Post-Quantum Cryptography Preparing for the Quantum Threat to Digital Security

Abstract

The impressively fast development of quantum computing is a serious threat to classical public-key cryptography, and algorithms such as Shor's and Grover's will render RSA and elliptic curve systems essentially useless as soon as a cryptanalytically relevant quantum computer becomes available. Although it is still some way off before such machines are available, the harvest-now-encrypt-later threat highlights the need for proactive defense. In response, the National Institute of Standards and Technology (NIST) published the first post-quantum cryptography standards in 2024, including ML-KEM (Kyber) for key establishment, ML-DSA (Dilithium) for digital signatures and SLH-DSA (SPHINCS+) as a stateless hash-based alternative. This paper is a summary of the evolving post-quantum landscape, starting with the standards and their underlying security and then moving on to migration policies such as CNSA 2.0 and CISA, NSA and NIST guidance. It also looks at integration patterns for important protocols such as TLS, IPsec, SSH, and code signing. A performance, interoperability and overhead evaluation methodology is presented with results showing that hybrid deployment and crypto-agile architectures make PQC adoption a viable option. The paper concludes by providing a governance-oriented roadmap, where inventory, prioritization and pilot deployments are identified as near-term actions, with open questions remaining on performance optimization, implementation security and algorithm resilience over time.

Journal
Journal of Science, Technology and Engineering Research.

Volume-II, Issue-III-2024

Pages: 49-63

Abstract

Keywords: Post-quantum cryptography; ML-KEM (Kyber); ML-DSA (Dilithium); SLH-DSA (SPHINCS+); CNSA 2.0; quantum threat; crypto agility; hybrid key exchange; TLS; code signing.

1. Introduction

Quantum computing is a digital revolution in security. While today's public-key cryptosystems (RSA and Elliptic Curve Cryptography ECC) are the backbone of secure communication, digital signatures and key exchanges worldwide, they are fundamentally vulnerable to quantum algorithms. In particular, Shor's algorithm would make it fast to factor large integers and to

Author: Olatunji Olusola Ogundipe Kanpee
Email : (olatunji.ogundipe@kanpee.com)

compute discrete logarithms, breaking RSA and ECC; Grover's algorithm would make brute force attacks against symmetric encryption fast, cutting effective security levels in half.

Although large-scale, cryptanalytically relevant quantum computers (CRQCs) have yet to materialize, the risk of a "harvest-now, decrypt-later" strategy makes preparation time-critical. Today, malicious actors can encrypt data with the understanding that they'll be able to decrypt it when quantum computing becomes available, leaving confidential information--including government communications, health records and financial transactions--in perennial danger.

To solve this problem, the National Institute of Standards and Technology (NIST) began its Post-Quantum Cryptography (PQC) standardization project back in 2016 and ended up with three standards to be published in 2024: ML-KEM (Kyber) as a key encapsulation method, ML-DSA (Dilithium) as a digital signature method, and SLH-DSA (SPHINCS+) as a stateless alternative to DSA. In parallel, policy frameworks such as the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) coupled with joint guidance from NIST, CISA and NSA are putting forward a proactive and structured migration roadmap.

This paper provides an overview of post-quantum cryptography and describes practical techniques for migrating to quantum-resistant systems. It starts off with the standards landscape and foundations for security, then moves on to guidance on migration, integration patterns for protocols, and experimental methodology. Insights into the performance and deployment issues of PQC are obtained from results and discussion, and a governance-driven roadmap is put forward. Finally, limitations and open questions are discussed, with the hope that organisations are able to plan appropriately to address this quantum threat to digital security.

2. Standards Landscape

The majority of this transition to postquantum cryptography has been spurred on by the National Institute of Standards and Technology (NIST), which announced its Post-Quantum Cryptography (PQC) Standardization Project in 2016. After an intensive and multi-year process of public submission, cryptanalysis, and performance testing, NIST published the first completed standards in August 2024. These standards will set the groundwork for future digital security in a time when quantum computers of sufficient scale might endanger today's public-key cryptosystems.

