Quantum Resistant Cryptography: Preparing for the Post-Quantum Era

TNE30009 Research Report

Dylan Rodwell   
105341089  
105341089@student.swin.edu.au

*Abstract*—The imminent arrival of practical quantum computers poses a significant threat to classical cryptography systems like RSA and ECC. These foundational systems are the roots of global digital security and are now vulnerable to quantum attacks, particularly Shor’s algorithm, which can efficiently solve the hard mathematical problems on which these systems rely. In response, the field of post-quantum cryptography (PQC) was created, focusing on developing and standardising algorithms resistant to both classical and quantum adversaries. This report provides an overview of quantum-resistant cryptographic frameworks, with a particular emphasis on lattice-based schemes, which have recently been standardised by NIST. The report examines the motivations behind PQC, current standards and protocols, the practical challenges of migrating from legacy systems, unresolved issues, and best practices for effective PQC adoption.

Keywords—post-quantum cryptography, quantum computing, lattice-based cryptography, Kyber, Dilithium, NIST, migration, quantum-resistant.

# Introduction

With the rapid evolution of quantum computing, it is certain to disrupt the foundations of modern digital security. Classical cryptographic algorithms, like RSA and Elliptic Curve Cryptography (ECC), have long been the standard for confidentiality, integrity, and authentication of data across global networks. However, with the arrival of quantum algorithms, most notably Shor’s algorithm, new threats render these widely used mechanisms obsolete by enabling efficient solutions to mathematical problems considered unmanageable for normal computers [1][3][4]. As quantum hardware advances, this looming threat of breaking current public-key systems creeps closer to reality. This has significant implications for sectors ranging from government and finance, to critical infrastructure and healthcare [1][2].

Anticipating this shift, the field of **post-quantum cryptography (PQC)** has emerged, focusing on the development and standardisation of algorithms that can resist both classical and quantum attacks. The US National Institute of Standards and Technology (NIST), recognised the urgency of this threat and has led global efforts to standardise quantum-resistant algorithms, resulting in the recent selection and ratification of lattice-based schemes, such as CRYSTALS-Kyber and CRYSTALS-Dilithium, as new Federal Information Processing Standards (FIPS 203/204) [1][2][4]. The algorithms promise to ensure secure communication and data protection in the future where quantum adversaries are a reality.

The transition to PQC however, comes with technical, organisational and practical challenges. Migration from firmly established cryptographic protocols to quantum-resistant alternatives requires not only sturdy algorithmic solutions, but also careful consideration of implementation, interoperability, and regulatory compliance [2][3]. In high-stakes industries like healthcare, where sensitive patient data is increasingly managed in cloud-based environments, the stakes are especially high. Recent studies show that while awareness of quantum threats is growing, actual preparedness and migration to PQC remain limited [2][3].

This report provides an overview of quantum-resistant cryptography frameworks, focusing on the motivations behind PQC, the current landscape of standardisation, and the challenges associated with migration and implementation. By examining both foundational standards and recently applied research, the report aims to answer the key questions:

* Why are existing cryptography systems vulnerable in a post-quantum world?
* Which quantum-resistant frameworks and protocols are being adopted?
* What problems and unresolved issues persist in the migration to PQC?
* What approaches and best practices are emerging for effective transitions.

# Background and Motivation

## The Quantum Threat to Classical Cryptography

Classical public-key cryptographic systems, like RSA, DSA, and ECC, obtain their security from the computational difficulty of mathematical problems like integer factorisation and discrete logarithms. However, these foundations are threatened by advances in quantum computing. Shor’s algorithm, when run on a sufficiently powerful quantum computer, can solve these problems in polynomial time, rendering widely used encryption and digital signature schemes vulnerable [1][3][4]. As a result, financial transactions, personal healthcare records, and state secrets are at risk of future compromise.

## T*he Emergence of Post-Quantum Cryptography (PQC)*

Recognising this dooming threat, the cryptographic community and international standards organisations have prioritised the investigation and development of quantum-resistant cryptographic algorithms, collectively called “post-quantum cryptography (PQC)”. PQC schemes are designed to remain secure even against adversaries equipped with large-scale quantum computers [1][4].

