JOURNAL OF POST-QUANTUM CRYPTOGRAPHY AND SYSTEMS

RESEARCH ARTICLE

Volume 01, Issue 02, 2026

Post-Quantum Cryptography for Secure Digital Infrastructures: Algorithms, Implementation Challenges, Standardization, and Future Research Directions

Manmohan Singh

Department of Computer Application, National Institute of Technology Kurukshetra, Kurukshetra, Haryana, India

ABSTRACT

Post-quantum cryptography has emerged as a critical response to the anticipated threat that quantum computing poses to conventional public-key systems and long-term digital security. This review examines the principal post-quantum algorithm families, including lattice-based, code-based, hash-based, multivariate, and isogeny-based approaches, with attention to their security assumptions, operational strengths, and practical limitations. It evaluates key encapsulation mechanisms and digital signature schemes used to protect authentication, confidentiality, integrity, and secure key exchange across modern digital infrastructures. Major implementation challenges include large keys and signatures, increased computational and memory requirements, bandwidth overhead, side-channel exposure, hardware constraints, and compatibility with legacy systems. The review also assesses protocol-level integration across public-key infrastructures, TLS, wireless networks, cloud platforms, industrial systems, blockchain environments, and constrained Internet of Things devices. Standardization, interoperability, regulatory alignment, hybrid deployment, and cryptographic agility are identified as central requirements for secure migration. Existing evidence remains limited by heterogeneous benchmarking methods, rapidly evolving standards, and insufficient large-scale production data. Future research should prioritize lightweight designs, validated hardware implementations, automated migration tools, standardized performance evaluation, and longitudinal deployment studies. Early, coordinated, and phased adoption of post-quantum cryptography is essential to reduce harvest-now-decrypt-later risks and strengthen the long-term resilience of critical digital ecosystems worldwide before cryptographically relevant quantum computers can compromise widely deployed classical cryptographic protections.

Keywords:Cryptographic agility, Digital infrastructure, Post-quantum cryptography, Quantum computing, Standardization

1. Introduction

Today, digital infrastructures support government services, financial systems, healthcare systems, industry processes, cloud computing and telecommunications, as well as everyday communication. They rely heavily on mechanisms of cryptography for confidentiality, integrity, authentication, and non-repudiation of their security. Most modern systems are based on public-key cryptography, like elliptic-curve cryptography and RSA, as well as symmetric cryptography and hashing. Public-key cryptography (like elliptic-curve cryptography and RSA), symmetric cryptography, and hashing are most common in today's systems to set up trust in distributed environments. Under classical computational models, this architecture works well, but the ongoing progress of quantum computing poses challenges to classical models and creates a strategic cybersecurity problem for organizations needing to safeguard sensitive data for extended periods of time. Optimal technologies can support optimization, analytics, and threat detection in the future, but may also provide potential offensive tools against widely used cryptographic systems (Singh & Kumar, 2024).

The main issue is quantum algorithms that can solve some problems in mathematics in a considerably quicker time than a classical computer. Shor's algorithm poses a threat to integer factorization and the discrete logarithm problem, the two critical problems that underlie the security of the RSA, Diffie–Hellman, and elliptic-curve systems. However, Grover's algorithm brings a quadratic speedup to the problem of brute-force search, which lowers the effective security margin of symmetric-key algorithms and hash functions. While quantum computers that are already cryptographically relevant are not in use, the development of quantum hardware, error correction, and algorithmic work has led to the concern of future compromises of protected and stored communications and data (Khan et al., 2024). This is especially problematic for information that has extended confidentiality needs, as adversaries could encrypt information right now and decrypt it at some point in the future when the quantum capability is available.

The quantum threat is therefore not future, but present-day threats and risks to management. To withstand quantum attacks, operators of critical infrastructure, defense institutes, and financial and public institutions should consider the exposure of cryptographic methods, the dependency of systems, and data-retention requirements (Sodiya et al., 2024). The challenge is exacerbated by the proliferation of inter-connected environments like the Internet of Things, Fog Computing, Edge Platforms, Machine-to-Machine (M2M) communication, where devices can be heterogeneous and may have limited processing capacity, memory, bandwidth, and ability to be updated (De Macêdo et al., 2025). Such limitations, along with the fact that migration is more challenging than just replacing algorithms, pose obstacles to the adoption of quantum-resistant mechanisms.

Perhaps most importantly, a software-based solution has emerged as the main approach to this threat – that of post-quantum cryptography. It's a type of cryptographic algorithm that is capable of withstanding attacks from both classical and quantum computers, and that can be implemented on traditional computing systems. The main approaches are lattice-based, code-based, hash-based, multivariate, isogeny-based, etc., which have various compromises in terms of key size, security confidence, signature length, computational cost, and implementation complexity. The major constructions are lattice-based, code-based, hash-based, multivariate, isogeny-based, etc., each with its own set of compromises in terms of key size, security confidence, signature length, computational cost, and implementation complexity (Ravi, 2025). They are used in secure communication

and in other areas that include digital signatures, identity management, software updates, access to the cloud, electronic transactions, and distributed ledgers. Blockchain systems are particularly at risk because the principles of trust they rely on are based on long-lasting public keys and digital signatures that can be subject to attacks using quantum computing (Baseri et al., 2025).

