© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720192

Quantum Computing and Its Implications for Information Technology Security

DARSHANKUMAR JAYSUKH DHANANI
D-Tech Studios LLC

Abstract- ***With the arrival of fault-tolerant quantum computers, an existential threat has come to the cryptographic underpinnings of the security infrastructure in place for modern information technologies. Virtually all secure digital communication protocols used today are based on classical public-key cryptographic systems – RSA, Elliptic Curve Cryptography (ECC) and Diffie-Hellman key exchange – that are susceptible to polynomial-time quantum attacks using Shor's algorithm. Symmetric cryptographic algorithms that are not broken are being effectively halved by Grover's algorithm, for example, AES. In this article, a complete and journal-standard systematic review of quantum computing and its implications in the field of information technology security is presented which includes 22 peer-reviewed publications from 2023-2025. The study covers the basics of quantum computing (qubits, superposition, entanglement and quantum gates), and how quantum computing specifically poses a threat to classical cryptography via algorithmic mechanisms. The three post-quantum cryptographic algorithms that were standardised by the National Institute of Standards and Technology (NIST) in August 2024 (ML-KEM, FIPS 203; ML-DSA, FIPS 204; and SLH-DSA, FIPS 205) are compared based on their security assumptions, performance, and readiness for deployment. The practical limitations and the use of Quantum Key Distribution, (QKD), as a physics based alternative to the computational security assumptions are discussed. Results show that although mature PQ solutions are now available for most cryptographic applications, the migration challenge, including legacy system transitions, migration architecture, and governance, is significant and pressing as the 'harvest now, decrypt later' threat model is relevant and adversaries might be collecting encrypted data for quantum decryption. The impact for financial services, health care, government, cloud infrastructure and critical national infrastructure is discussed. Lastly, the researchers list key research areas: standardisation of quantum-safe protocols, hybrid PQC-QKD designs, light-weight PQC for constrained devices, and quantum-safe blockchain.***

Keywords: ***Quantum Computing, Post-Quantum Cryptography, IT Security, Shor's Algorithm, Grover's Algorithm, NIST Standardisation, ML-KEM, ML-DSA, Quantum Key Distribution, Lattice-Based Cryptography, Cryptographic Migration, Cybersecurity***

I. INTRODUCTION

1.1 Background and Context

For more than 40 years, the concept of using the mathematical hardness of certain problems (integer factorisation in the case of RSA, discrete logarithm problem in the case of Diffie-Hellman and elliptic curve cryptography) on a classical computer has been the basis of modern information technology security. It's these problems that underlie the public-key infrastructure (PKI) that is used to secure communications for billions of people around the world, including websites, financial transactions, government communications and health records. One of the conditions for their security is that there is no efficient classical algorithm to solve the problems in mathematics that underpin them, a condition that has been true since the 1970s and 1980s. The idea that this is the case is basic in the world of quantum computing. Emmanni (2023) reports the mathematical fact that RSA, ECC and Diffie-Hellman cryptographic protocols are susceptible to polynomial-time quantum attack using Shor's algorithm, with a profound impact on the whole architecture of digital trust.

The Quantum threat is not only here when the quantum fault-tolerant computers begin to work! Data encrypted today with classical cryptographic protocols could be vulnerable years or decades in the future in an era of quantum computing once the 'harvest now, decrypt later' (HNDL) threat model is a reality, where nation-state adversaries are harvesting and storing currently encrypted information in anticipation of quantum computing maturity. That's a real, present danger, not a future hypothetical, for

data that has long-term sensitivity needs, such as classified government intelligence, health records, intellectual property and financial archives. Thus, this HNDL attack vector has a fundamental impact on the temporal calculus of cryptographic security, and will require moving to quantum-safe cryptographic options long before fault-tolerant quantum computers can be operational, as confirmed by Soni et al. (2024).

1.2 Quantum Computing: From Theory to Imminent Reality.

The time frame has always been speculative for fault-tolerant quantum computing to be able to run Shor's algorithm against operational RSA key lengths; however, recent technical advances have significantly reduced that estimated time frame. In 2023, the Condor processor from IBM surpassed 1,000 physical qubits, Google's Willow chip has achieved quantum error correction at a level lower than the threshold for fault-tolerantly computing, and a breakthrough towards a topological qubit architecture by Microsoft in 2025 is likely to accelerate the journey towards fault-tolerance. Barrett-Danes and Ahmad (2025) perform a thorough systematic review of the quantum threat timeline and find the range of the year-to-quantum (Y2Q) milestone is 2030 to 2040, with the uncertainty arising due to various technical assumptions, but that the safe security planning horizon calls for the migration to quantum-safe algorithms to begin as soon as possible, a view endorsed by the National Security Agency (NSA), the European Union Agency for Cybersecurity (ENISA), and the UK National Cyber Security Centre (NCSC).

