JOURNAL OF POST-QUANTUM CRYPTOGRAPHY AND SYSTEMS

RESEARCH ARTICLE

Volume 01, Issue 02, 2026

Transitioning from Classical to Post-Quantum Security: Threat Models, Migration Strategies, Hardware Constraints, and Real-World Applications

Ankit Gupta[1], Shilpi Mittal[2]

[1]Independent Researcher, Dallas, USA

[2]Department of Information Science, University of North Texas, Denton, USA

ABSTRACT

Classical cryptographic systems that power modern digital communication, software security, digital financial transactions, and digital sign-in and security for critical infrastructures are challenged by very fast development of quantum computer. The review explores the shift from classical to post-quantum security, and how to combine threat models for the quantum era, post-quantum cryptographic methods, migration strategies, constraints on hardware, and practical examples. It describes how Shor's algorithm can break RSA, Diffie–Hellman and elliptic-curve cryptography, and how Grover's algorithm can break the security of symmetric encryption and hash functions. Focusing on the harvest-now-decrypt-later threat, protocol downgrade attacks, side-channel leakage, and fault injection. The review discusses the different approaches lattice-based, hash-based, code-based, multivariate, and isogeny-based, making a particular focus on the standardized ones, ML-KEM, ML-DSA, and SLH-DSA. It also suggests the concept of a phased migration program – cryptographic discovery, risk assessment, transitional deployment, optimization via crypto agile infrastructures. Other hardware and implementation related topics such as memory, computation, energy, secure randomness, masking and accelerator design are also explored. Migration needs differ significantly between industries, as evidenced by the myriad of practical implementations in secure messaging, finance, telecom, IoT systems, government, healthcare and critical infrastructure. In summary, it is necessary to coordinate standardization, risk-based planning, conducting interoperability testing, implementing cryptographically secure solutions, establishing organizational governance, preparing the workforce, continuously monitoring, and designing cryptographic architectures that can evolve to address new threats and future cryptanalyses.

Keywords: Post-quantum cryptography; quantum security; crypto-agility; migration strategies; quantum threat models

1. Introduction

The security of a cryptographic system is vital to the modern digital society, safeguarding the confidentiality, integrity, authenticity and availability of information moving over interwoven networks. Online banking, electronic commerce, the cloud computing paradigm, health care information systems, digital identity, secure messaging, industrial control systems, blockchain platforms, and national security communications all rely on classical cryptographic mechanisms. Secure key exchange, authentication, and digital signatures are enabled by public-key schemes like RSA, Diffie–Hellman, and elliptic-curve cryptography, which are used for large blocks of data in the symmetric key schemes like the Advanced Encryption Standard. The advent of quantum computing has thrown significant doubts into the future of these well-known security methods, though. The main danger is posed by quantum algorithms for the solution of mathematical problems which would be unsolvable by classical computers in a reasonable time. Shor's algorithm can solve integer factorisation and discrete log problems efficiently, which compromises the security of RSA, Diffie–Hellman, elliptic-curve cryptography and some other signature schemes. Grover's algorithm also increases the effectiveness of the security of symmetric encryption and cryptographic hash functions by speeding up exhaustive key searches. As a result, post-quantum cryptography has become a huge research and standardization initiative that aims to establish algorithms that are quantum resistant. This new area of research is blossoming as the international community strives to create reliable alternatives to quantum-resistant cryptography that can be used before quantum computers with cryptographic relevance enter the world (Dam et al., 2023).

The harvest-now-decrypt-later threat model adds to the urgency of transition. In this case, enemies would be able to intercept, store and process encrypted messages now while hoping that future quantum computers will be able to crack them. The danger is especially great for government information, military communications, financial details, medical data, intellectual property, and genomic information that needs to be kept confidential for decades. The exact timeline for the emergence of large-scale fault-tolerant quantum computing is still up in the air, but the process of replacing cryptography in highly complex infrastructure can take potentially years of planning, testing, certifying, and deployment. Thus, the delay in the preparation until quantum computers are fully functional would put organizations at significant operational and security risk (LaMacchia, 2021). Another area of quantum cyber security is a strategic issue as the consequences of cryptographic failure go beyond technical systems.

Decryption of confidential communication, spoofing, forgery of digital signatures, spoofing of software, and software manipulation could impact national sovereignty, military readiness, public safety, and economic stability. Quantum preparedness must thus be taken up as an institutional and policy level priority, not just a narrow cryptographic issue (Troublefield, 2026). In the national security context, quantum information science could significantly impact the intelligence community, national communications, defense systems, and national technological competition, and thus the adoption of quantum-resistant security measures as a prerequisite for long-term resilience becomes paramount (Jung, 2024). There have already been considerable advances in lattice-based, hash-based, code-based, multivariate and isogeny-based cryptography. However, the transition challenge does not end there the development of post-quantum algorithms is just one aspect.

The ability to select and deploy algorithms and the confidence in their long-term security is still hindered by cryptanalytic

breakthroughs, implementation issues, protocol incompatibility, hardware constraints, and the uncertainty surrounding future assumptions.Currently, cryptanalytic advances, implementation weaknesses, protocol incompatibility, hardware limitations, and uncertain future assumptions remain issues affecting algorithm selection and deployment confidence (Chenu & Sportiello, 2025). In addition, organisations need to be able to identify the cryptographic assets already in place, to select and prioritise high-risk systems, to understand third-party dependencies, to update certificates and protocols, and to build "crypto-agile" systems that can adapt to the change of cryptographic algorithms as standards or threat patterns evolve.