It will take time to move to the post-quantum world, and it is not straightforward. Research has grown at a significant pace, but evidence is now scattered around in various areas of algorithm design, implementing the security of the algorithms, protocol integration, performance benchmarking, and protocol governance on deployment (Barrett-Danes & Ahmad, 2025). The use of the same algorithm in different applications, such as blockchain and IoT, also shows that there is no universal best fit for every application, especially when considering scalability and resources (Wang & Ismail, 2025). There also needs to be coordinated planning of policy, standards, workforce development, and a phased migration approach at the national level, for national security planning (Ahmed, 2024). One more difficulty is that the certificates, anchors of trust, hardware security modules, as well as legacy protocols, will have to be updated without compromising operational continuity, which brings up the question of public-key infrastructures. The question of public-key infrastructures is another challenge, as certificates, anchors of trust, hardware security modules, and legacy protocols will have to be updated without disrupting operational continuity (Yunakovsky et al., 2021).

Special attention is paid to the protection of critical sectors, hardware and software performance, regulatory coordination, side channel resistance, hybrid deployment, and cryptographic agility. Combining these aspects, the review shows the importance of preparation even if the time frame for quantum computing with relevance to cryptography is not clear. The significant post-quantum algorithms, implementation issues, existing standardization activities, migration needs, and future research directions are discussed in this review. It assesses the technical and operational considerations that will play a role in the ability of digital infrastructures to provide quantum-era security that is resilient, interoperable, and scalable.

Objectives of the review:

1. To examine major post-quantum cryptographic algorithms and their security foundations.
2. To evaluate implementation, integration, performance, and standardization challenges.
3. To identify migration priorities and future research directions for secure digital infrastructures.

2. Quantum Computing and the Cryptographic Threat Landscape

The advent of quantum computers poses a new paradigm shift in the security paradigm that is currently used in modern digital infrastructure. General public-key systems such as RSA, Diffie–Hellman, and elliptic-curve cryptography require a computational task that can be easily solved on a quantum computer, but not a classical one. Quantum algorithms change this by allowing some calculations to be done more efficiently. With the emergence of quantum capabilities, traditional cryptographic methods could grow increasingly fragile, making it crucial for organizations to adapt their security strategies to a multi-layered approach that includes zero-trust architecture in addition to post-quantum migration (Okika et al., 2025).

The closest competitor is Shor's algorithm, which would be able to perform integer factorization and discrete logarithm problems in polynomial time on a powerful quantum computer. It would violate the mathematical principles of popular public-key encryption techniques and damage encrypted communications, digital signatures, certificates, and identity-management systems. However, Grover's algorithm poses a different threat as it can speed up the brute-force search against symmetric encryption and hash functions, thus narrowing their security gaps and requiring bigger keys and stronger parameters (Mohammed, 2024).

This threat is exacerbated by the "harvest, now decrypt later" approaches, where adversaries harvest the encrypted data before quantum computers exist and store it for future decryption. Government, financial, healthcare, and defence information, which is likely to be long-lived, is especially vulnerable as the confidentiality requirements could last beyond the timeframe of migration. It is important to understand that quantum-safe security needs to be proactive, not reactive, and that means conducting an inventory of cryptographic functions, understanding the risks associated with those functions, and planning for their replacement (Chhetri et al., 2025).

Legacy systems, protocol dependencies, certificate infrastructures, and operational continuity will also need to be taken into consideration when creating transition plans. To prepare effectively, migration roadmaps need to be coordinated, hybrid cryptographic models are required, there should be interoperability testing, and deployment should be done in stages, across critical systems (Cherkaoui Dekkaki et al., 2024). The figure below shows the threat of quantum computing to classical public-key cryptography by Shor's algorithm.

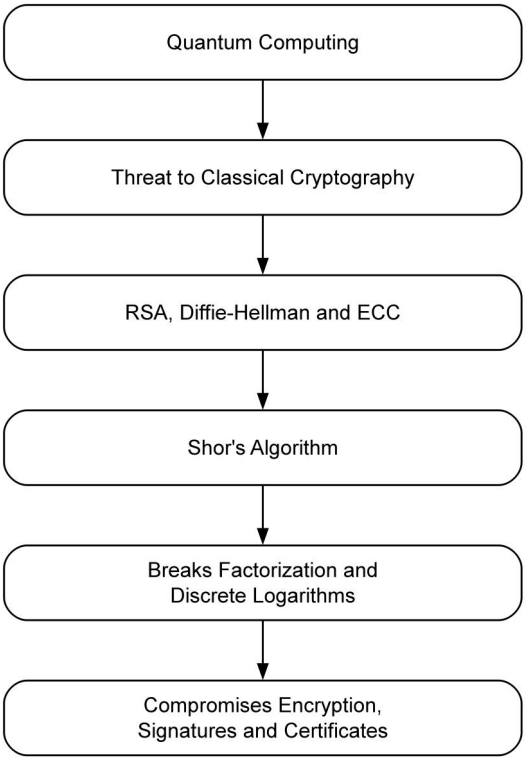

Figure 1. Quantum Computing Threat Pathway to Classical Public-Key Cryptography

3. Foundations and Security Assumptions of Post-Quantum Cryptography

The foundations of post-quantum cryptography are problems thought to be tough to solve for an exhaustive number of classical and quantum computers. While quantum cryptography is tailored for specialized quantum communication systems, post-quantum algorithms are engineered to run on traditional computers and on current digital communications systems and protocols. They are secure since they rely on other hardness problems that can be extracted from different fields such as lattices, error-correcting codes, hash functions, multivariate equations, and other constructions instead of factorization and discrete-logarithm problems. Standardization initiatives consider not only theoretical resistance to quantum attacks but also consideration of parameters, implementation reliability, interoperability, and long-term cryptanalytic confidence (Darzi et al., 2023).

