CORRESPONDANCE

“Harvest Now, Decrypt Later”

Chaminda Hewage*

Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, United Kingdom.
ORCID: 0000-0001-7593-6661

Abstract: Due to the increased threat of “Harvest Now, Decrypt Later” attacks, Post-Quantum Cryptography (PQC) is moving from theoretical research to real-world implementations. By 2024, the National Institute of Standards and Technology (NIST) finalized the first set of quantum safe cryptographic algorithms. At present, governments across the world are developing plans for mandatory PQC migration, typically targeting timelines between 2030 and 2035. This letter investigates key challenges in transition to PQC, ongoing standardization efforts by NIST and other organizations, and national policies of proposed migration strategies.

Keywords: PQC, NIST, ML-KEM, ML-DSA, FIPS

INTRODUCTION

The advent of quantum computing poses a significant threat to traditional cryptographic algorithms, including RSA, Diffie-Hellman, and Elliptic Curve Cryptography, due to the capabilities of quantum algorithms like Shor’s algorithm. PQC has emerged to address these challenges. Lattice-based cryptography (LBC) has emerged as a prominent candidate for PQC [1].

LBC, underpinned by hard mathematical problems like Learning with Errors (LWE) and Ring-LWE (RLWE), offers robust security against quantum and classical adversaries. LBC-based PQC can be used for access control in addition to the encapsulation and signature schemes. Ciphertext-Policy Attribute-Based Encryption (CPABE) has become a critical tool for enabling fine-grained access control in data-sharing scenarios, such as secure cloud storage and IoT. While existing CP-ABE implementations rely on bilinear pairings vulnerable to quantum attacks, lattice-based CPABE schemes provide a quantum-resistant alternative. Despite their potential, these schemes face challenge in Computational efficiency, collusion resistance, and implementation correctness.

Recent work by the author and collaborators [2] presents a detailed mathematical breakdown of one of the states of the art (SOTA) lattice-based CP-ABE schemes and a novel correctness proof for the same scheme.

This letter discusses the key challenges associated with transition to PQC algorithms, standardization efforts and migration strategies of selected countries.

KEY CHALLENGES IN PQC TRANSITION

There are several challenges in the transition to PQC including incompatibility with legacy systems to performance and resource demands of proposed PQC algorithms. This section summarizes key challenges faced by the researchers, developers, service providers and policy makers.

"Harvest Now, Decrypt Later" Threat: The urgency of a fast-tracked transition to PQC is driven by the risk that adversaries may harvest encrypted data today, with the aim to decrypt them later using quantum computers when they are widely available. Some researchers have also suggested that nation-state actors could possess more advanced quantum capabilities than publicly disclosed, although such claims remain unverified. In February 2025, Microsoft announced a major quantum computing breakthrough with the introduction of Majorana 1, the world’s first Quantum Processing Unit (QPU) powered by a topological core. According to the announcement, this new chip uses a novel state of matter to create smaller, stable, and highly resilient qubits, aiming for a million-qubit system within 10 years. These developments reinforce the need for a timely transition to PQC, with researchers, standardization bodies, and different governments across the world actively working toward secure and scalable solutions [3].

*Corresponding author. E-mail address: chewage@cardiffmet.ac.uk (Chaminda Hewage)

RESOURCE CONSTRAINTS AND PERFORMANCE LIMITATIONS

The proposed PQC algorithms generate large key sizes, signatures and cipher texts in comparison to traditional algorithms such as RSA or ECC. This results in increased computational requirements, memory usage, network latency and storage overhead. Tables 1, 2 and 3 present the key sizes of the proposed PQC algorithms. In contrast, traditional cryptographic algorithms generate significantly smaller keys and cipher texts (e.g., public key sizes for RSA-3072 and ECDSA P-256 are approximately 384 bytes and 32 bytes respectively) which are considerably smaller than those shown in the Tables. Consequently, PQC algorithms introduce additional constraints when deployed in resource constrained environments such as IoT and sensor networks. These differences may also create compatibility challenges with legacy systems, where some IoT or Industry Control Systems (ICSs) may require hardware upgrades to support PQC.

Table 1: Cryztals-Kyser Key Sizes ML-KEM (Module Lative Based Key Encapsulation Mechanism)

Algorithm	Encapsulation Key size	Decapsulation key size	Ciphertext size
ML-KEM 512	800	1632	768
ML-KEM 768	1184	2400	1088
ML-KEM 1024	1568	3168	1568

Table 2: Crystals- Dilithium Key Sizes - ML-DSA (Module-Lattice-Based Digital Signature Standard)

Algorithm	Private Key size	Public key size	Signature size
ML-DSA-44	2560	1312	2420
ML-DSA-65	4032	1952	3309
ML-DSA-87	4896	2592	4627

Crypto Agility Requirement and validation bottlenecks:

Similar to Shor's algorithm, new quantum threats will emerge in the future. Therefore, organizations and standardization bodies should design processes and systems that enable rapid evaluation, standardization, validation and deployment of new algorithms if current PQC options are compromised. At present, validation of proposed PQC algorithms takes considerable time, which further delays their deployment in real-world applications.