Current studies tend to focus on the mathematical characteristics or capabilities of the post-quantum algorithms and less on the broader transition process. Implementing migration will involve risk assessment, standards, governance, hardware readiness, interoperability, workforce capability, and the process of a phased implementation. Migration routes, therefore, need to be strategically linked with technical readiness and organizational planning and regulatory alignment. Therefore, the transition to quantum security is explored in four related aspects quantum security threat models, migration strategies and crypto-agility, hardware and implementation limitations, and real-world applications. It makes a key contribution in helping to bridge the gap between the development of post-quantum algorithms and deploying them across today's digital ecosystems.

2. Classical Cryptography and the Quantum Security Transition

2.1 Classical Cryptographic Infrastructure

Classical cryptography is the base of modern digital security and it allows for confidentiality, authentication, integrity verification, and secure key exchange. Symmetric algorithms (e.g., Advanced Encryption Standard and ChaCha20) are used for efficient protection of large amounts of data, hash functions and message authentication codes are used for integrity checking and authentication. RSA, elliptic curve cryptography, elliptic curve digital signatures and Diffie–Hellman are among the public-key mechanisms that are used for key establishment, identity verification, software signing, and digital certificates. These techniques are integrated into TLS, virtual private networks, secure email, cloud computing, financial systems, digital identities, blockchain applications and critical infrastructure. They are based on the difficulty of three computational tasks integer factorization, discrete logarithm, and elliptic-curve discrete logarithm.

2.2 Quantum Algorithms and Cryptographic Vulnerability

These assumptions are broken by the development of quantum computing as some quantum algorithms can solve problems which are not feasible for conventional computers. Shor's algorithm is efficient on large integers and is able to resolve problems of discrete logarithms, posing a threat to RSA, Diffie–Hellman, elliptic-curve cryptography, and other digital-signature systems. On the other hand, Grover's algorithm mainly impacts symmetric encryption and hash functions with a quadratic acceleration in exhaustive search. This does not imply that symmetric algorithms are broken or found to be insecure, but only that they are weakened and do not necessarily have to be broken to maintain a satisfactory level of security, and may be adequately protected with a longer key or stronger output lengths. In order to deal with the transition to a post-quantum world, responses must be different for public-key and symmetric cryptographic mechanisms (Dam et al., 2023).

To find public-key algorithms that are viable for deployment and resistant to both classical and quantum attacks, the NIST standardization process was begun. The second round evaluation was based on security, performance, implementation complexity, key size, signature size and resistance to known cryptanalytical methods (Alagic et al., 2020). Assessment in the

third round further reduced the candidates and gave significance to algorithm variety, implementation safety and application specific performance prior to final standardization (Alagic et al., 2022). The impact of Shor's and Grover's algorithms on classical algorithms, like RSA, Diffie–Hellman, ECC, AES, and hash functions, is mapped to the post-quantum ones, including ML-KEM, ML-DSA, SLH-DSA, stronger symmetric encryption, and crypto-agile infrastructure, as shown in Figure 1.

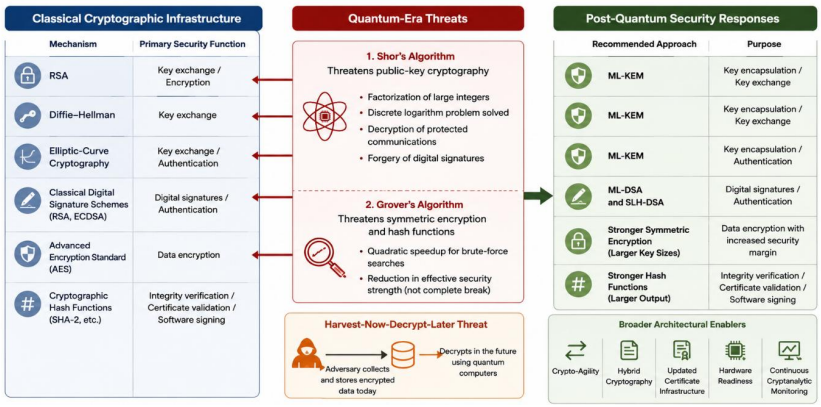

Figure 1. Transition from Classical Cryptographic Mechanisms to Post-Quantum Security.

2.3 Harvest-Now-Decrypt-Later and Long-Term Risk

The quantum challenge, the most immediate one, doesn't depend on the availability of a full-fledged quantum computer now. Harvest now decrypt later attacks involve intercepting encrypted messages and keeping them until such time as quantum technology is developed that allows them to be decrypted. This risk is particularly high for information that has to be kept confidential for a long period of time such as military communications, diplomatic records, medical data, genomic information, intellectual property, financial transactions and plans for critical infrastructure. This means, however, that quantum cybersecurity is a strategic issue – compromising long-lived data could have implications for national sovereignty, economic stability, and institutional trust (Troublefield, 2026).

National-security systems are especially vulnerable, as they are frequently equipped with highly sensitive information, have long lifecycles and slow replacement cycles. The implications of quantum information science for intelligence gathering, secure communication, defense planning, and international technological competition could shift, underscoring the need to move quickly to ensure strategic resilience (Jung, 2024).

2.4 Requirements for a Quantum-Safe Transition

Developing and deploying a post-quantum security strategy involves more than just swapping out a few algorithms. Organizations need to understand the locations of vulnerable cryptography being used, categorize the data by the length of time it must remain confidential, evaluate hardware and software requirements, test a standardized cryptography, update certificates and key-management systems, and ensure interoperability when implementing cryptography. Legacy systems, embedded devices, vendor products, regulatory requirements, and cryptographic components that might not be easy to find or

replace should also be considered in the migration planning process. The goal of a structured migration approach is to start with cryptographic discovery, prioritization of risk, and stages of implementing quantum-safe mechanisms (Barker et al., 2021). Overall, the classical-to-post-quantum transition can be seen as an architectural shift. The key components of a quantum-safe security are crypto-agility, standardisation of algorithms, secure implementation of algorithms, flexible protocols, compatible hardware, and ongoing monitoring of the advances in cryptanalysing. This wider view guarantees that organizations will be ready for quantum threats and future shifts in standards, technologies, and security expectations.