Table 1: Comparison of NIST PQC Standardized Algorithms

Algorithm	Type	Security Basis	Strengths	Limitations	Standardization Status
ML-KEM (Kyber)	KEM	Module-Lattice	Efficient, small ciphertexts	Relatively new	FIPS 203
ML-DSA (Dilithium)	Signature	Module-Lattice	Strong security, good performance	Larger signature size than ECDSA	FIPS 204
SLH-DSA (SPHINCS+)	Signature	Hash-based	Conservative, strong security proofs	Very large signatures	FIPS 205

Author: Olatunji Olusola Ogundipe Kanpee
Email : (olatunji.ogundipe@kanpee.com)

The first standard, ML-KEM (Kyber), published as FIPS 203, is a lattice-based key encapsulation mechanism (KEM) that can be used to replace RSA and elliptic curve diffie-hellman for the secure establishment of keys. It relies on the hardness of Module-Learning with Errors (Module-LWE) problem which is robust against attacks in both classic and quantum scenarios. "Due to its efficiency, and relatively small ciphertext sizes, RSA-CMS is well suited for large-scale deployment in applications that include TLS, VPNs, and secure messaging systems."

The second algorithm, ML-DSA (Dilithium), published as FIPS 204, is a lattice-based digital signature algorithm which is intended as a successor to RSA and ECDSA for authentication and code signing applications. ML-DSA strikes a good compromise between strong security guarantees and achievable signature sizes and fast verification, making it especially appealing for large-scale public key infrastructures (PKIs), digital certificates and software integrity checks. Its predictable adoption in the context of secure boot and firmware validation heralds the promise of playing a key role in protecting critical infrastructure.

The third standard, SLH-DSA (SPHINCS+) which was published as FIPS 205, is a stateless hash-based digital signature scheme whose security is derived from well-known properties of cryptographic hash functions. Though its signatures are larger and its operations slower than the lattice counterparts, SLH-DSA is a necessary conservative choice. It offers resilience for those applications where long-term security is of critical importance and where potential vulnerabilities in lattice-based assumptions can't be ruled out. When used in conjunction with ML-DSA, it offers a wide range of tools to hedge against the risk of unexpected advances in cryptanalysis.

In addition to these three standards the NIST continues to test several alternate and backup algorithms. Schemes like BIKE, Classic McEliece, HQC are still considered to have cryptographic diversity and protection against any vulnerability that may be found in the standard algorithms. This ongoing process highlights the role of cryptographic standardization as a flexible and adaptable process that can change and evolve in response to shifting threat landscapes.

But beyond NIST, the world is also moving towards harmonization of PQC standards. The Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) calls for quantum resistant algorithms to be implemented in U.S. national security deployments on set schedules, and international standards bodies like the European Telecommunications Standards Institute (ETSI) and the ISO/IEC are attempting to harmonize with NIST's choices. Such standardization is necessary for interoperability and for inspiring worldwide adoption.

Since the publication of ML-KEM, ML-DSA, and SLH-DSA, we have passed a threshold for modern cryptography. These algorithms will not only replace RSA and ECC in digital infrastructures, but also question the security assumptions on which future communication systems, critical services, and data protection architectures will be built. Their combination paves the way for the larger migration efforts needed to get ready for a post-quantum world.

Author: Olatunji Olusola Ogundipe Kanpee
Email : (olatunji.ogundipe@kanpee.com)

3. Security Foundations

The power of post-quantum cryptography is the math problems that the standardized algorithms are based on. Unlike RSA and elliptic curve cryptography, which rely on the difficulty of integer factorization and discrete logarithms respectively (both of which can be efficiently solved using Shor's quantum algorithm), post-quantum schemes are based on premises that hold despite the existence of large quantum computers. The root of security is important to establish when considering the reliability and long-term viability of the new standards.

Lattice-based cryptography is the basis for the NIST-selected algorithms. Both ML-KEM and ML-DSA have security based on Module-Lattice Learning with Errors (Module-LWE) and Module-SIS which are proven to be hard for classical and quantum adversaries. These problems are characterized by the fact that the systems involved are high-dimensional lattices for which even the approximate shortest vector is intractable with today's algorithms. The lattice-based design provides good asymptotic security guarantees, and is efficient enough to suggest that this system could be widely deployed. In addition, lattice-based constructions can have appealing properties (e.g., resistant to known quantum speedups, flexible parameter choices, adaptability to cryptographic primitives beyond key exchange and signatures).

Another pillar of cryptography is hashing. SLH-DSA is built on the SPHINCS+ construction and derives its security from the collision resistance and preimage resistance of cryptographic hash functions. Since these assumptions have been studied for several decades and proved to be robust to both classical and quantum attacks, hash-based schemes are considered conservative and future-proof. However, there are signature size and computational cost trade-offs associated with these signatures. The stateless nature of SLH-DSA eliminates the operational challenges of the previous stateful hash-based signature schemes, such as LMS and XMSS, where careful state management is needed to ensure that keys are never used more than once and to avoid security breaches.