NIST initiated a global PQC standardisation process in 2016, inviting cryptographers worldwide to submit candidate algorithms that could withstand both classical and quantum attacks [1][4]. After an extensive multi-year evaluation, lattice-based schemes such as CRYSTALS-Kyber (for key encapsulation) and CRYSTALS-Dilithium (for digital signatures) emerged as leading candidates and have now been selected as new Federal Information Processing Standards (FIPS 203/204) [4]. The adoption of these standards is a critical milestone, marking the beginning of practical migration efforts across the industry and government.

## Motivation for Migration

The urgency to migrate to PQC is escalated by the “harvest now, decrypt later” threat model, in which adversaries collect encrypted communications today with the intention of decrypting them once quantum computers mature [1][3]. This is particularly concerning for long-lived sensitive information, like health records and government data, which must stay confidential for years or decades [2].

In the healthcare sector, for example, the migration to PQC is not just a technical upgrade, but a necessity for regulatory compliance and upholding patient privacy. Recent research highlights that while awareness of PQC is increasing, actual implementation remains slow due to organisational inertia, resource constraints, and uncertainty about migration strategies [2][3]. The risks are compounded in cloud environments, where sensitive patient data can be exposed to additional attack vectors [2].

# Frameworks and Protocols

## What is Post-Quantum Cryptography (PQC)?

The primary objective of PQC is to develop cryptographic schemes that can withstand attacks from both classical and quantum computers. Multiple frameworks have been proposed and analysed, but lattice-based cryptography has emerged as the leading candidate due to its strong security proofs, versatility, and practical performance [1][4]. Other notable PQC families include code-based, hash-based, multivariate, and isogeny-based cryptography, but these alternatives often face challenges concerning key sizes, efficiency, or have yet to reach the same stage in standardisation [1][3][4].

## NIST Standardisation and Protocols

The NIST PQC project began in 2016, inviting global submissions for quantum-resistant algorithms. Over four rounds of extensive public evaluation, the focus was narrowed to lattice-based schemes due to their strong mathematical foundations and demonstrated quantum resistance [1][4]. In 2024, NIST announced new Federal Information Processing Standards:

* **FIPS 203:** Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM, Kyber)
* **FIPS 204:** Module-Lattice-Based Digital Signature Algorithm (ML-DSA, Dilithium)
* **FIPS 205:** Stateless Hash-based Digital Signature Algorithm (SPHINCS+) as a backup [4]

These standards form the backbone of future quantum-resistant protocols for public-key encryption, key exchange, and digital signatures.

## Implementation in Protocols and Applications

Lattice-based schemes like Kyber and Dilithium are being integrated into widely used security protocols, including Transport Layer Security (TLS), SSH, VPNs, and secure messaging platforms [3][4]. The PQC migration is not limited to software, hardware implementations are actively being explored to optimise performance and reduce resource consumption [4]. In sectors like healthcare, cloud-based patient information systems are beginning to pilot lattice-based encryption for stronger data protection [2].

## Strengths and Limitations

Lattice-based cryptography provides strong security guarantees against quantum adversaries, efficient key exchanges, and digital signatures with competitive performance [4]. However, challenges remain, including larger key and signature sizes, side-channel resistance, and integration complexity, especially in resource-constrained environments [3][4].

In critical sectors, such as healthcare, the adoption of PQC is also influenced by regulatory compliance, data privacy requirements, and the need for seamless migration with minimal disruption [2].

# Problems Addressed by PQC

## Vulnerabilities of Classical Cryptography

Traditional cryptographic algorithms such as RSA, DSA, and ECC, are fundamentally threatened with the advance of quantum computing. Shor’s algorithm can efficiently solve the integer factorisation and discrete logarithm problems that make up these schemes, making them breakable by sufficiently powerful quantum computers [1][3][4]. As a result, encrypted communications, digital signatures, and authentication protocols based on these methods will not provide long-term security once large-scale quantum computers become available. This vulnerability affects not only future data but also data that is encrypted today and stored for long periods, creating the well-documented “harvest now, decrypt later” risk [1][3].