Lattice-based cryptography has become the most popular solution due to its ability to ensure that cryptographic functions, such as encryption, key encapsulation, digital signatures, and more, can be implemented with relatively efficient performance. It is usually secured by problems like Learning With Errors, Ring Learning With Errors, Module Learning With Errors, and the Shortest Vector Problem. These assumptions add carefully designed noise to algebraic systems, making it difficult to recover the secret information from the system without the use of a computer. Though memory consumption, key size, bandwidth requirements, and implementation difficulty are still critical limitations, lattice-based schemes are especially pertinent for IoT networks due to their relatively good efficiency and flexibility.

Mathematical and operational assumptions need to be taken into account for security analysis. Despite the high quality of formal proofs, a scheme can have many security vulnerabilities via side channels, weak randomness, sampling errors, misused parameters, or insecure software optimizations. It is important to check key sharing mechanisms, as leakages of secret values or non-valid ciphertexts can be generated due to small implementation mistakes. A strong post-quantum security will thus require conservative parameters, validated implementations, constant-time operations, and ongoing assessment of classical and quantum cryptanalytic attacks (Ravi et al., 2021).

4. Major Families of Post-Quantum Cryptographic Algorithms

Typical post-quantum cryptographic algorithms are categorized based on the mathematical problems that they solve. Lattice-based, code-based, hash-based, multivariate, and isogeny-based are the main families of cryptography. Every family has its own pros and cons with respect to computation speed, key size, signature size, implementation difficulty, and resistance to known attacks. Currently, lattice-based schemes are the most popular due to their practical performance in many computing environments, and because they support important functions such as key encapsulation, cryptography, and digital signatures. While code-based systems can offer robust security guarantees, they tend to involve relatively large public keys, while hash-based signatures allow for more conservative security assumptions but result in more cumbersome signatures and limited capability (Sane & Patel, 2025).

Multivariate cryptography is based on the hardness of solving a set of non-linear polynomial equations in finite fields. These schemes can be designed to offer rapid signing operations; however, there have been several proposals that have been weakened by structural cryptanalysis. Isogeny-based cryptography had long been viewed as desirable due to its small key sizes,

but major attacks against popular constructions have shown that continued cryptanalytic scrutiny must be performed before implementation. The developments demonstrate that the diversity of algorithms is vital not only because of their ability to resist common errors but also because of the possibility of their becoming vulnerable in the future if any attacks compromise their base mathematical assumption (Paul & Trivedi, 2022).

In the lattice-based family, there are constructions based on Learning With Errors, Ring Learning With Errors, and Module Learning With Errors. Module-based designs aim to achieve a balance between the efficient security of structured arrangements and the relatively more conservative security of less structured designs. They have proven to be strong contenders for realistic migration due to their performance, scalability, and compatibility with the existing protocols, but further steps are required for parameter security and side-channel resistance (Angom et al., 2025). Table 1 implies that the post-quantum algorithm families have various security attributes, efficiency, key sizes, and degree of maturity.

Table 1. Comparative Overview of Major Post-Quantum Cryptographic Families

Algorithm family	Underlying security assumption	Principal applications	Main advantages	Key limitations	In-text citation
Lattice-based cryptography	Learning With Errors, Ring Learning With Errors, Module Learning With Errors, Shortest Vector Problem	Key encapsulation, encryption, digital signatures, advanced cryptographic functions	Strong versatility, efficient computation, broad protocol compatibility	Large keys and ciphertexts, implementation complexity, side-channel risks	(Sane & Patel, 2025; Angom et al., 2025)
Code-based cryptography	Difficulty of decoding random linear error-correcting codes	Public-key encryption and key establishment	Long-standing security assumptions and strong resistance to known quantum attacks	Very large public keys and substantial storage requirements	(Paul & Trivedi, 2022)
Hash-based cryptography	Security of cryptographic hash functions	Digital signatures, software authentication, firmware signing	Conservative security assumptions and strong cryptanalytic confidence	Large signatures, restricted functionality, and possible state-management requirements	(Sane & Patel, 2025)
Multivariate cryptography	Difficulty of solving nonlinear multivariate polynomial equations	Primarily digital signatures	Potentially fast signing operations	Several constructions have been compromised by structural attacks	(Paul & Trivedi, 2022)
Isogeny-based cryptography	Difficulty of finding mappings between elliptic curves	Key exchange and compact public-key mechanisms	Historically attractive because of compact key sizes	Major cryptanalytic attacks have weakened confidence in prominent schemes	(Paul & Trivedi, 2022)

5. Post-Quantum Key Encapsulation and Encryption Algorithms

Post-quantum key encapsulation mechanisms are mechanisms that are designed to provide a secure establishment of shared cryptographic secrets even in the presence of adversaries that have quantum capabilities. They are typically based on quantum-resistant hardness assumptions, such as lattices, codes, or other assumptions, unlike public-key encryption based on integer factorization or discrete logarithms. They are primarily used to secure the establishment of session keys in protocols like Transport Layer Security, virtual private networks, mobile communications, and secure messaging. Hybrid designs have been proposed for transition use, as they provide the security guarantees of the classical algorithms, with additional security from the quantum algorithms. This is especially applicable to new 6G authentication and key-agreement architectures, which require interoperability, low latency, mobility, and ubiquitous connectivity to a large number of devices to be upheld (Turnip et al., 2025).