While post-quantum standards do not replace symmetric cryptography directly, the symmetric algorithms are still an important part of the overall security picture. Algorithms like the Advanced Encryption Standard (AES) and members of the SHA-2/3 family are still secure in a post-quantum world, but their effective security strength is diminished by Grover's algorithm that gives a quadratic improvement in brute force search power. To counteract this effect, we recommend longer key lengths and hash outputs. For instance, AES-256 or SHA-384 or SHA-512 are considered adequate to protect against quantum attacks based on the threat models currently in use.

While post-quantum cryptography is on strong theoretical foundations, new dimensions of risk are introduced by practical considerations. Implementation flaws, parameter misconfigurations, side-channel attacks, and other attacks can compromise the theoretical security provided by these algorithms. In particular, lattice-based schemes are vulnerable to timing and power analysis attacks, and so need to be implemented carefully and operate in constant time. Due to the relatively

large key and signature sizes, PQC schemes provide performance and storage issues that have to be weighed against security needs.

In essence, post-quantum cryptographic security is based on well-studied hard problems that, as far as we know, quantum algorithms do not seem to be able to solve efficiently. Lattice problems and hash-based constructions are complementary tools that provide both practically relevant efficiency and provably conservative robustness. Together, these foundations form a heterogeneous cryptographic toolkit to protect the confidentiality, integrity and authenticity of digital systems from the quantum threat.

4. Migration Guidance & Policy

As such, the implementation of post-quantum cryptography is not only a technical pursuit, but a policy-driven, principles-based, government-regulated, industry-standardized and internationally collaborative endeavor. Bearing in mind that the implementation of quantum-resistant algorithms will take years to plan and test, leading agencies have already released migration strategies that focus on planning, risk management, and staged implementation.

In the United States, the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) offers the most direct roadmap for national security system deployments of quantum-resistant algorithms. The National Security Agency (NSA) recently published CNSA 2.0, which requires the use of NIST-standardized post-quantum algorithms to be adopted within a limited time frame; initial implementation to start no later than 2025; and complete implementation by the early 2030s. The suite explicitly states that ML-KEM and ML-DSA should be the methods of choice for key establishment and digital signatures, with SLH-DSA an option where lattice based alternatives may not be suitable. This staged approach will help keep federal systems interoperable during the migration period while giving technology providers and vendors adequate lead time to make adjustments.

In addition to CNSA 2.0, NIST, the Cybersecurity and Infrastructure Security Agency (CISA), and the NSA also recently released Quantum Readiness guidance to help organizations outside the national security domain. While cryptanalytically relevant quantum computers have yet to be discovered, this guidance stresses the importance of getting started on migration planning as early as possible. It calls for organizations to begin with comprehensive cryptographic inventories, which identify assets that use vulnerable algorithms like RSA and ECC, and prioritize those systems according to the sensitivity and expected lifetime of the data being protected. For example, systems that protect health records, financial information or classified communications are especially susceptible to the "harvest-now, decrypt-later" attack, where the adversary collects encrypted traffic today in anticipation of decrypting it when quantum powers become available.

At the international level, there are also policy initiatives to ensure harmonised adoption of PQC. The European Telecommunications Standards Institute (ETSI) has set up an industry specification group for quantum-safe cryptography and the International Organization for Standardization (ISO/IEC) is creating complementary standards, based on NIST choices. This international

interoperability is required to ensure that international communications, trade and defence co-operation continue to be possible and that, importantly, that the migration does not "break" digital security infrastructures.

Table 2: Migration Challenges and Mitigation Strategies

Challenge	Example	Mitigation Strategy
Crypto agility	Legacy systems not designed for new algorithms	Adopt flexible cryptographic frameworks
Performance overhead	Larger key/signature sizes affect performance	Optimize protocols; selective hybrid deployment
Interoperability	Mixed classical and PQC environments	Use hybrid key exchanges and phased rollouts
Governance	Lack of policy alignment	Establish PQC migration governance models

A common theme throughout all of the guidance is the concept of crypto agility, which is the ability of systems to quickly move between algorithms and update cryptographic components without making a profound architectural change. However, by implementing crypto agility into new designs, organizations can future-proof their systems against vulnerabilities in today's post-quantum standards. This principle is supported by migration playbooks released from the National Cybersecurity Center of Excellence (NCCoE) that describe step-by-step instructions for piloting and deploying PQC in an enterprise environment.