## Addressing Forward Secrecy and Data Longevity

Many industries including healthcare, government, and financial, require data confidentiality and integrity for decades. For example, patient medical records must remain private for the lifetime of the individual and beyond [2]. The threat posed by quantum computers is especially dangerous for long-lived data like this, as adversaries can capture encrypted traffic now and decrypt it later using quantum resources. PQC directly addresses these risks by introducing cryptographic schemes that are believed to be secure against both classical and quantum attacks, ensuring forward security, secrecy, and long-term data protection [1][2][4].

## Implementation and Migration Challenges

While PQC schemes are designed to be quantum-resistant, their integration into existing systems is not easy. The key challenges of this process include:

* **Larger Key and Signature Sizes:** Lattice-based algorithms, while efficient, typically require larger keys and signatures compared to classical alternatives, impacting bandwidth and storage [3][4].
* **Performance Overhead:** Some PQC schemes have higher computational requirements, affecting system performance, particularly in resource-constrained environments like IoT devices [3][4].
* **Standardisation and Interoperability:** The migration to PQC must be coordinated across global standards, protocols, and regulatory frameworks. Not all industries or organisations are equally prepared or resourced for this transition [2][3].
* **Side-Channel Attacks:** New schemes that introduce unforeseen vulnerabilities, like susceptibility to timing or power analysis attacks, necessitating ongoing research and robust implementation guidelines [4].
* **Organisational Awareness and Skills Gap:** Studies show a lack of preparedness and understanding of PQC migration paths among decision-makers, especially in sectors handling sensitive data [2][3].

## Regulatory Compliance Pressures

The regulatory environment is evolving to mandate stronger data protection in the face of quantum threats. For example, in healthcare, compliance with privacy regulations such as HIPPA and GDPR is driving the need for timely PQC adoption to avoid future liability [2]. Failure to address quantum risks can result in exposure of sensitive personal data, financial loss, reputation damage, and potential legal penalties.

## Summary of PQC Benefits

By addressing these vulnerabilities and challenges, PQC provides a path to sustained data security, regulatory compliance, and future-proofed cryptographic infrastructure. Its adoption is not merely a technical upgrade, but a necessary evolution to defend against the quantum threat landscape [1][2][3][4].

# Unresolved Issues and Current Challenges

## Algorithmic and Security Uncertainties

While lattice-based schemes like Kyber and Dilithium have been standardised and are widely regarded as secure, the cryptographic community acknowledges that these are relatively new compared to classical algorithms like RSA and ECC. Their long-term security depends on the assumed hardness of lattice problems, which remain unproven against all possible quantum and classical attacks [1][4]. Continued cryptanalysis and research are essential to validate their resilience as new mathematical techniques and quantum algorithms develop [4].

## Implementation and Integration Challenges

Integrating PQC into existing infrastructures presents several practical difficulties:

* **Legacy Systems Compatibility:** Many systems rely on rooted cryptographic libraries and hardware, making seamless PQC integration complex. Hybrid deployments are often necessary during the transition period, increasing implementation complexity [3][4].
* **Resource Constraints:** Larger key and signature sizes, along with increased computational demands, can strain devices with limited processing power or memory, like IoT sensors and embedded systems [3][4].
* **Side-Channel and Implementation Attacks:** PQC algorithms may introduce new side-channel vulnerabilities or implementation errors, especially as their software and hardware adoption accelerates [4].

## Organisational and Policy Barriers

* **Awareness and Training Gaps:** Many organisations lack awareness of quantum risks and the skills necessary for PQC migration, hindering timely adoption [2][3].
* **Cost and Resource Allocation:** Migration to PQC can require significant investment in new hardware, software updates, and staff training, posing a barrier for organisations with limited budgets [2][3].
* **Regulatory Uncertainty:** Evolving legal frameworks and standards can create ambiguity regarding compliance requirements, with organisations uncertain about timelines and obligations for implementing PQC [2][3].

# Approaches Being Considered for Unresolved Issues

## Hybrid Cryptography and Gradual Transition

Given the complexity of replacing entrenched cryptographic systems, a staged migration strategy is widely recommended. Hybrid cryptography enables organisations to maintain security while validating PQC schemes and ensuring backward compatibility [3][4]. This approach is especially useful for protocols like TLS, where hybrid cryptographic handshakes can provide resilience against both classical and quantum adversaries during the migration period.