The trade-off between cryptographic security and operational efficiency has to be considered for its practical adoption. Encapsulation of public keys and ciphertexts in post-quantum cryptography could be larger than current schemes using elliptic curves, as could the amount of memory required for these schemes, or the processing power required. These constraints are more pronounced with lightweight Internet of Things protocols, when devices may be constrained in terms of energy, bandwidth, storage, and computing power. Therefore, it is essential to select the parameters efficiently, compactly implement the algorithms, and accelerate them in the hardware domain without compromising the security enhancements and affecting the system's responsiveness or battery consumption (Almutairi & Sheldon, 2025).

The two more challenging aspects of Vehicular ad hoc networks are the need for quick secure key exchange between vehicles, roadside units, and decentralized trust entities. Impersonation/replay attacks, privacy issues, intermittent connectivity, and high mobility make deployment difficult. The post-quantum encapsulation mechanisms must therefore be able to provide for fast authentication, easy certificate management, and trust establishment that is robust and not burdened with excessive delay. Protocol redesign, interoperability testing, and coordinated migration across diverse digital ecosystems (AlMarshoud et al., 2024) will be crucial to their successful integration. Table 2 shows the conditions and problems for operating and deploying a post-quantum key encapsulation in digital systems.

Table 2. Post-Quantum Key Encapsulation and Encryption in Digital Systems

Deployment environment	Security requirement	Potential post-quantum approach	Operational challenge	Implementation priority	In-text citation
6G mobile networks	Rapid authentication and secure session-key establishment	Hybrid classical and post-quantum key-agreement protocols	Low-latency requirements, mobility, interoperability, and large-scale connectivity	Optimize hybrid handshakes and support seamless transition across network generations	(Turnip et al., 2025)
Lightweight IoT systems	Confidentiality and secure communication between constrained devices	Compact lattice-based key encapsulation mechanisms	Limited memory, processing capability, energy, bandwidth, and storage	Develop lightweight implementations with efficient parameters and hardware acceleration	(Almutairi & Sheldon, 2025)

Vehicular ad hoc networks	Rapid authentication, privacy, and decentralized trust establishment	Quantum-resistant key exchange integrated with vehicular certificates	High mobility, intermittent connectivity, replay attacks, and communication delay	Enable scalable certificate management and low-latency trust establishment	(AlMarshoud et al., 2024)
TLS and virtual private networks	Secure session-key establishment over existing protocols	Hybrid key encapsulation combining classical and quantum-resistant algorithms	Enlarged messages, certificate fragmentation, and compatibility problems	Test protocol interoperability and maintain backward compatibility	(Egbuagha & Ikwunna, 2025)
Cloud and secure messaging systems	Protection of long-lived communications and stored data	Standardized post-quantum key encapsulation	Increased key size, ciphertext overhead, and computational demand	Prioritize high-value data exposed to harvest-now-decrypt-later attacks	(Chhetri et al., 2025)

6. Post-Quantum Digital Signature Algorithms

Post-quantum digital signature algorithms offer authentication, integrity, and non-repudiation without relying on the assumptions of factorization or the discrete logarithm problem, which are susceptible to quantum attacks. The schemes are vital for software updates, digital certificates, electronic transactions, blockchain systems, secure boot processes, and identity-management platforms. There are several leading approaches, such as lattice-based signatures and hash-based signatures, which have significantly different key sizes, signature lengths, computation time, and implementation complexity, among others. The use of multiple participants for signing further decentralizes signing authority, which increases resilience in financial, governmental, and distributed systems, while using a threshold signature architecture. For post-quantum adaptation, they must be able to coordinate well, generate shares securely, and be resistant to malicious signers but not have too much communication overhead (Sedghighadikolaei & Yavuz, 2025).

The lattice-based signatures are well-founded due to their high efficiency for the signing and verification operations, and the ability to implement these signatures in different computing platforms. The security they are usually based on comes from problems based on structures such as lattice problems and variants thereof that are based on modules and strike a balance between performance and security assumptions. Rejection sampling, polynomial arithmetic, randomness, and selection of parameters must be carefully handled in the implementation since if there is a weakness in one of these components, it may reveal secret information. The performance of the network, constrained devices, and the length of the certificate chain may also be impacted by large signatures and large public keys (Nguyen et al., 2025).

This is because there are risks associated with the deployment of hardware that are not represented in mathematical proofs of security. During signing operations, intermediate values might be susceptible to being revealed by power analysis, electromagnetic leakage, timing variation, fault injection, and memory-access patterns. Therefore, secure implementations must be constant-time, masked, redundant, fault-detecting, and use valid random number generators. A hardware-software co-design approach can help to optimize and enhance performance, while not compromising side-channel resistance. Reliable post-quantum signatures, on the other hand, rely on standardisation of algorithms, best practices for signature implementation,

interoperability tests, and ongoing assessment of the algorithms to account for the latest cryptanalytic and physical attacks (Bellizia et al., 2021). Table 3 gives an overview of applications, technical risks, and protective controls for digital signatures based on post-quantum cryptography.

