[165] OWASP CycloneDX Project. *Authoritative Guide to CBOM: Implement Cryptography Bill of Materials for Post-Quantum Systems and Applications*. Informative guidance; the normative standard is ECMA-424. OWASP Foundation. 2024. URL: https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-CBOM-en.pdf.

[166] Christof Paar, Brendon Richard Chetwynd, Thomas J Connor, Sheng Yung Deng, and Stephen J Marchant. "Algorithm-agile cryptographic coprocessor based on FPGAs". In: *Reconfigurable Technology: FPGAs for Computing and Applications*. Vol. 3844. SPIE. 1999, pp. 11–16.

[167] Edward Parker. *U.S.-Allied Militaries Must Prepare for the Quantum Threat to Cryptography*. Last Accessed: 2025-09-08. URL: https://www.rand.org/pubs/commentary/2025/06/us-allied-militaries-must-prepare-for-the-quantum-threat.html.

[168] Sebastian Paul and Melanie Niethammer. "On the importance of cryptographic agility for industrial automation: Preparing industrial systems for the quantum computing era". In: *at-Automatisierungstechnik* 67.5 (2019), pp. 402–416. DOI: 10.1515/auto-2019-0019.

[169] Kyrylo Petrenko, Atefeh Mashatan, and Farid Shirazi. "Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization". In: *Journal of Information Security and Applications* 46 (2019), pp. 151–163. DOI: 10.1016/j.jisa.2019.03.007.

[170] Nelly Porter and Christiane Peters. *PQC in plaintext: How we're helping customers prepare for a quantum-safe future*. Last Accessed: 2026-03-02. Google Cloud. Oct. 2025. URL: https://cloud.google.com/blog/products/identity-security/how-were-helping-customers-prepare-for-a-quantum-safe-future.

[171] Post-Quantum Cryptography (PQC) Working Group. *Risk Model Technical Paper, Appendix A*. Tech. rep. Last Accessed: 2026-01-05. 2023. URL: https://www.fsisac.com/hubfs/Knowledge/PQC/RiskModel.pdf.

[172] PROFIBUS-PROFINET. *PROFIsafe System Description Technology and Application*. System Description. PROFINET, 2024.

[173] PROFINET. *About PI*. 2026. URL: https://www.profibus.com/pi-organization/about-pi (visited on 04/21/2026).

[174] PROFINET. *Secure Communication with PROFINET*. 2026. URL: https://www.profinet.com/profinet-explained/security (visited on 04/17/2026).

[175] Michael Prorock and Orie Steele. *ML-DSA for JOSE and COSE (draft-ietf-cose-dilithium-11)*. Internet Draft, IETF. Mar. 2026. URL: https://datatracker.ietf.org/doc/draft-ietf-cose-dilithium/.

[176] Michael Prorock, Orie Steele, and Hannes Tschofenig. *FN-DSA for JOSE and COSE (draft-ietf-cose-falcon-04)*. Internet Draft, IETF. Mar. 2026. URL: https://datatracker.ietf.org/doc/draft-ietf-cose-falcon/.

[177] Michael Prorock, Orie Steele, and Hannes Tschofenig. *SLH-DSA for JOSE and COSE*. Internet-Draft draft-ietf-cose-sphincs-plus-07. Internet Engineering Task Force, Mar. 2026. URL: https://datatracker.ietf.org/doc/draft-ietf-cose-sphincs-plus/.

[178] QuEra Computing. *What is Quantum Decoherence*. https://www.quera.com/glossary/quantum-decoherence. Last Accessed: 2025-10-22.

[179] Tirumaleswar Reddy and Hannes Tschofenig. *Post-Quantum Cryptography Recommendations for TLS-based Applications (draft-ietf-uta-pqc-app-01)*. Internet Draft, IETF. Feb. 2026. URL: https://datatracker.ietf.org/doc/draft-ietf-uta-pqc-app/.