## Cryptographic Inventory and Risk Assessment

A critical first step in migration is conducting a thorough cryptographic inventory, identifying where and how cryptography is used within organisational infrastructure [3]. This includes cataloguing all algorithms, protocols, libraries, and hardware security modules in use. Organisations should assess quantum risk associated with each system, prioritising the protection of long-lived sensitive data and mission-critical applications [1][2][3].

## Proof-of-Concepts and Pilot Projects

Pilot implementations and controlled proof-of-concepts are essential for understanding the real-world performance and integration challenges of PQC schemes [2][3][4]. For example, healthcare organisations have begun integrating lattice-based encryption into cloud-based patient information systems to evaluate security and operational impact [2]. These pilots inform best practices for deployment.

## Crypto Agility and Future-Proofing

Systems should be designed with crypto agility, the ability to rapidly replace cryptographic primitives as new standards emerge or vulnerabilities are discovered [3][4]. This design philosophy reduces reliance on any single algorithm and enables a more flexible, future-proof security posture. Automated tools for algorithm substitution and centralised key management can help streamline migration and maintenance [3][4].

## Regulatory Compliance and Documentation

Organisations must stay informed of evolving standards and legal requirements, documenting their migration plans and compliance efforts [2][3]. Engaging early with regulators and industry groups can help clarify expectations and ensure that migration strategies align with sector-specific mandates.

# Conclusion and Recommendations

The transition to a post-quantum cryptographic landscape is both a technical necessity and a fierce challenge. The looming threat brought by quantum computers to classical cryptographic systems demands a proactive and well-coordinated migration to quantum-resistant alternatives. Lattice-based schemes, now standardised by NIST, offer a promising foundation for next-generation cryptographic protocols, providing strong security assurance against quantum adversaries.

However, successful PQC adoption requires more than technical upgrades. Organisations must address practical issues like integration with legacy systems, increased computational and storage requirements, side-channel resilience, and staff training and awareness. Sectors dealing with long-lived sensitive information, like healthcare, face additional pressures from regulatory compliance and data privacy concerns. Hybrid cryptography, crypto agility, and careful inventory and risk management are among the best practices that can help mitigate these challenges and ensure a smooth migration.

Although unresolved issues remain, the road to a quantum-secure future is complex. Early and thoughtful action, guided by current best practices and evolving standards, will equip organisations to safeguard their critical information assets against both present and future cryptographic threats.

# References

1. L. Chen et al., “Report on Post-Quantum Cryptography,” Report on Post-Quantum Cryptography, Apr. 2016, doi: https://doi.org/10.6028/nist.ir.8105.S. Dudek, “Low Powered and High Risk: Possible Attacks on LoRaWAN Devices,” Trend Micro, Jan. 26, 2021. <https://www.trendmicro.com/en_au/research/21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html>.
2. O. Juliana Tiwo, T. Oluwatoyin Adesokan-Imran, D. Comfort Babarinde, S. Michael Oyekunle, A. Titilola Olutimehin, and O. Oladeji Olaniyi, “Advancing Security in Cloud-based Patient Information Systems with Quantum-resistant Encryption for Healthcare Data,” researchgate.net, Mar. 20, 2025. <https://www.researchgate.net/profile/Oluwaseun-Olaniyi/publication/390023438_Advancing_Security_in_Cloud-based_Patient_Information_Systems_with_Quantum-resistant_Encryption_for_Healthcare_Data/links/67dc3697e62c604a0df77de5/Advancing-Security-in-Cloud-based-Patient-Information-Systems-with-Quantum-resistant-Encryption-for-Healthcare-Data.pdf>.
3. S. A. Käppler and B. Schneider, “Post-Quantum Cryptography: An Introductory Overview and Implementation Challenges of Quantum-Resistant Algorithms,” easychair.org, 2022. <https://easychair.org/publications/paper/z7P1/download>.
4. H. NGUYEN, S. HUDA, Y. NOGAMI, and T. TAN NGUYEN, “Security in Post-Quantum Era: A Comprehensive Survey on Lattice-Based Algorithms”:, Ieee.org, 2025. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=11006701>.