Table 3. Post-Quantum Digital Signature Applications and Security Considerations

Application area	Signature requirement	Suitable approach	Major technical concern	Recommended control	In-text citation
Software and firmware updates	Authentication and integrity of distributed code	Lattice-based or hash-based signatures	Large signatures and verification overhead	Use validated implementations and secure update pipelines	(Nguyen et al., 2025)
Digital certificates and public-key infrastructures	Long-term authentication and non-repudiation	Standardized lattice-based signatures	Larger certificate chains and increased network transmission	Redesign certificate profiles and assess chain-size limits	(Nguyen et al., 2025)
Financial and governmental systems	Distributed signing authority and reduced single-key dependence	Threshold post-quantum signatures	Secure share generation, malicious signers, and communication overhead	Apply robust threshold protocols and protected key-share management	(Sedghighadikolaei & Yavuz, 2025)
Blockchain and distributed ledgers	Transaction authentication and durable signature security	Quantum-resistant lattice- or hash-based signatures	Long-lived public keys, increased transaction size, and scalability	Introduce phased migration and hybrid signature support	(Sedghighadikolaei & Yavuz, 2025)
Hardware security modules and embedded devices	Secure signing with physical attack resistance	Hardware-accelerated post-quantum signatures	Power analysis, electromagnetic leakage, timing attacks, and fault injection	Use masking, constant-time execution, redundancy, and fault detection	(Bellizia et al., 2021)

7. Implementation Challenges and Practical Security Risks

While the introduction of post-quantum cryptography in operating systems has various technical, architectural, and security-related issues, it is hoped that they will be addressed. Compared to traditional elliptic-curve algorithms, many post-quantum algorithms have public keys, ciphertexts, and signatures that are larger, thus consuming more bandwidth than their conventional counterparts, using more memory, requiring more storage, and making handshake latencies larger. In an Internet of Things (IoT) and machine-to-machine (M2M) environment, these constraints are more important, as the devices are typically constrained in computing resources and are subject to less stable communications. Other possible problems for existing Transport Layer Security and public-key infrastructure are the increase in certificate size, the fragmentation of messages, the validation of certificate chains, and the limited size of the trust stores (Diaz-Sanchez et al., 2019); an adaptation of the protocol and certificate management reform are required.

The challenges faced by IoT for the industrial sector are further compounded by the presence of legacy equipment, real-time operations, communication protocols from various types, and device lifecycles that can last as long as 10 years. Where it is not

possible to upgrade the firmware securely that is, where additional computing burden could impact critical timing- it may be challenging to migrate to post-quantum. Other algorithms, when not implemented correctly, have vulnerabilities which can be exploited by using weak implementations of the key storage, insecure update methods, and poor random number generation. If not, a variety of side-channel attacks, fault injection, timing leakage, and power analysis can reveal secret values, depending on the implementation (Abosata et al., 2021).

The protocol-level transition is a greater readiness issue. During migration, organizations will have to determine cryptographic requirements and dependencies, conduct interoperability tests, assess hybrid concepts, and ensure backwards compatibility. Early deployment of immature implementations can result in new vulnerabilities; late deployment can lead to more time to be vulnerable to harvest-now-decrypt-later attacks. Therefore, the implementation of the concept needs to be standardized in terms of libraries, validated parameters, coding security, performance testing, and vendor, infrastructure operator, and regulator coordination. Additionally, algorithm selection is not the only factor that will make a system practical to use; continuous operation testing and crypto-agile system design (Egbuagha & Ikwunna, 2025) are also important. The risks and requirements for implementation and migration to Post-Quantum Cryptography are summarized in Figure 2.

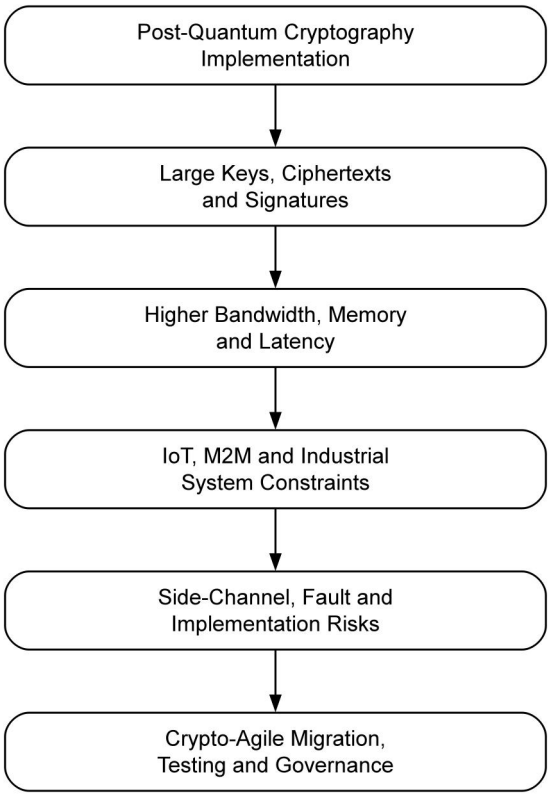

Figure 2. Implementation Challenges and Migration Pathway for Post-Quantum Cryptography

8. Integration Into Existing Digital Infrastructures

There will be a need for coordinated changes to the communication protocols, software platforms, public-key infrastructures, network devices, and operational security policies when PQC is integrated into existing digital infrastructure. Wireless and

distributed systems are particularly difficult to implement due to the presence of devices with varying capabilities, limited bandwidth, intermittent connections, and deployment time. Post-quantum keys, signatures, and ciphertexts could be larger, which would add to the latency to transfer these, the fragmentation of packets, energy consumption, and storage requirements. The limitations can also apply to wireless infocommunication systems, mobile networks, Internet of Things (IoT) platforms, and edge environments that need to provide both cryptographic security and dependability while maintaining real-time communication capabilities (Laktionov et al., 2025).