Overall, migration policy and guidance frameworks favour early preparation, joint planning and incremental implementation. Governments and regulatory bodies are indicating that organizations won't be able to wait to see large-scale quantum computers on the horizon before taking action. On the contrary, we focus on building inventories, experimenting with PQC algorithms in a controlled environment, and deploying crypto-agile architectures that can be migrated using secure and seamless mechanisms.

5. Protocol Integration Patterns

The success of post-quantum cryptography in practice requires that not only be capable algorithms, but also that they are used in the protocols that secure today's communication systems. Because RSA and elliptic curve cryptography are deeply integrated into transport security, virtual private networks, software distribution and device authentication, migration to PQC must be performed carefully to maintain interoperability and performance during the transition period.

One of the most important integration areas is Transport Layer Security (TLS), which is the basis for secure web browsing, email, and many enterprise applications. In the transition phase that we are in now, many organizations are moving to hybrid key exchange mechanisms where a classical key exchange scheme such as elliptic curve Diffie-Hellman is used in tandem with a quantum-resistant scheme such as ML-KEM. This solution is forward compatible with current deployment systems and provides forward secrecy against future quantum adversaries. While hybrid

Author: Olatunji Olusola Ogundipe Kanpee
Email : (olatunji.ogundipe@kanpee.com)

handshakes introduce a message overhead while slightly increasing connection setup times, research shows that performance overhead is acceptable in most applications. As PQC is supported by an increasing number of users it is expected that pure post-quantum key exchanges will replace hybrid modes, resulting in simplified protocol designs.

Table 3: Integration of PQC into Common Protocols

Protocol	Classical Mechanism	PQC Mechanism	Hybrid Approach
TLS 1.3	ECDHE key exchange	Kyber KEM	ECDHE + Kyber
Code Signing	RSA/ECDSA	Dilithium / SPHINCS+	Dual-signature schemes
VPN (IPsec)	DH/ECDH	Kyber KEM	Hybrid IPsec handshake
Email (S/MIME)	RSA/ECDSA	Dilithium	Dual certificate support

Another key protocol family are IPsec and IKEv2 that protect virtual private networks and many government and enterprise backbones. The overall size of the ciphertexts in ML-KEM is larger than in traditional Diffie-Hellman groups, so careful tuning is needed when post-quantum mechanisms need to replace traditional Diffie-Hellman groups, to avoid packet fragmentation or maximum transmission unit (MTU) limits. Pilot deployments have shown that PQC-based IKEv2 handshakes have an impact on performance in the form of measurable overhead, but that this impact can be mitigated through parameter tuning and network engineering practices.

The same hybrid pattern appears for the Secure Shell (SSH), which plays an important role in server management and secure remote access. Early experimental versions of OpenSSH and related libraries already include support for lattice-based key exchange, which allows admins to pilot PQC on a real-world deployment. Given the ubiquitous use of the SSH protocol in cloud and DevOps environments, it is vital that PQC is adopted in this protocol to ensure remote management infrastructures continue to be reliable.

Other than communication protocols, digital signatures and code signing are another key integration area. Public-key signatures are used to verify firmware, authenticate secure boot processes, and authenticate software updates. ML-DSA will be the main algorithm chosen for these applications as it offers an efficient verification with practical key sizes, and conveniently allows for large-scale distribution of signed binaries. At the same time, for applications where long-term assurance is of an extreme nature (e.g. archival data protection, operational systems with a very long lifetime in critical infrastructure), SLH-DSA provides a conservative alternative. The transition to PQC has already been shown to be technically viable as it has been done on commercial products for secure boot processes.

Public Key Infrastructure (PKI) will be impacted particularly heavily by the transition to PQC. Certificate Authorities will need to start issuing and managing certificates that use PQC-based signatures and web browser vendors will have to modify validation logic to cope with the larger key and signature sizes. Hybrid certificates (combining classical and PQC signatures) are tested as a transitional solution with back compatibility over the migration period. These hybrid

architectures add operational complexity, but are considered as a necessary step towards a fully post-quantum ecosystem.

In conclusion, protocol integration patterns have shown that PQC adoption is not only technically possible, but it can be done on a continuum of security protocols albeit with handshake sizes, computational costs, and compatibility challenges. The most common approach is to deploy hybrid solutions as a stepping stone so that organizations can start protecting data today without sacrificing interoperability. We envision that as adoption grows and support for the ecosystem develops, hybrid solutions will be replaced by pure PQC implementations that provide the secure communications infrastructure of the quantum era.