[180] Tirumaleswar Reddy.K. *Post-Quantum Enhancements to EAP-TLS and EAP-TTLS*. Internet-Draft draft-reddy-emu-pqc-eap-tls-02. Internet Engineering Task Force. URL: https://datatracker.ietf.org/doc/draft-reddy-emu-pqc-eap-tls/.

[181] Tirumaleswar Reddy.K, Valery Smyslov, and Scott Fluhrer. *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC*. Internet-Draft draft-ietf-ipsecme-ikev2-pqc-auth-06. Internet Engineering Task Force. URL: https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-pqc-auth/06/.

[182] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*. STOC '05. New York, NY, USA: Association for Computing Machinery, 2005, pp. 84–93. DOI: 10.1145/1060590.1060603.

[183] *Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector*. 2022. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

[184] E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. 2018. URL: https://datatracker.ietf.org/doc/html/rfc8446.

[185] Eric Rescorla, Hannes Tschofenig, and Nagendra Modadugu. *The Datagram Transport Layer Security (DTLS) Protocol Version 1.3*. RFC 9147. Apr. 2022. DOI: 10.17487/RFC9147. URL: https://www.rfc-editor.org/info/rfc9147.

[186] Morteza SaberiKamarposhti, Kok-Why Ng, Fang-Fang Chua, Junaidi Abdullah, Mehdi Yadollahi, Mona Moradi, et al. "Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data". In: *Heliyon* 10 (May 2024), pp. 1–19. DOI: 10.1016/j.heliyon.2024.e31406.

[187] Vipin Samar. *Securing Oracle AI Database 26ai for the Quantum Era*. Last Accessed: 2026-03-06. Oct. 2025. URL: https://blogs.oracle.com/database/oracle-ai-database-26ai-pqc.

[188] J. Schaad. *CBOR Object Signing and Encryption (COSE): Structures and Process*. RFC 9052. Aug. 2022. DOI: 10.17487/RFC9052.

[189] J. Schaad, B. Ramsdell, and S. Turner. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification*. RFC 8551. Apr. 2019. DOI: 10.17487/RFC8551.

[190] Rolfe Schmidt. *The ML-KEM Braid Protocol*. Signal Specifications. URL: https://signal.org/docs/specifications/mlkembraid/.

[191] Scott Twaddle. *Offering a sovereign cloud designed for the European Union*. Last Accessed: 2026-04-02. 2023. URL: https://blogs.oracle.com/cloud-infrastructure/offering-a-sovereign-cloud-designed-for-the-european-union.

[192] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509. DOI: 10.1137/S0097539795293172. URL: https://doi.org/10.1137/S0097539795293172.

[193] Signal Foundation. *Signal Protocol and Post-Quantum Ratchets*. Signal Blog. Last Accessed: 2026-03-17. Oct. 2025. URL: https://signal.org/blog/spqr/.

[194] Signal Foundation. *Signal: Say "hello" to a different messaging experience*. Last Accessed: 2026-03-17. URL: https://signal.org/.

[195] Dimitrios Sikeridis, David Ott, Sean Huntley, Shivali Sharma, Vasantha Kumar Dhanasekar, Megha Bansal, et al. "ELCA: Introducing enterprise-level cryptographic agility for a post-quantum era". In: *Cryptology ePrint Archive* (2023).

[196] Alexandr Silonosov and Lawrence Henesey. "Towards cryptographic agility manifesto in end-to-end encryption systems: a position paper from the perspective of crypto-consumers". In: *2024 IEEE Conference on Dependable, Autonomic and Secure Computing (DASC)*. IEEE. 2024, pp. 65–72.

[197] Heli Snellman, Joonas Savolainen, and Antti Hirvonen. "Quantum computing is coming – Is the financial sector ready?" In: *Bank of Finland Bulletin* (Aug. 2025). Last Accessed: 2026-02-23. URL: https://www.bofbulletin.fi/en/2025/articles/quantum-computing-is-coming-is-the-financial-sector-ready/.