The classical public-key algorithms are at the core of many standard protocols, including TLS, SSH, IPsec, DNSSEC, and secure email, which are unlikely to be able to function with the post-quantum mechanisms without changes. A hybrid setup of classical and quantum-resistant algorithms may decrease transitional risk, but adds to the complexity of the protocol, the size of messages, demands in certificate management, and interoperability issues. When operating in mixed-algorithm mode, it is therefore important to carefully redesign to ensure: authentication, confidentiality, and backwards compatibility; and no implementation weaknesses (Chood et al., n.d.).

Another challenge with software migration is that cryptographic functions can be incorporated into applications, libraries, firmware, cloud services, and third-party dependencies throughout the software environment. The first step is to determine where vulnerable algorithms are being employed, how sensitive the data is being protected, the length of time protected data is being retained, and prioritizing systems by risk. Reducing disruption and facilitating future algorithm replacement, crypto-agile architectures, modular cryptographic interfaces, automated testing, and staged deployment can help achieve this. Comprehensive asset inventories, vendor coordination, compatibility assessment, and monitoring of assets throughout the migration lifecycle are necessary to ensure successful integration (Näther et al., 2024). Figure 3 shows the integration path of the deployment of post-quantum cryptography in existing digital infrastructures.

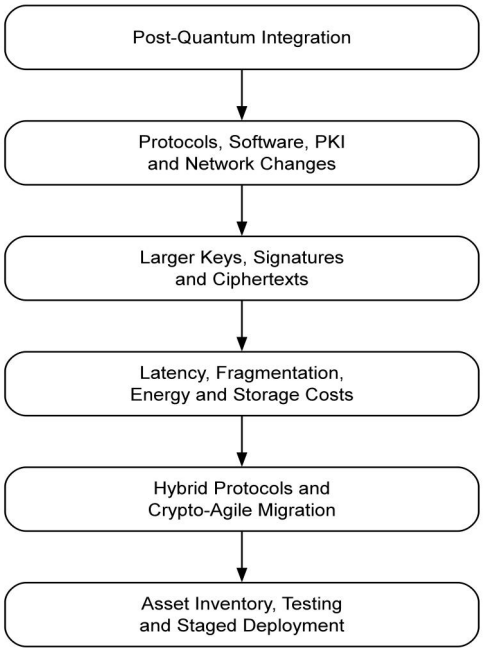

Figure 3. Integration Pathway for Post-Quantum Cryptography in Existing Digital Infrastructures

9. Standardization, Evaluation, and Regulatory Developments

Organizations must have algorithms that have been well vetted within the community through public evaluation, analysis, interoperability testing, and performance evaluation to ensure reliable adoption of post-quantum cryptography. Experimental schemes and single institutional decisions are not enough to ensure quantum readiness. It is paramount that it is done in a coordinated fashion with a set of standards for accepted algorithms, security parameters, implementation constraints, validation methods, and migration dates. In addition, standardization also minimizes fragmentation by allowing vendors, governments, communication protocols, and public key infrastructures to use compatible mechanisms across software, hardware, communication protocols, and public key infrastructures. The concept of strategic readiness, therefore, includes the process of technical deployment and aligning with national cybersecurity policies and procurement, and the long-term governance of cryptography (Erol, 2025).

There are more factors than quantum resistance that need to be taken into account for evaluation frameworks. Classical and quantum security, key and signature sizes, computational efficiency, implementation complexity, side-channel resistance, and fit for various operational environments should be evaluated for some of the proposed algorithms. Existing constructions that had previously been shown to be promising require further cryptanalysis: new attacks may be found in the implementation or mathematically, and weaken old constructions. Regulatory guidance should therefore enable algorithm replacement and periodic re-evaluation of algorithms and should not be blind to the need for "crypto-agile architectures" (Phuc, n.d.).

A major regulatory challenge in the IoT ecosystems comes from the devices, which are often limited in processing power, typically have long lifetimes, may not have the ability to update the software, and have a variety of vendor practices. The standards for lightweight post-quantum must provide security, while also being energy efficient, memory efficient, with low communications overhead, and low latency. Consistent protection in healthcare, industrial and transportation systems, as well as smart city systems requires certification schemes, secure update requirements, minimum implementation baselines, and sector-specific guidance. The post-quantum deployment will rely on the cooperation between the international community, transparent assessment, and harmonized requirements for enabling scalable and interoperable deployment (Mahdi & Abdullah, 2025). Table 4 shows the key challenges that remain in implementing, integrating, standardizing, and migrating to post-quantum readiness.

Table 4. Implementation, Integration, Standardization, and Migration Challenges

Domain	Principal challenge	Potential consequence	Recommended response	Strategic relevance	In-text citation
TLS and public-key infrastructure	Large certificates, fragmented messages, and constrained trust stores	Failed handshakes, latency, and interoperability problems	Update certificate profiles, protocol limits, and trust-management mechanisms	Essential for web, cloud, and machine-to-machine security	(Diaz-Sanchez et al., 2019)
Industrial IoT	Legacy equipment, long device lifecycles, and limited firmware updateability	Extended exposure to vulnerable cryptography and disruption of real-time operations	Use secure update mechanisms, staged replacement, and hardware protection	Critical for manufacturing, energy, transportation, and control systems	(Abosata et al., 2021)

