Global and Domestic Progress in Post-Quantum Cryptography Migration Standardization

Boyeon Song

Korea Institute of Science and Technology Information

bysong@kisti.re.kr

Abstract

This paper provides a brief overview of the current status of post-quantum cryptography (PQC) migration standardization, with a focus on initiatives led by the National Institute of Standards and Technology (NIST), contributions from international standardization organizations such as the European Telecommunications Standards Institute (ETSI) and the Internet Engineering Task Force (IETF), and domestic efforts by Korean Post-Quantum Cryptography (KpqC) team.

Ⅰ. Introduction

As quantum computing progresses, the threats that it poses to existing cryptographic infrastructure have spurred an urgent transition to quantum-resistant cryptosystems. In response, global standardization bodies, national governments, and industry consortia have accelerated their efforts to define, adopt, and implement post-quantum cryptography (PQC) standards.

This paper provides a brief overview of the current status of PQC migration standardization, with a focus on key initiatives led by the National Institute of Standards and Technology (NIST), along with relevant contributions from international standardization organizations such as the European Telecommunications Standards Institute (ETSI) and the Internet Engineering Task Force (IETF), highlighting their roles, strategies, and milestones in developing quantum-resistant cryptographic frameworks. Additionally, it addresses domestic efforts initiated by the National Intelligence Service (NIS) and the National Security Research Institute (NSR) to develop and adopt national PQC standards. By summarizing these activities, the paper aims to provide insight into the next steps for preparing secure digital infrastructure for the post-quantum era.

Ⅱ. NIST-Led Initiatives

The United States' NIST is playing a central and foundational role in the global transition to PQC. Its contributions span from algorithm standardization to implementation guidance, so that governments, industries, and international bodies are able to prepare for quantum-era threats.

NIST launched the PQC Standardization project in December 2016 to identify, evaluate, and standardize quantum-resistant public-key cryptographic algorithms [1]. After three rounds of evaluation and analysis, NIST announced in July 2022 the selection of four PQC algorithms for standardization, along with four candidates for a fourth round of analysis, The first PQC algorithms selected for standardization include CRYSTALS-KYEBER for key encapsulation mechanism (KEM), and CRYSTALS-Dilithium, FALCON and SPHINCS$^+$ for digital signatures [1]. Among the fourth-round candidates, HQC was selected for standardization on March 11, 2025, and is set to become the second NIST PQC KEM standard [1]. NIST has published three Federal Information Processing Standards (FIPS) for PQC on August 13, 2024, as follows [1]:

- FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) Standard (based on CRYSTALS-KYBER)
- FIPS 204: Module-Lattice-Based Digital Signature (ML-DSA) Standard (based on CRYSTALS-Dilithium)
- FIPS 205: Stateless Hash-Based Digital Signature (SLH-DSA) Standard (based on SPHINCS+)

In September 2022, NIST issued a new call for additional quantum-resistant digital signature proposals as part of the PQC standardization process [1]. The institute expressed particular interest in general-purpose signature schemes that are not based on structured lattice assumptions, and that offer short signature sizes and fast verification times [1]. Forty algorithms were selected and evaluated in the first round, and in October 2024, fourteen candidates were announced for the second-round evaluation process. The evaluation process for these candidates is currently ongoing [1].

NIST is encouraging organizations to begin transitioning to the new standards in preparation for the era of quantum computing. To support this effort, NIST has released a draft Internal Report (IR) and a Special Publication (SP) that provide guidance on migration to PQC, as follows [1]:

- IR 8547 (Initial Public Draft) Transition to Post-Quantum Cryptography Standards, published November 12, 2024.
- SP 800-227 (Initial Public Draft) Recommendations for Key-Encapsulation Mechanisms, published January 7, 2025.

Ⅲ. International Contributions

1. ETSI

ETSI has been at the forefront of PQC standardization in Europe through its Technical Committee on Cybersecurity (TC CYBER) Quantum-Safe Cryptography (QSC) working group [2]. It aims to assess and make recommendations for QSC primitive protocols and implementation considerations, but does not include the development of cryptographic primitives [2].