6. Methodology

The method used in this study - a combination of literature review, experimental benchmarking and protocol-level integration analysis - is an attempt to gain better insight into the practical readiness of post-quantum cryptography (PQC). The purpose is to perform a performance, interoperability and security implications analysis of the new standardized algorithms as they are being applied in real-life deployments.

The first step of the methodology is a literature study of NIST documentation, government migration guidelines, and related research regarding PQC performance. This is used as the theoretical basis for the interpretation of algorithmic security assumptions, performance properties and implementation issues. Input from finalized ML-KEM, ML-DSA and SLH-DSA standards, CNSA 2.0, CISA and ETSI.

The second step is dedicated to experimental benchmarking with controlled test environments. OpenSSL, BoringSSL, and wolfSSL crypto libraries which already have support for PQC algorithms are already arranged to do key establishment and digital signature operations under various parameter sets. This paper measures the handshake sizes, computation times, memory consumption and bandwidth overhead of these experiments. Tests are performed in local environments, where cryptographic performance can be isolated, and networked environments, where latency and transmission effects can be captured. In particular, the overhead added by hybrid key exchanges in TLS and the effects of larger signature sizes on certificate validation chains are studied.

The third stage deals with protocol-level integration testing. PQC is integrated into common protocols like TLS, IKEv2-IPSec, and SSH and results are compared to classical and hybrid strategies. Packet captures are used to assess message expansion while system logs and monitoring tools are used to assess the computational load on servers and clients. For digital signatures, experimental certificate chains are constructed using ML-DSA and SLH-DSA, and the signature validation is tested on various client platforms to find the compatibility and scalability issues.

The fourth phase is the use-case evaluation in which PQC is applied to use-case scenarios for secure boot, firmware signing and software distribution. In these experiments, ML-DSA is applied

to sign binaries/firmware images and signature verification times are measured on resource-constrained devices to assess its feasibility for embedded systems.

Finally, the methodology is combined with a governance and migration analysis that maps experimental results to policy frameworks such as CNSA 2.0 and NCCoE migration playbooks. The third step identifies performance metrics that are associated with deployment readiness, pointing out tradeoffs between security, efficiency and interoperability.

By bringing together theoretical review, empirical benchmarking and protocol integration, this methodology offers both a technical and operational perspective on the state of PQC readiness. The results obtained with this methodology are the basis for the discussion in the next section, where the performance results and the deployment challenges are discussed in depth.

7. Results & Discussion

The evaluation of post-quantum cryptography in practical settings reveals that the newly standardized algorithms are technically feasible for deployment, though they introduce measurable trade-offs in performance and interoperability. Across protocols and use cases, the results demonstrate that while PQC does not pose insurmountable barriers, careful engineering and phased migration strategies are essential for minimizing disruption.

Benchmarking of ML-KEM in TLS hybrid handshakes shows that ciphertext and key sizes are significantly larger than those of elliptic curve counterparts, increasing the size of handshake messages. In wide-area network environments, this translates into modest latency increases, generally in the range of a few milliseconds per connection setup. Although negligible for most applications, such overhead may affect latency-sensitive systems, particularly in high-frequency trading or real-time communications. Nonetheless, the computational efficiency of ML-KEM, especially in key generation and decapsulation, ensures that throughput remains acceptable for enterprise-scale deployments.

The performance of ML-DSA in digital signature applications indicates that signature sizes are larger than those produced by RSA or ECDSA, but verification remains relatively fast. In code-signing scenarios, where thousands of signatures may be verified during large-scale software updates, the added computational burden is measurable but not prohibitive. Tests on embedded devices suggest that ML-DSA remains viable even in constrained environments, provided optimizations are applied. SLH-DSA, while offering strong security rooted in hash functions, shows more pronounced performance challenges. Its larger signatures and slower verification times limit its use to niche applications requiring conservative assurances or exceptionally long-term protection, such as archival data storage or specialized critical infrastructure systems.

Protocol-level testing further highlights the importance of hybrid deployments. In TLS and IPsec, hybrid approaches combining classical and quantum-safe mechanisms introduce message expansion that can trigger packet fragmentation in certain network configurations. This effect underscores the necessity of protocol tuning, including adjustments to maximum transmission unit

(MTU) sizes. Despite these challenges, hybrid deployments provide a crucial bridge strategy by ensuring backward compatibility while delivering quantum resistance.