3. Quantum-Era Threat Models

3.1 Threats to Cryptographic Primitives and Security Services

The first step in threat modelling for the quantum era is to realize that the threat can be the same for both the algorithm and the services running on top. When the security of a public-key protocol relies on integer factorization or discrete logarithms, it can be compromised in public-key encryption, key exchange, digital signatures, authentication, certificate validation, secure messaging, software updates and blockchain transactions. If a knowledgeable adversary intercepts messages they could be able to decode the messages they intercept, impersonate a legitimate user, forge signatures, compromise certificate authorities, and approve fraudulent transactions. The threats could remain for the life of a system, as encrypted data acquired today could be kept for future decryption using quantum technologies.

Secure messaging is a practical example. Apple's PQ3 protocol aims to enhance post-compromise security by continually injecting post-quantum key material into subsequent conversations. Independent analysis shows that such designs should be analysed against both classical and quantum adversaries as it relies on the evolution of keys, authentication, recovery from breach and proper protocol composition (Stebila, 2024). Formal verification of PQ3 also illustrates the necessity of using well-defined adversarial models to assess security properties such as secrecy, authentication and post-compromise protection, which go beyond what can be claimed at the algorithm-level.Formal verification of PQ3 also shows the need for using well-defined adversarial models to assess security properties such as secrecy, authentication and post-compromise protection, beyond what can be claimed at the algorithm level (Basin et al., 2024).

3.2 Adversaries and Attack Scenarios

Future quantum-computing services could be used by quantum era threats such as nation-states, cybercriminals, malicious insiders, supply-chain attackers, and more. While they might have different goals, the typical cases involve the capture of encrypted network traffic, attacking certificate issuers, hijacking software signing keys, spoofing software updates, and stealing digital assets secured with classical signatures. It is therefore interesting to investigate hybrid key exchange schemes, which use a combination of classical and post-quantum mechanisms to provide security for the session if at least one of the two mechanisms is secure (Crockett et al., 2019). Hybrid TLS 1.3 designs follow this approach and use a traditional key establishment handshake with a post-quantum key encapsulation handshake. But such constructions must maintain integrity of the transcripts, key independence and downgrade resistance to attacks, and interoperability, and that an attacker would not force its use of weaker parameters (Stebila et al., 2022). Figure 2 shows the quantum era threats, attack methods, targeted

cryptographic assets, security implications, and protective measures needed to mitigate the risks at the algorithm, protocol, and implementation levels. Table 1 gives an overview of the key threats from the quantum era, along with their key targets and likely security implications.

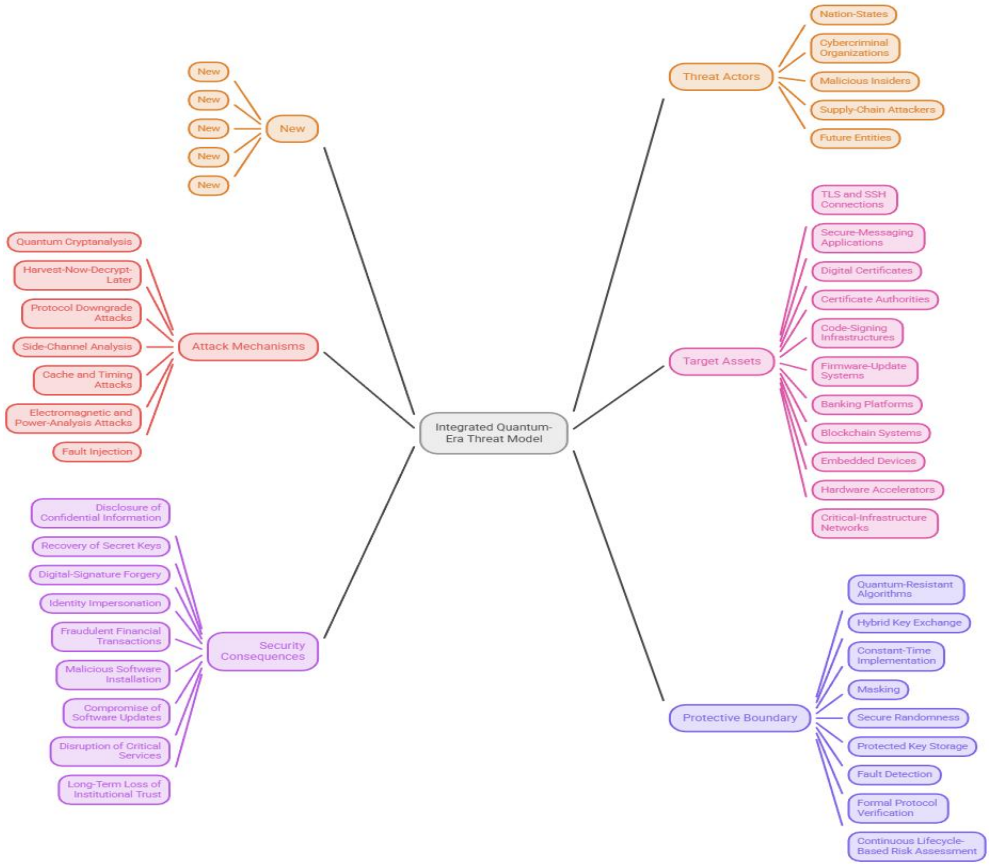

Figure 2. Integrated Quantum-Era Threat Model for Cryptographic Systems.

Table 1. Major Quantum-Era Security Threats.