[198] SPHINCS+ Team. *SPHINCS+: Stateless Hash-Based Signatures*. Last Accessed: 2025-10-20. URL: https://sphincs.org/.

[199] SSH Academy. *What is the Secure Shell (SSH) Protocol?* https://www.ssh.com/academy/ssh/protocol. Last Accessed: 2025-09-19.

[200] Douglas Stebila, Scott Fluhrer, and Shay Gueron. *Hybrid Key Exchange in TLS 1.3*. Sept. 2025. URL: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/.

[201] Keith Stouffer, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, et al. *Guide to Operational Technology (OT) security*. Tech. rep. NIST SP 800-82r3. Gaithersburg, MD: National Institute of Standards and Technology (U.S.), 2023, p. 299. DOI: 10.6028/NIST.SP.800-82r3.

[202] Bryan Sullivan. *Security Briefs: Cryptographic Agility*. Last Accessed: 2026-01-05. 2009. URL: https://learn.microsoft.com/en-us/archive/msdn-magazine/2009/august/cryptographic-agility.

[203] Nick Sullivan. *A Detailed Look at RFC 8446 (a.k.a. TLS 1.3)*. https://blog.cloudflare.com/rfc-8446-aka-tls-1-3/. 2018.

[204] Matt Swayne. *China Opens Its Superconducting Quantum Computer For Commercial Use*. Last Accessed: 2026-01-13. Oct. 2025. URL: https://thequantuminsider.com/2025/10/14/china-opens-its-superconducting-quantum-computer-for-commercial-use/.

[205] The FrodoKEM Team. *FrodoKEM: Practical quantum-secure key encapsulation from generic lattices*. Last Accessed: 2026-01-14. URL: https://frodokem.org/.

[206] The SIKE Team. *A note on the insecurity of SIKE*. Last Accessed: 2026-02-19. URL: https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/sike-team-note-insecure.pdf.

[207] C. J. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van Geest, O. Garcia-Morchon, et al. *Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)*. RFC 9370. May 2023. DOI: 10.17487/RFC9370. URL: https://www.rfc-editor.org/rfc/rfc9370.

[208] Ioanna Tzialla and Sophie Schmieg. *Announcing quantum-safe Key Encapsulation Mechanisms in Cloud KMS*. Last Accessed: 2026-03-03. Google Cloud. Oct. 2025. URL: https://cloud.google.com/blog/products/identity-security/announcing-quantum-safe-key-encapsulation-mechanisms-in-cloud-kms.

[209] U.S. Crypto Assets Task Force - SEC. *Post-Quantum Financial Infrastructure (PQFIF): A Roadmap for the Quantum-Safe Transition of Global Financial Infrastructure*. Technical Proposal. Sept. 2025.

[210] Guilin Wang and Valery Smyslov. *KEM-based Authentication for the Internet Key Exchange Protocol Version 2 (IKEv2) with Post-quantum Security*. Internet-Draft. Internet Engineering Task Force. URL: https://datatracker.ietf.org/doc/draft-wang-ipsecme-kem-auth-ikev2/03/.

[211] IETF PQUIP WG. *State of protocols and PQC*. https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc. Last Accessed: 2026-04-07. 2026.

[212] Alexander Wiesmaier, Nouri Alnahawi, Tobias Grasmeyer, Julian Geißler, Alexander Zeier, Pia Bauspieß, et al. "On PQC migration and crypto-agility". In: *arXiv preprint arXiv:2106.09599* (2021).

[213] Paul Wouters, Daniel Huigens, Justus Winter, and Niibe Yutaka. *OpenPGP*. Tech. rep. RFC 9580. Internet Engineering Task Force (IETF). URL: https://datatracker.ietf.org/doc/rfc9580/.

[214] Tatu Ylonen and Chris Lonvick. *The Secure Shell (SSH) Protocol Architecture*. RFC 4251. Jan. 2006. DOI: 10.17487/RFC4251.