ETSI published a Technical Report (TR) 103 619 to define migration strategies and recommend quantum-safe schemes, and enhance cryptography awareness across all business sectors in July 2020 [2]. It outlines a structured, three-stage approach for organizations to transition to fully quantum-safe cryptographic state [2]. ETSI released a Technical Specification (TS) 104 015 in March 2025, introducing a hybrid KEM named Covercrypt [2]. This mechanism combines classical and post-quantum cryptographic techniques, enhancing security by ensuring that only authorized users with the correct permission can access and decrypt sensitive data [2]. Notably, updates to TS 103 744 in March 2025 focus on authenticated quantum-safe hybrid key establishment, aiming to provide robust security mechanisms suitable for integration into existing infrastructures [2]. The following list are the TR and TSs mentioned above, which are published by ETSI to support the transition to PQC [2].

- ETSI TR 103 619 v1.1.1 CYBER; Migration strategies and recommendations to Quantum Safe schemes (2020-07)
- ETSI TS 104 015 V1.1.1 CYBER; Quantum-Safe Cryptography (QSC); Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies (2025-02)
- ETSI TS 103 744 V1.2.1 CYBER; Quantum-Safe Hybrid Key Establishment (2025-03)

2. IETF

IETF is actively progressing in facilitating the migration to PQC through its dedicated working group, Post-Quantum Use in Protocols (PQUIP) [3]. The group focuses on assisting by providing guidance, identifying use cases, and supporting the integration of PQC into existing Internet protocols, ensuring the resilience of Internet protocols against emerging quantum threats [3]. Working groups within IETF have explored incorporating PQC into protocols like TLS and IPsec. Some important IETF draft proposals related to PQC transition include the following [3]:

- draft-ietf-pquip-pqc-engineers-11, Post-Quantum Cryptography for Engineers, updated on 2025-05-06.
- draft-ietf-pquip-pqt-hybrid-terminology-06, Terminology for Post-Quantum Traditional Hybrid Schemes, updated on 2025-01-10.

ⅡⅡ. Domestic Efforts

In July 2023, South Korea's NIS announced a master plan for migration to PQC, developed in collaboration with NSR and the Ministry of Science and ICT. The plan outlines a comprehensive roadmap to transition the nation's cryptographic infrastructure to a quantum resistant one by 2035, aligning with timelines set by the United States and Europe. This roadmap covers algorithm standardization, phased implementation, and international collaboration.

In line with the roadmap, the KpqC competition was launched in November 2021 to develop domestic PQC standard algorithms [4]. In November 2022, the KpqC team selected 16 candidate algorithms for the first round, and in December 2023, announced eight candidates for the second round [4]. The final four algorithms selected for standardization were announced in January 2025: SMAUG-T and NTRU+ for PKE/KEMs, and HAETAE and AIMer for digital signatures.

The next phase of the roadmap includes standardization of PQC, along with the development of transformation, evaluation and detection technologies. This will be followed by the creation of supporting systems for cryptographic transformation and pilot implementations in critical sectors such as finance, healthcare, and government services. The ultimate goal is a comprehensive transition to PQC by 2035 [4].

V. Conclusion

The global migration to PQC is no longer a theoretical consideration, but a strategic imperative. NIST is playing a pivotal role in shaping the future of quantum-resistant cryptographic systems through its rigorous PQC selection process and algorithm standardization. International organizations such as ETSI and IETF are also contributing by defining migration strategies and recommending quantum-safe schemes. South Korea's proactive approach, exemplified by the KpqC competition and the NIS's roadmap, demonstrates strong national commitment to aligning with global efforts while fostering domestic innovation.

In parallel with the efforts of global and domestic standardization bodies and national governments to enable PQC migration across digital infrastructures, it is essential to conduct research and development on how to efficiently implement the PQC standards, step by step, within our specific application domains.

ACKNOWLEDGMENT

This research was supported by Korea Institute of Science and Technology Information (KISTI). (No. K25L5M2C2-01)

REFERENCES

[1] NIST, Post-Quantum Cryptography, https://csrc.nist.gov/projects/post-quantum-cryptography.

[2] ETSI, Quantum-Safe Cryptography (QSC), https://www.etsi.org/technologies/quantum-safe-cryptography.

[3] IETF, Post-Quantum Use In Protocols (pquip), https://datatracker.ietf.org/wg/pquip/about/.

[4] KpqC, https://kpqc.or.kr.