Threat category	Primary target	Possible consequence	Reference
Quantum cryptanalysis	RSA, ECC, and Diffie–Hellman	Decryption of confidential information and forgery of digital signatures	(Dam et al., 2023)
Harvest-now-decrypt-later	Stored encrypted communications and long-lived sensitive data	Future disclosure of information collected before quantum computers become operational	(Troublefield, 2026)
Protocol manipulation	TLS, SSH, and secure-messaging protocols	Downgrade attacks, compromised key exchange, or authentication failure	(Stebila et al., 2022)
Side-channel attack	Software and hardware implementations	Recovery of secret keys through timing, power, cache, or electromagnetic leakage	(Andrysco et al., 2018)
Fault attack	Cryptographic accelerators and embedded devices	Incorrect cryptographic computation, information leakage, or secret-key recovery	(Xie et al., 2024)

3.3 Hybrid and Implementation-Level Threats

Although they are mathematically secure, post-quantum algorithms can be vulnerable if not properly implemented. Secret values may be revealed by timing variation, power consumption, electromagnetic leakage, cache behavior, memory access patterns and injected faults. It is thus essential to have constant time programs because operations, whose execution time varies according to secret information, can lead to leakage. There are techniques that can eliminate such risks by linking the behaviour of an implementation with formally checked security properties, and these techniques are verified to be constant time (Andrysco et al., 2018). From the hardware perspective, it is also well understood that post-quantum schemes consume vastly different amounts of resources, are variously slow, need different amounts of memory, and are vulnerable to different implementation attacks. Such differences can impact the deployment of an algorithm in an embedded, mobile, or high-performance application (Basu et al., 2019). Therefore, hardware circuits should not only be evaluated in terms of speed and area efficiency, but also for side-channel resistance, fault detection, secure key storage, randomness generation, and secure arithmetic operations (Xie et al., 2024).

3.4 Lifecycle-Based Threat Modeling

A complete threat model should include the following elements Algorithm selection, key generation, key storage, certificate issuance, data transmission, system decommissioning, key rotation, software updating, and parameter configuration. Any weakness at any point can compromise the security of a good post-quantum scheme. It should be secured through the use of secure algorithms, verified protocols, hardened implementation, controlled key management and continuous assessment during the lifecycle of cryptography.

4. Post-Quantum Cryptographic Approaches and Standardization

4.1 Lattice-Based Cryptography

Lattice-based cryptography has become the most promising basis for post-quantum key establishment and digital signatures, as it offers very efficient software and hardware implementations, while its security requirements are very strong. Its security is typically grounded on problems that are thought to be secure against classical and quantum attack, including Learning with Errors (LWE), Module-LWE, Short Integer Solution (SIS), and Module-SIS. They enable several important key-encapsulation techniques, digital signatures, identity-based systems and sophisticated privacy-preserving applications. CRYSTALS-Dilithium, later renamed ML-DSA, is an example of the utility of module-lattice signatures. Offers a practical signing and verification mechanism without some of the complex sampling techniques used in previous lattice designs. But its public keys and signatures are larger than classical elliptic-curve systems, resulting in extra storage and communication costs (Ducas et al., 2018). Similarly, research into lattice-based key-establishment schemes has evolved from theory to practice, developing schemes with enhanced security, performance, and implementation flexibility (Angom et al., 2025).

Specialized functions other than a feature space signature can also be supported by module-lattice methods. Pan et al., 2025, present a scheme called ML-GS that uses lattice-based assumptions to achieve group signatures with anonymity and controlled traceability properties in a post-quantum context. However, higher level functionality can come at the expense of

higher computational costs, key size and complexity in implementation. Optimization of the hardware is thus crucial for practical deployment. For example, CRYSTALS-Kyber can use resource-reuse architectures that share arithmetic components among various cryptographic operations, to save circuit area, which has been standardized as ML-KEM. These designs illustrate that polynomial arithmetic and memory organization can be optimized efficiently to implement efficient LBM in restricted hardware platforms (Huang et al., 2020).

4.2 Hash-Based and Alternative Approaches

The main features of hash-based signatures are the explicit security assumptions that are made conservatively and the security of cryptographic hash functions. SLH-DSA is stateless, so no risks are associated with key-management with hash-based schemes. The drawback of its principal is the huge size of its signature and relatively high computational expense. Signing and verifying performance can be drastically boosted with a dedicated hash unit, as hash-based schemes may have practical drawbacks that can be mitigated with architectural optimization (Saarinen, 2024). The cryptography based on codes is still important due to its long-standing resistance to cryptanalysis, although the public keys are very large, restricting its applicability with certificates, constrained devices and bandwidth limited systems. There have also been multivariate approaches and isogeny-based approaches to algorithmic diversity, with several candidates having suffered from large cryptanalytic failures. These results illustrate the importance of using conservative numbers, independent evaluation, and backup algorithm.

4.3 Standardization and Comparative Evaluation

Security, algorithms performance to standards, implementation characteristics, algorithm key sizes, and resistance to known algorithms were considered during the NIST standardization process. The second round report revealed significant differences between the lattice-based, code-based, multivariate, hash-based, and isogeny-based candidates, and showed that none of the candidates were optimal for all applications (Alagic et al., 2020). The third round evaluation then focused on a subset of algorithms and included additional elements related to implementation maturity, algorithm variety and confidence in the mathematical assumptions (Alagic et al., 2022). The current transition guidance is concerned with the use of standardized algorithms and flexibility due to the evolution of cryptanalysis and implementation. NIST's transition framework highlights that ML-KEM, ML-DSA, and SLH-DSA are pivotal components of the future quantum-resistant public-key ecosystem, and that public-key algorithms vulnerable to quantum computers will need to be gradually phased out (Moody et al., 2024). However, as seen from the track record of broken candidates, post-quantum standardization is still a process that will need to be continually tested, security audited, and diversified algorithm portfolios (Chenu & Sportiello, 2025). The main advantage, disadvantage and potential application of each approach are compared in Table 2.