Table 3: Sphincs+ - Slh-Dsa (Stateless Hash-Based Signature Standard)

Algorithm	Security Category	Public Key size	Signature Size
SLH-DSA-SHA2-128s SLH-DSA-SHAKE-128s	1	32	7856
SLH-DSA-SHA2-192s SLH-DSA-SHAKE-192s	3	48	16224
SLH-DSA-SHA2-256s SLH-DSA-SHAKE-256s	5	64	29792

Standardization Efforts (NIST & International)

NIST has led the standardization efforts of quantum safe cryptographic algorithms. The effort began in November 2017 and resulted in the first set of standards finalized in 2024: FIPS 203 (ML-KEM/Kyber for general encryption), FIPS 204 (ML-DSA/Dilithium for signatures), and FIPS 205 (SLH-DSA/SPHINCS+ for signatures) towards end of 2024 [4]. NIST continues to evaluate the security and performance of additional algorithms. To this end it has selected the Hamming Quasi-Cyclic key encapsulation mechanism (HQC) for encryption and is working on FALCON digital signature scheme (FIPS 206) as alternatives to the primary lattice-based methods. The focus has now shifted toward implementing these standardized algorithms in sectors such as cloud services, telecommunications and finance. While NIST leading the PQC standardization activities other international bodies/organizations (IETF, ISO/IEC, ETSI, ITU-T) and national agencies (e.g., NCSC-UK) are actively working to facilitate the migration by finalizing guidelines, protocols and standards. For instance, Internet Engineering Task Force (IETF) is working on updating the internet protocols such as TLS and IKEv2 to accommodate PQC algorithms.

Policies of Different Countries

Many governments across the world are moving beyond awareness and advisory stages towards PQC implementations, auditing and compliance. For instance, the United States is working to adopt PQC algorithms standardized by the NIST across critical systems and services with migration targets extending into the early 2030s. To this end, several policy documents and guidelines have been published, including the executive

orders EO-14144, EO-14306, and the memorandum by the Department of War on "Preparing for Migration to Post-Quantum Cryptography", Nov 2025. In contrast, China is pursuing the development and adoption of its own PQC algorithms and has recently issued a call for submissions of new PQC candidates, with a timeline from 10 Oct 2025 to 30 June 2026. Within the European Union (EU), member states are evaluating both NIST and other alternative PQC algorithms. For instance, countries including Germany and Netherland have shown interest in schemes such as FrodoKEM alongside NIST selected algorithms. The EU is also working toward establishing a coordinated PQC roadmap for member states by 2026.

Sri Lanka's PQC Transition

Following the urgent need to address the threats faced by emerging quantum computers, many countries including Sri Lanka are in the process of evaluating and implementing PQC algorithms across critical platforms and service sectors. The Sri Lanka Computer Emergency Response Team (SLCERT) has launched a PQC initiative aimed at safeguarding Sri Lanka's Digital Public Infrastructure (DPI) from potential quantum enabled threats [5]. The completion of migration targets by 2035 is mandatory to ensure long-term security and interoperability. The global systems (e.g., TLS) are gradually cooperating PQC algorithms and lack of adoption may lead to security vulnerabilities and potential compatibility challenges.

Migration Strategy

Migration is being urged now, with a target of 2030 for deprecating legacy systems and 2035 for full transition. The migration strategy can be implemented through the following steps:

- Inventory & Discovery: Identify all systems that rely on vulnerable public-key cryptography (e.g., RSA/ECC).
- Hybrid Deployment: Use both classical and quantum-safe algorithms together to guard against unforeseen weaknesses in newly developed PQC algorithms.
- PKI Upgrades: Prioritizing upgrading of Public Key Infrastructure (PKI), including code-signing and digital certificates, to support PQC.

CONCLUSION

The letter discusses the challenges associated with the transition to PQC including migration strategies, standardization efforts and the policies adopted by different governments to implement quantum safe cryptographic algorithms. The standardisation efforts are now shifting towards implementing the selected algorithms along with auditing and compliance. Many technologists and policy makers aim to complete this migration as early as possible, with the latest target being 2035.

REFERENCES

[1] Manish Kumar, Post-quantum cryptography Algorithm's standardization and performance analysis, *Array*, Volume 15, 2022, 100242, ISSN 2590-0056, https://doi.org/10.1016/j.array.2022.100242.

[2] J. Loughridge, R. Rahulamathavan, C. Hewage, et al., "Correctness proof for a Ring-Learning-with-Errors Multi-Authority Ciphertext-Policy Attribute-Based Encryption Scheme," *2025 IEEE 45th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, Glasgow, United Kingdom, 2025, pp. 315-320, doi:10.1109/ICDCSW63273.2025.00059.

[3] Bolgar, Catherine. "Microsoft's Majorana 1 Chip Carves New Path for Quantum Computing - Source.", *Microsoft*, 19 Feb. 2025, news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/.

[4] NIST. "Post-Quantum Cryptography | CSRC | CSRC." *CSRC | NIST*, 3 Jan. 2017, csrc.nist.gov/projects/post-quantum-cryptography.

[5] "SLCERT to Launch Post-Quantum Cryptography to Safeguard SL's DPI." *Print Edition - the Sunday Times, Sri Lanka*, 2025, www.sundaytimes.lk/251116/business-times/slcert-to-launch-post-quantum-cryptography-to-safeguard-sls-dpi-620859.html.