Software migration	Hidden cryptographic dependencies across libraries, applications, and third-party components	Incomplete migration and persistent use of vulnerable algorithms	Conduct cryptographic inventories and introduce modular crypto-agile interfaces	Supports scalable algorithm replacement across complex software ecosystems	(Näther et al., 2024)
Wireless and edge infrastructures	Bandwidth constraints, energy use, packet fragmentation, and real-time requirements	Reduced performance and unreliable communication	Benchmark algorithms under realistic wireless and constrained-device conditions	Important for IoT, mobile networks, and distributed edge systems	(Laktionov et al., 2025)
Standardization and governance	Fragmented algorithm adoption, validation procedures, and migration schedules	Inconsistent protection and cross-platform incompatibility	Align standards, procurement requirements, certification, and regulatory guidance	Enables coordinated national and international quantum readiness	(Erol, 2025)
Lightweight post-quantum deployment	High computational, memory, and communicatio n overhead	Unsuitable performance for constrained devices	Develop compact implementations and sector-specific security baselines	Necessary for healthcare, smart cities, industrial devices, and transportation systems	(Mahdi & Abdullah, 2025)
Transition management	Dependence on legacy algorithms and uncertain quantum timelines	Premature deployment or delayed migration	Use hybrid mechanisms, phased implementation, testing, and continuous reassessment.	Reduces harvest-now-decrypt-later exposure and operational disruption	(Egbuagha & Ikwunna, 2025)

10. Limitations and Future Directions

The pace of research and evolution of post-quantum cryptography (PQC) makes it difficult to assess algorithms, standards, and implementation readiness, which could make this review incomplete or even contentious in the near future. The diversity in the methods used, benchmarking conditions, hardware platforms, and security assumptions of the available literature makes direct comparison with other studies difficult. There are still many publications that are written conceptually, based on preprints and/or simulation studies, with only a few based on large-scale production deployments. Furthermore, sector-specific constraints, costs of long-term maintenance, and interoperability problems in the real world are not uniformly reported.

There is a need for standardized benchmarking, deployment studies over the long term, and independent validation in various types of cloud, mobile, IoT (Industrial, Vehicular, and Constrained) environments. Side-channel resistance, fault-tolerance, secure hardware design, and automated migration tools are all areas in which more attention must be given. Lightweight algorithms, cryptoagile architectures, hybrid transition models, and efficient certificate management frameworks should also be developed as part of research. There is a need for international cooperation to establish harmonisation of standards,

regulatory guidance, testing procedures and workforce preparation and to keep abreast of new quantum and classical threats to cryptanalysis.

11. Conclusion

The need for post-quantum cryptography to safeguard digital infrastructures has become an important requirement to address the new capabilities of quantum computers. Classical public-key systems still face a threat from quantum algorithms that can compromise factorization- and discrete-logarithm-based security, compromising communications, digital identities, software integrity, financial transactions, and critical services. Lattice-based, code-based, hash-based, and other hard mathematical problems are promising alternatives for quantum-resistant algorithms, but come with significant challenges in terms of computational cost, key/signature size, interoperability, side-channel resistance, and legacy system compatibility. While algorithm choice will not guarantee long-term security, it is important to establish a groundwork for trusted deployment through standardization efforts. For the transition to be effective, cryptographic inventories, a phased migration, hybrid mechanisms, validated implementations, and crypto-agile architectures to accommodate future algorithm replacement are needed. Additionally, testing requirements vary across sectors as different platforms, such as cloud, industrialized systems, wireless networks, blockchain applications, and even constrained IoT devices, have different operational needs. The effectiveness of the transition will be further determined by ongoing research, coordinated regulation and harmonisation of international standards. This means organizations need to start preparing for post-quantum readiness now – before digital machines capable of implementing quantum cryptography enter the picture – to minimise current exposure and provide enhanced long-term digital resilience.

References

1. Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors, 21(11), 3654.
2. Ahmed, F. (2024). Quantum-resistant cryptography for national security: A policy and implementation roadmap. Int. J. Multidisciplinary on Science and Management, 1(4), 54-65.
3. AlMarshoud, M., Sabir Kiraz, M., & H. Al-Bayatti, A. (2024). Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions. ACM Computing Surveys, 56(10), 1-39.
4. Almutairi, M., & Sheldon, F. T. (2025). Resilience of Post-Quantum Cryptography in Lightweight IoT Protocols: A Systematic Review. Eng, 6(12), 346.
5. 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.