Table 2. Comparison of Major Post-Quantum Cryptographic Approaches

Approach	Main strength	Principal limitation	Likely application	Reference
Lattice-based	Strong performance, versatile functionality, and comparatively mature implementation	Moderate-to-large public keys, ciphertexts, and signature sizes	TLS, digital certificates, key encapsulation, and software signing	(Ducas et al., 2018)
Hash-based	Conservative security foundation based primarily on established hash functions	Large signatures and intensive hashing requirements	High-assurance and long-term digital signatures	(Saarinen, 2024)
Code-based	Long-standing resistance to cryptanalytic attacks	Extremely large public keys and substantial storage requirements	Specialized key-establishment and high-security systems	(Alagic et al., 2020)
Multivariate and isogeny-based	Provides structural and mathematical diversity among post-quantum approaches	Reduced confidence following significant cryptanalytic attacks against several candidates	Continued research and development of alternative or backup algorithms	(Chenu & Sportiello, 2025)

5. Migration Strategies and Crypto-Agility

5.1 Cryptographic Inventory and Risk Prioritization

The first step to migration to post-quantum security should be a comprehensive cryptographic inventory. The challenge for organizations is to determine where public-key algorithms are used in applications, protocols, certificates, hardware security modules, cloud services, virtual private networks, identity systems, code-signing processes, and third-party products. The discovery phase is crucial as it is difficult to find many cryptographic dependencies in legacy software, vendor libraries, and embedded systems. Data sensitivity, lifetime of required data confidentiality, algorithm vulnerability, system criticality, replacement difficulty, and operational dependence are all factors that should be used to classify assets in a structured migration programme (Barker et al., 2021). Preparation also involves a formal evaluation of the organization's readiness. This involves documenting their current cryptographic assets, identifying responsible parties, assessing the capabilities of their suppliers, setting up testing environments, and deciding which systems are in need of immediate, medium-term and long-term remediation. Migration planning must therefore be risk based and prioritize systems that safeguard long-lived sensitive data and critical digital services (Newhouse et al., 2023). In addition, transition guidance states that it is crucial to phase out quantum-vulnerable algorithms by implementing carefully planned milestones, instead of replacing them on demand after the first quantum computer is released and becomes cryptographically relevant (Moody et al., 2024).

5.2 Hybrid Cryptography and Crypto-Agility

Hybrid cryptography can offer an important transition mechanism, using both classical and post-quantum cryptography in the same protocol. Session security is preserved if one or more component is secure in such systems. Hybrid key exchange and authentication has been demonstrated to enhance quantum resistance without compromising legacy protocols and infrastructures for TLS and SSH (Crockett et al., 2019). But hybrid designs add to a message size, computational burden, protocol complexity, and implementation risk. Hybrid TLS 1.3 key exchange is a hybrid elliptic-curve key exchange

mechanism that uses post-quantum key encapsulation.

The design should not allow downgrade attacks, maintain integrity of the transcript and should not affect the combined secret if one component fails (Stebila et al., 2022). Beyond classical and post-quantum cryptography, the hybridization can be extended to the quantum key distribution in special high-assurance networks, but with limitations due to infrastructure costs, distances and interoperability requirements (Vaněk et al., 2026). Crypto-agility is more comprehensive than hybridization. It's about the ability to identify, replace, configure and govern cryptographic algorithms without redesigning entire systems. Modular interfaces, algorithm independence, control of policies, automated certificate management, flexible key infrastructures and vendor support are all key features of effective crypto-agility. The importance of cryptographic agility is now being recognized through regulatory frameworks that are increasingly viewing it as an operational requirement, as organizations need to be able to quickly adapt to algorithm deprecation and new cryptanalytic vulnerabilities (Davis, 2026). Figure 3 shows the four-phase migration roadmap, which includes discovery, assessment, transition, and optimization, along with ongoing governance, regulatory alignment, workforce development and supplier accountability, and performance monitoring.

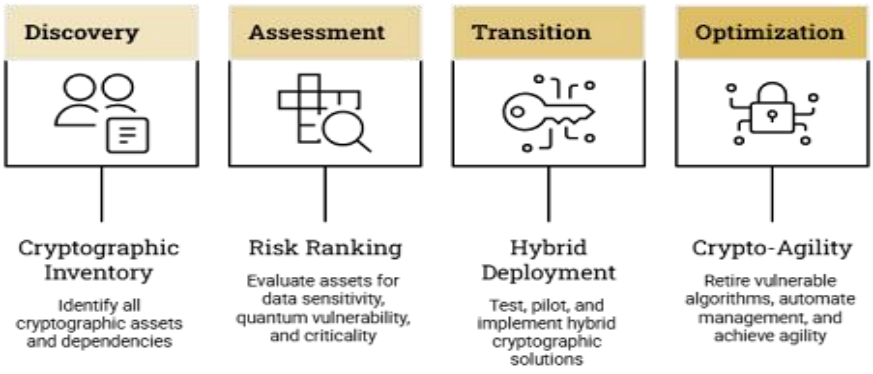

Figure 3. Phased Roadmap for Migration to Post-Quantum and Crypto-Agile Infrastructure.