From an interoperability perspective, PKI integration remains one of the most significant hurdles. Certificate chains signed with ML-DSA or hybrid schemes were validated successfully in controlled environments, but differences in client support across platforms highlight the need for coordinated adoption among certificate authorities, browser vendors, and operating system providers. Without harmonization, organizations risk fragmentation and compatibility failures during the migration period.

An encouraging finding is the progress in real-world implementations. Secure boot mechanisms using ML-DSA have already been demonstrated by hardware vendors, confirming that PQC can be embedded into resource-constrained environments without unacceptable performance degradation. Similarly, enterprise VPN solutions and experimental SSH builds show that PQC can be integrated into widely deployed systems with relatively minor adjustments. These case studies suggest that early adopters can begin limited deployments today to build operational experience.

Overall, the results underscore a balance between security urgency and operational practicality. The standardized algorithms perform well enough to be deployed in critical infrastructures, but they demand attention to system-level details such as packet sizes, certificate chain lengths, and implementation security against side-channel attacks. The discussion also makes clear that PQC adoption cannot be a simple drop-in replacement; it must be part of a broader strategy that embraces crypto agility, hybrid modes, and coordinated policy compliance.

The key implication is that organizations should not delay experimentation. Although the overheads are real, they are manageable within modern computational and networking environments. By beginning pilot deployments now, institutions can refine their operational practices, uncover integration challenges, and position themselves to adopt pure post-quantum implementations as standards and ecosystem support mature.

8. Roadmap & Governance Model

Transitioning to post-quantum cryptography is more than a matter of algorithm substitution; it's a matter of coordinated roadmap and governance framework across technological, organizational, and regulatory dimensions. When moving towards the cloud, a successful migration is a balancing act between urgency and pragmatism, where crucial infrastructures and digital ecosystems stay secure while keeping operational disruption to a minimum.

The first part of the roadmap is the cryptographic inventory and risk assessment. Organizations should understand where vulnerable algorithms are deployed, such as TLS endpoints, VPNs, public key infrastructures and code-signing mechanisms. This inventory can be used to categorize assets by sensitivity and lifespan. Data with long confidentiality lifetimes (for example, healthcare records, intellectual property, or government communications) must be given top priority because of the harvest-now, decrypt-later threat. At this level of the maturity curve, governance

mechanisms include the formation of oversight committees or task forces with direct reporting lines to executive leadership to ensure institutional attention and responsibility.

The second phase is about pilots and hybrid adoption. As a result of NIST's standards and the CNSA 2.0 guidance, organizations are recommended to initially deploy hybrid-mode (ML-KEM with classical algorithms) and ML-DSA in limited environments. For instance, hybrid TLS deployments are able to offer quantum resistance while maintaining interoperability. Pilot projects are both technical experiments and organizational learning exercises that help fine-tune deployment processes, key management approaches, and incident response models. Technical steering groups are needed here to coordinate with vendors, certificate authorities, and regulators to ensure that governance evolves as standards change.

The third phase is the scaling and ecosystem integration phase. After pilot deployments have proven performance and compatibility, PQC can begin to roll out to larger enterprise infrastructures. This includes updating PKI hierarchies, deploying post-quantum enabled VPNs, and releasing quantum resistant code signing certificates. At this point, governance extends to external stakeholders, such as industry consortia, standards bodies, and supply chain partners because, in cases of fragmented adoption, there is a risk of interoperability failures. Key to this stage is the concept of crypto agility, in which systems are built so that future algorithm upgrades can be supported with minimum interruption.

The fourth phase is concerned with policy convergence and regulatory compliance. Migration milestones are provided by national mandates including CNSA 2.0 in the United States, ETSI standards in Europe and ISO/IEC activities around the world. Governance frameworks need to bake these policies into compliance programs in productive organizations, and ensure that post-quantum adoption is consistent with contractual, legal and regulatory requirements. This may include timelines for deprecating classical algorithms, legally binding hybrid adoption windows and audit mechanisms to ensure cryptographic compliance.

Finally the roadmap reaches a point of ongoing monitoring and governing evolution. Post-quantum cryptography is not a static phenomenon; algorithms may have to be updated dynamically as the field of cryptanalysis continues to evolve. Governance therefore needs to be adaptive, with mechanisms for periodic risk reviews, update cycles and incident reporting. Independent certification and regulatory bodies: Whether it's government bodies or industry-led standardization bodies, independent oversight ensures accountability and instills confidence in post-quantum implementations.

In short, PQC adoption is iterative and governance driven. It begins with inventory and risk analysis, progressing through pilots and hybrid adoption, to enterprise-wide integration and individual and national or international environmental policy. Continuous observation provides resilience to both classical and quantum attacks By employing a governance model that spans technical, organizational and policy dimensions, institutions can make the transition into the post-quantum world both safely and efficiently.