6. Asif, R. (2021). Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms. IoT, 2(1), 71-91.
7. Barrett-Danes, F., & Ahmad, F. (2025). Quantum computing and cybersecurity: a rigorous systematic review of emerging threats, post-quantum solutions, and research directions (2019–2024). Discover Applied Sciences, 7(10), 1083.
8. Baseri, Y., Hafid, A., Shahsavari, Y., Makrakis, D., & Khodaiemehr, H. (2025). Blockchain security risk assessment in quantum era, migration strategies and proactive defense. IEEE Communications Surveys & Tutorials.
9. Bellizia, D., El Mrabet, N., Fournaris, A. P., Pontié, S., Regazzoni, F., Standaert, F. X., ... & Valea, E. (2021, October). Post-quantum cryptography: Challenges and opportunities for robust and secure hw design. In 2021 IEEE International Symposium on Defect and fault tolerance in VLSI and Nanotechnology systems (DFT) (pp. 1-6). IEEE.
10. Cherkaoui Dekkaki, K., Tasic, I., & Cano, M. D. (2024). Exploring post-quantum cryptography: Review and directions for the transition process. Technologies, 12(12), 241.
11. Chhetri, G., Somvanshi, S., Hebli, P., Brotee, S., & Das, S. (2025). Post-quantum cryptography and quantum-safe security: A comprehensive survey. arXiv preprint arXiv:2510.10436.
12. Chood, R., Kilgerd, M., Contie, M., & Misoczkig, R. Future of Cyberspace: A Critical Review of Standard Security Protocols in the Post-Quantum Era.
13. Darzi, S., Ahmadi, K., Aghapour, S., Yavuz, A. A., & Kermani, M. M. (2023). Envisioning the future of cyber security in post-quantum era: A survey on pq standardization, applications, challenges and opportunities. arXiv preprint arXiv:2310.12037.
14. De Macêdo, A. R. L., Jagatheesaperumal, S. K., Da Costa, K. A. P., Acharya, K., Song, H., Guizani, M., & De Albuquerque, V. H. C. (2025). Quantum ai-enhanced iot-fog communication: A survey from cybersecurity and data privacy perspective. IEEE Communications Surveys & Tutorials.
15. Diaz-Sanchez, D., Marín-Lopez, A., Mendoza, F. A., Cabarcos, P. A., & Sherratt, R. S. (2019). TLS/PKI challenges and certificate pinning techniques for IoT and M2M secure communications. IEEE Communications Surveys & Tutorials, 21(4), 3502-3531.
16. Egbuagha, O., & Ikwunna, E. (2025). Post-quantum cryptography in practice: A literature review of protocol-level transitions and readiness. Cryptology ePrint Archive.
17. Erol, V. (2025). The Strategic Imperative of Quantum Readiness: A Comprehensive Review of Post-Quantum Cryptography. Preprints. org.
18. Khan, S., Krishnamoorthy, P., Goswami, M., Rakhimjonovna, F. M., Mohammed, S. A., & Menaga, D. (2024). Quantum computing and its implications for cybersecurity: A comprehensive review of emerging threats and defenses. Nanotechnology Perceptions, 20, S13.
19. Laktionov, I., Diachenko, G., Moroz, D., & Getman, I. (2025). A Comprehensive Review of Cybersecurity

Threats to Wireless Infocommunications in the Quantum-Age Cryptography. IoT, 6(4), 61.

20. Mahdi, L. H., & Abdullah, A. A. (2025). Fortifying future IoT security: A comprehensive review on lightweight post-quantum cryptography. Engineering, Technology & Applied Science Research, 15(2), 21812-21821.
21. Mohammed, A. (2024). Cyber security implications of quantum computing: Shor's algorithm and beyond. Innov. Comput. Sci. J, 10, 1-23.
22. Näther, C., Herzinger, D., Gazdag, S. L., Steghöfer, J. P., Daum, S., & Loebenberger, D. (2024). Migrating software systems toward post-quantum cryptography-a systematic literature review. IEEE access, 12, 132107-132126.
23. Nguyen, H., Huda, S., Nogami, Y., & Nguyen, T. T. (2025). Security in post-quantum era: A comprehensive survey on lattice-based algorithms. IEEE access.
24. Okika, N., Nwatuzie, G. A., Olarinoye, H. S., Nwaka, A. A., Igba, E., & Dunee, R. (2025). Assessing the vulnerability of traditional and post-quantum cryptographic systems through penetration testing and strengthening cyber defenses with zero trust security in the era of quantum computing. International Journal of Innovative Science and Research Technology, 10(2), 1240-1258.
25. Paul, B., & Trivedi, G. (2022, December). Post quantum cryptography algorithms: A review and applications. In International Conference on Intelligent Technologies (pp. 3-17). Singapore: Springer Nature Singapore.
26. Phuc, M. N. Implications of Quantum Computing for Classical Cryptographic Security: A Systematic Review.
27. Ravi, C. (2025). Quantum computing and cybersecurity: Systematic review of algorithms, challenges, and emerging solutions. Quantum Computing, Cyber Security and Cryptography: Issues, Technologies, Algorithms, Programming and Strategies, 407-440.
28. Ravi, P., Howe, J., Chattopadhyay, A., & Bhasin, S. (2021). Lattice-based key-sharing schemes: A survey. ACM Computing Surveys (CSUR), 54(1), 1-39.
29. Sane, P., & Patel, S. P. (2025, November). Post-Quantum Cryptography: A Review of Algorithms, Challenges, and Future Research Directions. In 2025 8th International Conference on Signal Processing and Information Security (ICSPIS) (pp. 1-6). IEEE.
30. Sedghighadikolaei, K., & Yavuz, A. A. (2025). A Survey of Threshold Signatures: NIST Standards, Post-Quantum Cryptography, Exotic Techniques, and Real-World Applications. ACM Computing Surveys, 58(6), 1-39.
31. Singh, S., & Kumar, D. (2024). Enhancing cyber security using quantum computing and artificial intelligence: A review. algorithms, 4(3), 1-18.
32. Sodiya, E. O., Umoga, U. J., Amoo, O. O., & Atadoga, A. (2024). Quantum computing and its potential impact on US cybersecurity: A review: Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets. Global Journal of Engineering and Technology Advances, 18(02), 049-064.

33. Turnip, T. N., Andersen, B., & Vargas-Rosales, C. (2025). Towards 6G authentication and key agreement protocol: A survey on hybrid post quantum cryptography. IEEE Communications Surveys & Tutorials.
34. Wang, Y., & Ismail, E. S. (2025). A Review on the advances, applications, and prospects of post-quantum cryptography in blockchain, IoT. IEEE Access.
35. Yunakovsky, S. E., Kot, M., Pozhar, N., Nabokov, D., Kudinov, M., Guglya, A., ... & Fedorov, A. K. (2021). Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. EPJ Quantum Technology, 8(1), 14.