5.3 Phased Migration Framework

The discovery, assessment, transition and optimization phases of post-quantum cryptographic migration have main activities and expected outcomes as outlined in Table 3. This migration can be broken down into four phases:

Table 3. Phased Framework for Post-Quantum Cryptographic Migration

Phase	Principal activities	Expected outcome	Reference
Discovery	Inventory cryptographic algorithms, keys, certificates, protocols, libraries, and system dependencies	Comprehensive visibility of organizational cryptographic exposure	(Barker et al., 2021)
Assessment	Rank systems according to data sensitivity, confidentiality lifetime, operational criticality, and replacement difficulty	Risk-based priorities and clearly defined migration timelines	(Newhouse et al., 2023)
Transition	Test and deploy hybrid cryptography and standardized post-quantum mechanisms while maintaining interoperability	Controlled migration with reduced disruption to existing services	(Moody et al., 2024)
Optimization	Retire quantum-vulnerable algorithms, automate	Sustainable and adaptable	(Davis, 2026)

	certificate and key management, and establish crypto-agile architectures	post-quantum security infrastructure	

Technical implementation should be aligned with policy, workforce development, procurement, compliance and executive oversight when implementing strategic migration pathways (Uddin & Azim, 2025). In the financial sector, payment systems, digital identities, interbank networks, and the need to store customer records for long periods need to be coordinated in terms of timelines and a high degree of interoperability testing (Kuka et al., 2026).

5.4 Migration Barriers and Governance

Challenges such as legacy systems, lack of vendor readiness, delays in certification, large key size, large signature size, performance uncertainty, and skilled manpower shortage are significant obstacles. This is expected to happen over a long period of time, and should not be regarded as a software upgrade, but rather as a long-term infrastructure programme (LaMacchia, 2021). Effective governance, measurable targets, supplier accountability and ongoing review are vital to minimise migration risk while maintaining continuity of operations.

6. Hardware and Implementation Constraints

6.1 Computational and Memory Requirements

While the mathematical security of post-quantum cryptography is important, the platform in which it can be practically deployed may require larger keys, larger signatures, larger ciphertexts and more complicated arithmetic operations. Unlike traditional elliptic-curve cryptography, many of the post-quantum cryptographic algorithms have significantly more memory, data transfer and computing requirements. While they work well in servers and high-performance systems, they can prove restrictive in embedded devices, smart cards, sensors, mobile platforms, and when deployed in the Internet of Things.

The latency, throughput, circuit size, area, energy consumption and memory needs have been found to vary significantly across the various candidate proposals when evaluated in hardware. These differences also imply that algorithm choice should be made in accordance with the capacity and mission of the intended platform, and not solely on the theoretical security level of the algorithm (Basu et al., 2019). The type of implementation may vary according to the need, as in light weight devices, where compactness may be more important, or in data-centre applications where high speed and parallel processing may be needed.

6.2 Lattice-Based Implementation Challenges

Polynomial arithmetic, modular reduction, sampling and number theoretic transforms are essential to lattice based schemes like ML-KEM and ML-DSA. These operations can be sped up with special hardware but efficient implementation requires coordination and synchronisation of the arithmetic units, memory banks and the control logic. The silicon area can be saved by reusing the same computational units to carry out several cryptographic functions in a resource-reuse architecture, however, a high level of reusability can result in high latency (Huang et al., 2020). Typical designs include parallel number-theoretic

transform units, pipelining and optimized modular multiplication. However, accessing the memory may be a major limitation due to polynomial coefficients need to be repeatedly loaded, transformed, and stored. Designers of hardware, then, need to strike a balance among throughput, area efficiency, memory consumption and energy consumption. However, lattice-based cryptography is more achievable in restrictive environments with optimized processors/accelerators and using various architectural trade-offs depending on the application (Dang et al., 2020).

6.3 Constrained Devices and Software Optimization

Microcontroller implementations have limited random access memory, flash memory, processor frequency, and power. Efficient software requires therefore optimizing the software level, managing the stack, minimizing temporary memory storage and arithmetic on platforms. Several lattice- and hash-based algorithms have been benchmarked on embedded processors and found to run on constrained processors, but with very different performance depending on parameter sets and security levels (Kannwischer et al., 2019). There are also concerns about battery life, communication overhead, firmware size and real-time response for the adoption of post-quantum cryptography in IoT and edge devices. These limits can be overcome by using the hardware-software co-design, where the computationally intensive operations can be assigned to the accelerators and the protocol control still remains to be done in software (Liu et al., 2024).

6.4 Side-Channel and Fault Resistance

Good implementation is not sufficient for security. Even though the encryption algorithm itself is mathematically secure, secret keys can be leaked due to timing, caching, power consumption, electromagnetic emissions, and fault injection. Constant time execution, masked arithmetic, protected memory, fault detection, randomness generation, and controlled error handling are all required properties to be added to hardware implementations.

To guarantee the safety of the quantum computing era, it is essential to thoroughly analyze systematic physical attacks, including passive and active attacks, on the dedicated post-quantum accelerators (Xie et al., 2024). Masking countermeasures can be used to break up sensitive values into randomized shares, thereby reducing side-channel leakage. But these protections make circuits larger, slower to execute, more random consuming and more complicated to implement. The design of such a hardware device must then be both capable and resistant to physical attacks (Fritzmann et al., 2020).

6.5 Hash-Based Signature Acceleration

The benefits of hash-based signatures are that they are based on mature and well-studied hash-function assumptions, but their signatures are large and the hashing operation results in computational and communication overhead. Signing and verifying can take a performance hit on the GPUs, but with dedicated hash accelerators the GPUs can be relieved and the speed increased (Saarinen, 2024). To this end, hardware readiness should be considered a fundamental aspect of post-quantum migration, especially for constrained and long-lived systems.