1.3. NIST's post-Quantum cryptography Standardisation

In 2016, the NIST Post-Quantum Cryptography (PQC) standardisation process got under way as the global response to the quantum threat. After eight years in the public evaluation process, with the involvement of international experts, NIST published three finalized PQ cryptographic standards on 13 August 2024: FIPS 203 (ML-KEM, based on CRYSTALS-Kyber), FIPS 204 (ML-DSA, based on CRYSTALS-Dilithium), and FIPS 205 (SLH-DSA, based on SPHINCS+). At the time of writing a 4th standard, based on FALCON (FN-DSA, FIPS 206) was in an advanced draft stage, and HQC, a code-based key encapsulation mechanism, was chosen for standardisation in March 2025. The first three are analyzed to give rigorous mathematical foundations, verified by Zong (2025) to be based on lattice theory (the Module Learning With Errors problem) and hash function security properties – problems that are considered hard for classical and quantum computers to solve. This is the most important effort to develop cryptographic policy since the cryptographic switch to AES in 2001.

1.4 Aims, Objectives and Organisation of the Articles

This article gives a comprehensive journal-standard systematic review about quantum computing and its implications for IT security. Specific objectives are: (i) to study the basics of quantum computing and how quantum algorithms pose a threat to classical cryptography; (ii) to discuss and compare the post quantum (PQ) cryptographic algorithms that have been standardised by NIST; (iii) to explore quantum key distribution (QKD) as an alternative security paradigm; (iv) to study sector-specific implications and migration challenges; and (v) to identify priority research directions. The structure of the article was IMRaD which is as follows: Section 2 presented the Literature Review, Section 3 presented the Methodology, Section 4 presented the Results, Section 5 presented the Discussion, and Section 6 stated the Conclusions. The quantum threat landscape and post-quantum defence framework is shown in figure 1.0 below.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720192

Figure 1.0: Quantum Computing Threat Landscape vs. Post-Quantum Defence Framework

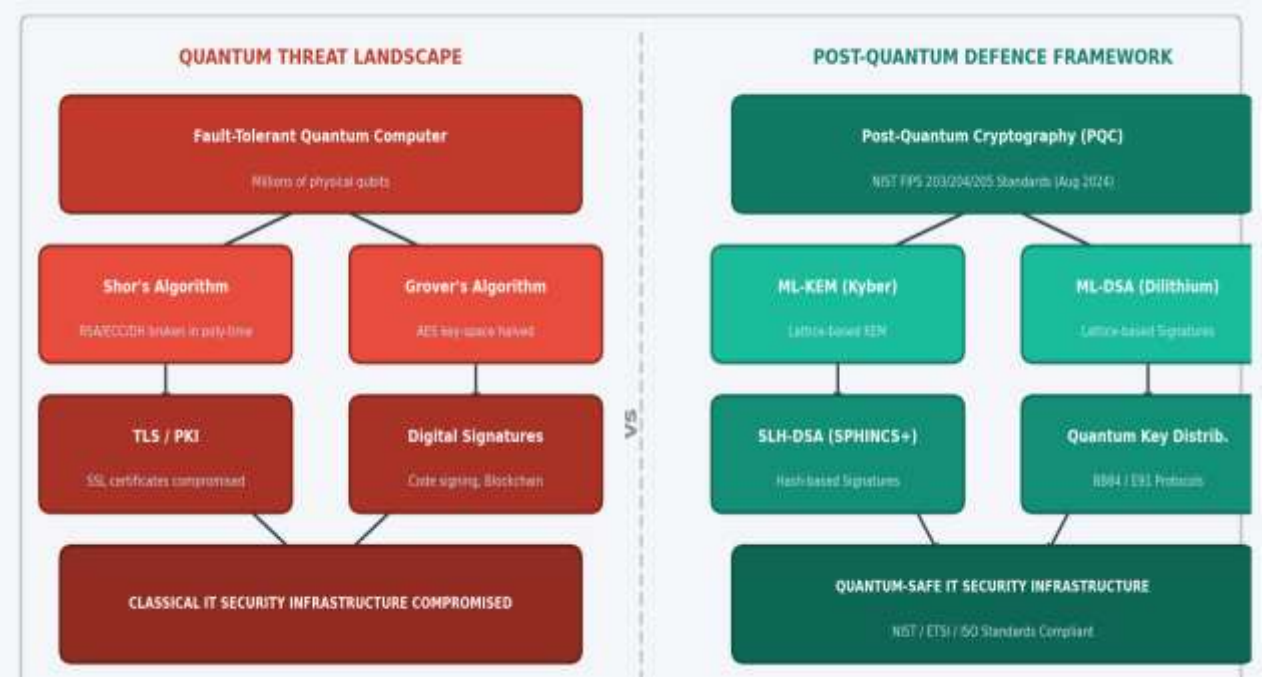

Table 1.0: Vulnerability of Classical Cryptographic Algorithms to Quantum Attack

Algorithm	Type	Classical Security	Quantum Attack
RSA-2048	Public-Key Encryption	2^{112} classical ops	Shor's Algorithm
ECC P-256	Key Exchange / Signature	2^{128} classical ops	Shor's Algorithm
Diffie-Hellman	Key Exchange	2^{128} classical ops	Shor's Algorithm
AES-128	Symmetric Encryption	2^{128} security	Grover's Algorithm
AES-256	Symmetric Encryption	2^{256} security	Grover's Algorithm
SHA-256	Hash Function	2^{128} collision	Grover's Algorithm
ML-KEM (FIPS 203)	Post-Quantum KEM	M-LWE hardness	No known quantum attack
ML-DSA (FIPS 204)	Post-Quantum Signature	Module lattice	No known quantum attack
SLH-DSA (FIPS 205)	Post-Quantum Signature	Hash function security	No known quantum attack