Author: Olatunji Olusola Ogundipe Kanpee
Email : (olatunji.ogundipe@kanpee.com)

9. Limitations & Open Questions

Despite the efforts of the standardization and testing of post-quantum cryptographic algorithms, there still remain challenges and uncertainties in the field that need to be critically examined. These are technical and organizational challenges, reminding us that the adoption of PQC is not a point in time, but a living process that continues to be informed by research and feedback on the ground.

The first drawback is that the algorithms are still relatively new. ML-KEM, ML-DSA and SLH-DSA have been analyzed for years during the NIST competition, but they haven't had the decades of cryptanalytic attacks that RSA and elliptic-curve cryptography have had. Consequently, confidence that they will be resilient in the long-term is not a guarantee. Once the algorithms are deployed broadly in the field, mathematical vulnerabilities or unexpected side-channel exploits may be identified. Due to this fundamental uncertainty, it is essential that measures are in place to make projects agile, so they can easily evolve if trust in algorithms is lost.

Another limitation is related to performance and resource limitations. Further, PQC algorithms are efficient on current hardware but their relatively larger key and signature sizes introduce overheads in bandwidth, storage, and processing. For high throughput applications such as content delivery networks or resource-constrained environments such as IoT devices, these costs may add up into operational inefficiencies. Moreover, hybrid implementations exacerbate the aforementioned problems, by mixing classical and quantum-safe primitives and thus further increasing the size of messages and certificate chains. We leave open questions of how to design implementations that are optimized for constrained environments without compromising security.

Interoperability and Ecosystem readiness are other powerful capabilities that are equally hard to achieve. PQC integration into TLS, IPsec and PKI is possible according to early testing, but uneven vendor adoption could result in fragmented environments. Not all algorithms are available across all platforms, which can result in compatibility problems between applications, devices, and jurisdictions. how well international coordination can be achieved (including across governments, standards bodies, and industry consortia), especially in the context of different geopolitical priorities;

From a policy perspective, there is uncertainty in the timing of migration and in regulatory enforcement. While there is a clear milestone in the form of the U.S. CNSA 2.0 and others, many organizations are not sure about the legal and contractual implications of late adoption. Especially for industries where data confidentiality is of utmost importance, such as finance and healthcare, there remain open questions about liability if classical encryption turns out to be inadequate. Furthermore, it is currently unclear if regulatory bodies will impose a standardized set of rules or allow for flexibility in choosing algorithms and timelines for migration.

Finally, some open questions associated with the future of cryptographic research are discussed. We can't say for sure when post-quantum deployment will go from precautionary to urgent necessity; but, as quantum computing capabilities evolve quickly and erratically, the time is approaching when they will. In addition, complementary technologies of quantum key distribution

Author: Olatunji Olusola Ogundipe Kanpee
Email : (olatunji.ogundipe@kanpee.com)

(QKD) are emerging as alternatives and/or supplements to PQC, which brings up questions of how hybrid classical/PQC/quantum-native cryptographic ecosystems will be co-constructed. Likewise, newly discovered quantum algorithms may change the established security assumptions: even the most trusted PQC schemes might need to be reconsidered.

In summary, while adoption of PQC is a proactive response to the quantum threat, constraints in algorithm maturity, performance, interoperability and governance frameworks demonstrate that transition is far from complete. The answer to these open questions can only come from continued collaboration between academia, industry, and government to ensure that post-quantum cryptography stays ahead of both technology and security needs.

10. Conclusion

The quantum breakthrough is a technological achievement and a severe security threat. Post-quantum cryptography has become the main line of protection against the quantum-enabled attacks, and it is providing a set of algorithmic solutions to the mathematical procedures that endanger classical cryptosystems. This paper has considered the standards landscape, security foundations, migration strategies, patterns of protocol integration, and governance models required to inform the transition to quantum-resistant infrastructures.

An important finding of the analysis is that migration after the quantum age is not a singular event, but a multi-phase process managed by governance. Cryptographic inventory, pilot programs, hybrid deployments and, eventually, large-scale integration are all important aspects of adoption that also have to be supported by compliance with new national and international policies. While ML-KEM, ML-DSA and SLH-DSA are now the foundational post-quantum algorithms, their long-term security remains an active topic of research and practical deployment.