7. Real-World Applications of Post-Quantum Security

7.1 Secure Communication and Messaging

To secure data sent across messaging services, web services and enterprise networks, post-quantum cryptography is now being embedded in communication protocols. The areas of practical application include secure communication, and there are still practical methods of key exchange that are susceptible to future quantum attacks. Experimental applications have shown that post-quantum algorithms can be efficiently deployed in popular protocols with acceptable level of compatibility and performance. The use of lattice-based mechanisms in the implementation of post-quantum key exchange for Transport Layer Security (TLS) shows how to test these mechanisms in the current internet architecture prior to the global transition (Paquin et al., 2020). Secure messaging apps need to be protected from future decryption and from compromising the device. The PQ3 protocol for Apple does not use just one set of post-quantum key material for the entire conversation, but rather reuses key material several times. This design provides enhanced security even if the protocol's temporary key is compromised, as it allows for the re-establishment of cryptographic protection after the event (Stebila, 2024). This is another example of formal analysis of PQ3, showing that there is a need to model real-world deployment with strict models for secrecy, authentication, compromise recovery, and quantum-capable adversaries (Basin et al., 2024).

7.2 Financial Services and Digital Transactions

Public-key cryptography is crucial for financial institutions, where it's utilised in payment authorisation, digital banking, customer authentication, communication between financial institutions, certificate validation, and transaction signing. In the event of a quantum assault, a bad guy could be able to sign as an authorized user, impersonate a user, or crack the encryption of financial data stored anywhere. As a result, banks and payment networks will need to start identifying and evaluating cryptographic assets that are vulnerable to quantum attacks and find new solutions that are quantum resistant. Migration strategy in financial conditions needs coordination among banks, payment processors, regulators, technology vendors, and international settlement networks. It is impractical to replace them abruptly, due to their long system lifecycles, strict availability requirements and interoperability dependency. Therefore, a phased approach to continuity is required in the financial sector, starting from the cryptographic inventory, the risk classification, the hybrid deployment, and the standardization of algorithms (Kuka et al., 2026).

7.3 Telecommunications and Critical Infrastructure

The telecommunication networks enable mobile services, emergency communication, industrial systems, cloud connectivity and national infrastructure. The migration in those environments needs to consider the high traffic volumes, the low latency requirements, distributed network componentry and long-lived equipment. Future mobile networks are especially at risk for quantum-safe security, as it is necessary for authentication, roaming, network slicing and device-to-device communication to depend on cryptographic trust. The study of post-quantum secure advanced wireless networks is investigating the integration of resistant algorithms without too much overhead in terms of processing and communication capacity (Sanon & Schotten, 2025). The new generation networks are believed to be sixth-generation networks that are expected to be connected to a large

number of autonomous systems, intelligent devices, and edge platforms. The security architecture they must design should then integrate with the efficient management of identities, distributed trust, and hardware-aware implementation, while also incorporating post-quantum cryptography (PQC) (Kwon et al., 2025).

7.4 Internet of Things and Embedded Systems

Internet of Things devices face unique challenges due to their low memory, processing power, battery life, and communications bandwidth. Larger keys or intensive arithmetic-based post-quantum algorithms might thus be hard to implement without optimization. Polynomial operations can be enhanced by hardware–software co-design as it not only increases the feasibility but also reduces the overhead of the processor and memory (Liu et al., 2024). Also, embedded benchmarking shows that these carefully designed schemes could be practically implemented on resource-constrained microcontrollers (Kannwischer et al., 2019).

7.5 High-Assurance and Hybrid Networks

In cases where the level of assurance is very high, these systems may be made using a hybrid approach to cryptography, post-quantum algorithms, and quantum key distribution. These can be used in government, defense, healthcare, and critical infrastructure applications, but cost and interoperability are important considerations (Vaněk et al., 2026). In general, the matching of standardized algorithms to application-specific performance, security and lifecycle requirements (Paquin et al., 2020) is crucial in the deployment of real-world algorithms.

8. Conclusion

Moving from classical cryptography to post-quantum security is an emerging imperative for governments, industries and digital-service providers alike. The mathematical basis of widely deployed public-key systems, such as RSA, Diffie–Hellman or elliptic-curve cryptography is threatened by quantum computing. The harvest-now-decrypt-later model also compounds the need for migration since important data gathered now could be decrypted later. Lattice-based, hash-based, code-based, and other quantum-resistant methods offer a practical solution to post-quantum cryptography. Now, standardized mechanisms like ML-KEM, ML-DSA and SLH-DSA provide a base for secure key establishment and digital signatures. But algorithm selection is not the only factor that makes adoption a success. Organizations need to perform cryptographic inventories, ensure identification of the long-lived sensitive assets, test the interoperability, consider hardware and software limitations, and build architectures that will be able to incorporate future algorithm changes – crypto-agile architectures. There's also sector-specific planning that needs to be done for real-world deployment. Financial systems need to ensure transaction integrity and regulatory compliance, low latency and scalability must be ensured in the communication network, and embedded systems need to run within tight memory and energy constraints. There are hybrid options which can help with the gradual migration, but there is increased protocol and implementation complexity with hybrid options. Therefore migration should be done in stages, assessed, tested, deployed and monitored. In general, post-quantum security should be viewed as an evolution of the digital infrastructure, not just a cryptographic upgrade. To mitigate risks arising from quantum, early preparation, co-ordinated

governance, standardisation of implementation, secure hardware design and sustained crypto analytic evaluation will be necessary. Flexible and risk-based migration strategies will enable organisations to maintain the confidentiality, authentication and trust of information in future digital ecosystems.

References :

1. Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., ... & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process.
2. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., ... & Smith-Tone, D. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process. US Department of Commerce, NIST, 2, 69.
3. Andrysco, M., Nötzli, A., Brown, F., Jhala, R., & Stefan, D. (2018, October). Towards verified, constant-time floating point operations. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1369-1382).
4. Angom, A., Kar, N., Debbarma, T., & Biswas, P. (2025, March). A survey on Lattice-Based Key Establishment Schemes: Types, Evolution and Advances. In 2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI) (Vol. 3, pp. 1-6). IEEE.
5. Barker, W., Souppaya, M., & Newhouse, W. (2021). Migration to post-quantum cryptography. NIST National Institute of, Standards and Technology and National Cybersecurity, Center of Excellence, 1-15.
6. Basin, D., Linker, F., & Sasse, R. (2024). A formal analysis of the iMessage PQ3 messaging protocol. Apple Inc.
7. Basu, K., Soni, D., Nabeel, M., & Karri, R. (2019). Nist post-quantum cryptography-a hardware evaluation study. Cryptology ePrint Archive.
8. CHENU, M., & SPORTIELLO, L. (2025). Post-Quantum Cryptography, the Journey so far and the Challenges Ahead.
9. Crockett, E., Paquin, C., & Stebila, D. (2019). Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH. Cryptology ePrint Archive.
10. Dam, D. T., Tran, T. H., Hoang, V. P., Pham, C. K., & Hoang, T. T. (2023). A survey of post-quantum cryptography: Start of a new race. Cryptography, 7(3), 40.
11. Dang, V. B., Farahmand, F., Andrzejczak, M., Mohajerani, K., Nguyen, D. T., & Gaj, K. (2020). Implementation and benchmarking of round 2 candidates in the NIST post-quantum cryptography standardization process using hardware and software/hardware co-design approaches. Cryptology ePrint Archive: Report 2020/795.
12. Davis, P. A. E. (2026). Cryptographic Agility in EU Cybersecurity Law: From Concept to

Requirement. Available at SSRN 6985378.

13. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). Crystals-dilithium: A lattice-based digital signature scheme. IACR transactions on cryptographic hardware and embedded systems, 238-268.
14. Fritzmann, T., Sigl, G., & Sepúlveda, J. (2020). RISQ-V: Tightly coupled RISC-V accelerators for post-quantum cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 239-280.
15. Huang, Y., Huang, M., Lei, Z., & Wu, J. (2020). A pure hardware implementation of CRYSTALS-KYBER PQC algorithm through resource reuse. IEICE Electronics Express, 17(17), 20200234-20200234.
16. Jung, E. (2024). The Impact of Quantum Information Science and Technology on National Security (Doctoral dissertation, Purdue University).
17. Kannwischer, M. J., Rijneveld, J., Schwabe, P., & Stoffelen, K. (2019). pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4.
18. Kuka, C., Muhyaddin, S., Teh, P. L., & Davies, L. (2026). Global roadmaps for post-quantum era in finance: Policies, timelines, and a pragmatic playbook for migration. FinTech, 5(1).
19. Kwon, H., Ko, Y., Pawana, I. W. A. J., & You, I. (2025). Toward Quantum-Safe 6G Mobile Networks: A Survey on EAP-AKA Prime Family with Formal Security Analysis and Empirical Evaluation. IEEE Transactions on Consumer Electronics.
20. LaMacchia, B. (2021). The long road ahead to transition to post-quantum cryptography. Communications of the ACM, 65(1), 28-30.
21. Liu, T., Ramachandran, G., & Jurdak, R. (2024). Post-quantum cryptography for internet of things: a survey on performance and optimization. arXiv preprint arXiv:2401.17538.
22. Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (2024). Transition to post-quantum cryptography standards (No. NIST Internal or Interagency Report (NISTIR) 8547 (Draft)). National Institute of Standards and Technology.
23. Newhouse, W., Souppaya, M., Barker, W., Brown, C., Kampanakis, P., Manzano, M., ... & Lee, C. (2023). Migration to post-quantum cryptography: Preparation for considering the implementation and adoption of quantum safe cryptography (No. NIST Special Publication (SP) 1800-38 (Draft)). National Institute of Standards and Technology.
24. Pan, D., Yang, Y., Sun, W., Wang, S., & Wang, K. (2025). ML-GS: Module Lattice-Based Group Signature Scheme. Journal of Information Assurance & Security, 20(3).
25. Paquin, C., Stebila, D., & Tamvada, G. (2020, April). Benchmarking post-quantum cryptography in TLS. In International Conference on Post-Quantum Cryptography (pp. 72-91). Cham: Springer International Publishing.
26. Saarinen, M. J. O. (2024, August). Accelerating SLH-DSA by two orders of magnitude with a single hash

unit. In Annual International Cryptology Conference (pp. 276-304). Cham: Springer Nature Switzerland.

27. Sanon, S. P., & Schotten, H. D. (2025, June). Securing mobile networks in the quantum era: Imperative role of post-quantum cryptography. In 2025 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit) (pp. 721-726). IEEE.
28. Stebila, D. (2024). Security analysis of the iMessage PQ3 protocol. Cryptology ePrint Archive.
29. Stebila, D., Fluhrer, S., Gueron, S., & Haifa, U. (2022, August). Hybrid key exchange in TLS 1.3–draft-ietf-tls-hybrid-design-05.
30. Troublefield, T. C. (2026). Quantum Cybersecurity: A Rising Strategic Imperative. Journal of Quantum Information Science, 16(2), 191-225.
31. Uddin, S. M. M., & Azim, N. (2025). CYBERSECURITY CHALLENGES AND STRATEGIC MIGRATION PATHWAYS IN THE ERA OF QUANTUM COMPUTING: RISKS, STANDARDS, AND POST-QUANTUM CRYPTOGRAPHIC READINESS. Spectrum of Engineering Sciences, 131-141.
32. Vaněk, M., Saadi, N., Isoard, V., Lauterbach, F., & Vozňák, M. (2026, May). Hybridization of Post-Quantum Cryptography and Quantum Key Distribution: A Survey of Key Establishment Approaches. In 2026 49th MIPRO ICT and Electronics Convention (MIPRO) (pp. 746-751). IEEE.
33. Xie, J., Zhao, W., Lee, H., Roy, D. B., & Zhang, X. (2024). Hardware circuits and systems design for post-quantum cryptography—A tutorial brief. IEEE Transactions on Circuits and Systems II: Express Briefs, 71(3), 1670-1676.