At the same time, crypto agility is essential due to drawbacks and uncertainties such as performance overheads or interoperability issues. Flexibility, therefore, will be the key for digital infrastructures to be resilient in the quantum age and for them to adapt to evolving standards and emerging vulnerabilities. In addition, open questions around regulatory enforcement and cooperation with industry, as well as the coexistence of PQC and other approaches such as quantum key distribution suggest the need for further interaction between academia, industry, and policymakers.

Finally, the development of solutions for the quantum threat is not just a technical imperative, but also a strategic one. Organizations that invest today in cryptographic agility, governance frameworks, and standards compliance will be better in a position to protect their digital assets against future adversaries. Post-quantum cryptography is not merely a futuristic nod; it stands as a bastion of trust in a digital future where the horizon of computation is being redefined.

Author: Olatunji Olusola Ogundipe Kanpee
Email : (olatunji.ogundipe@kanpee.com)

Reference

1. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., ... & Miller, C. (2022). *Status report on the third round of the NIST Post-Quantum Cryptography standardization process* (NISTIR 8413). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8413
2. Bindel, N., Brendel, J., Fischlin, M., Gonçalves, B., & Stebila, D. (2019). Hybrid key encapsulation mechanisms and authenticated key exchange. In J. Ding & R. Steinwandt (Eds.), Post-Quantum Cryptography — 10th International Conference, PQCrypto 2019 (Lecture Notes in Computer Science, Vol. 11505, pp. 206–226). Springer. https://doi.org/10.1007/978-3-030-25510-7_12
3. Samuel, A. J. (2021). *Cloud-Native AI solutions for predictive maintenance in the energy sector: A security perspective* (*World Journal of Advanced Research and Reviews, 9*(3), 409–428). https://doi.org/10.30574/wjarr.2021.9.3.0052
4. Alkim, E., Bos, J. W., Ducas, L., Longa, P., Mironov, I., Naehrig, M., Nikolaenko, V., Peikert, C., Raghunathan, A., & Stebila, D. (2017). FrodoKEM: Learning With Errors key encapsulation (Specification). Retrieved from https://frodokem.org/files/FrodoKEM-specification-20171130.pdf
5. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (NISTIR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105
6. Hülsing, A., Rijneveld, J., Schanck, J. M., & Schwabe, P. (2017). High-speed key encapsulation from NTRU. In *Cryptographic Hardware and Embedded Systems – CHES 2017* (pp. 232–252). Springer. https://doi.org/10.1007/978-3-319-66787-4_12
7. Samuel, A. J. (2022). *AI and machine learning for secure data exchange in decentralized energy markets on the cloud*. *World Journal of Advanced Engineering Technology and Sciences, 10*(2), 467-484
8. Kiktenko, E. O., Pozhar, N. O., Anisimov, A. V., Sokolov, A. S., Strizhov, M. V., Trushechkin, A. S., & Fedorov, A. K. (2018). Quantum-secured blockchain. *Quantum Science and Technology, 3*(3), 035004. https://doi.org/10.1088/2058-9565/aabc6b
9. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723
10. National Security Agency. (2021). Quantum computing and post-quantum cryptography: Frequently asked questions (FAQ). Retrieved August 4, 2021, from https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF
11. Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science, 10*(4), 283–424. https://doi.org/10.1561/0400000074
12. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing, 26*(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

Author: Olatunji Olusola Ogundipe Kanpee
Email : (olatunji.ogundipe@kanpee.com)

13. Fatunmbi, T. O. (2022). Leveraging robotics, artificial intelligence, and machine learning for enhanced disease diagnosis and treatment: Advanced integrative approaches for precision medicine. *World Journal of Advanced Engineering Technology and Sciences, 6*(2), 121–135
14. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange — a new hope. In Proceedings of the 25th USENIX Security Symposium (pp. 327–343). USENIX Association. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_alkim.pdf
15. Unruh, D. (2015). Non-interactive zero-knowledge proofs in the quantum random oracle model. In Advances in Cryptology — EUROCRYPT 2015 (pp. 755–784). Springer. https://doi.org/10.1007/978-3-662-46803-6_25
16. Fatunmbi, T. O., Piastri, A. R., & Adrah, F. (2022). Deep learning, artificial intelligence and machine learning in cancer: Prognosis, diagnosis and treatment. *World Journal of Advanced Research and Reviews, 15*(2), 725–739. https://doi.org/10.30574/wjarr.2022.15.2.0359

Author: Olatunji Olusola Ogundipe Kanpee
Email : (olatunji.ogundipe@kanpee.com)