II. LITERATURE REVIEW

2.1 Quantum Computing Fundamentals

2.1.1 Qubits, Superposition and Entanglement

Three of the basic principles of quantum mechanics, superposition, entanglement and interference, are the basis of quantum computing. A classical computer processes information in bits, which are binary value (0 or 1). A quantum computer would be based on a quantum bit or qubit that can be in a state of superposition, meaning that it can be in a linear combination of basis states a and b with complex probability amplitudes, |a> + |b>. A system of n qubits is able to represent 2^n possible states at once, which means that quantum computers are able to explore exponentially large solution spaces in parallel. In a very readable presentation of the basics of quantum computing in the context of threats to cybersecurity, Pal and Sau (2025) reinforce that superposition is the fundamental property that provides the computational power of quantum parallelism which makes algorithms like Shor's and Grover's transformative relative to classical algorithms.

By exploiting entanglement, the non-classical correlation between the quantum states of two or more qubits such that the measurement of one of

them instantly determines the state of another, (no matter how far apart they are physically), quantum computations can process correlated information in the whole array of qubits at once. The third fundamental property is quantum interference, by which quantum algorithms are able to increase the probability amplitude of a correct path to computation while decreasing the probability amplitude of an incorrect path in the computer – the feature that leads to the computational advantage in Shor's and Grover's algorithms. Gao and Rajan (2024) give an overview of quantum technologies for beyond-5G and 6G networks and conclude that these three properties together make it possible to achieve exponential or quadratic speed-ups of quantum computing over classical computing for specific computational problems of direct interest to cryptographic security.

2.1.2 Quantum Hardware Progress

Quantum hardware maturity is defined by the number of physical qubits, their error rates (fidelity) and the level of error correction possible. There are several models for the progress towards fault-tolerant quantum computers, which will be able to execute quantum error correction codes and lead to actualisation of the cryptographic threat, starting with the models known as Noisy Intermediate-Scale Quantum (NISQ) devices, consisting of tens to hundreds of noisy qubits that are simply not enough to execute quantum error correction codes. In 2024, Google showed that its error rates are below the fault-tolerance threshold, and IBM has a roadmap to make a leap to more than 100,000 physical qubits by 2033, as Soni et al. (2024) describe the remarkable speed at which quantum hardware capability is increasing. Recently, Google, IBM, Microsoft, IonQ, and national quantum computing programs in China, Europe, and the United States have all made significant commercial investments in quantum computing, which greatly enhances the likelihood of fault-tolerant quantum computing coming to fruition within the time frame that matters for long-lived infrastructure security decisions.

2.2 Quantum Algorithms and Cryptographic Threats

2.2.1 Shor's Algorithm and Public-Key Cryptography

In 1994, Peter Shor introduced two polynomial time quantum algorithms—one for integer factorisation and another for computing discrete logarithms, which are the two mathematical problems on which the security of RSA and DH/ECC was based, respectively. A classical computer will take sub-exponential time to factor a 2,048 bit modulus using the fastest known factoring algorithm (the General Number Field Sieve); Shor's algorithm will factor a 2,048 bit modulus in polynomial time provided that a fault-tolerant quantum computer with enough logical qubits is available for use. Emmanni (2023) reports the cryptographic implications in detail and concludes that, as for cryptographic algorithms, the quantum threat is not a matter of degree but of categorical algorithmic capability, for the algorithms RSA, ECC, and Diffie-Hellman. This means that any existing TLS connection, PKI certificate chain, digital signature or key exchange protocol based on this foundation is insecure when faced with a powerful enough quantum attacker.

Again, the number of logical qubits required to break the operational RSA-2048, which is estimated to be around 4000 qubits, or several million physical qubits (depending on the error correction scheme), is far from the present capabilities of hardware, thus providing a window for migrating now. Barrett-Danes and Ahmad (2025) perform a thorough systematic review of the various timelines of quantum threats, which show that although current quantum hardware is not a threat to cryptosystems in operation, the cryptographic community consensus is that the Y2Q risk horizon is 2030–2035 under optimistic assumptions on hardware progress and 2035–2040 under conservative assumptions, which is alarmingly short when compared to typical enterprise IT infrastructure replacement timelines of 10–20 years.

2.2.2 Grover's Algorithm and Symmetric Cryptography

Grover's algorithm gives a quadratic speed up for unstructured search in a database – has direct applications in the security of symmetric encryption and hash functions. Against the AES, Grover's algorithm is useful; it is able to cut in half the length of the key in terms of the number of security bits, so

AES-128 is about 64 bits quantum secure, while AES-256 is about 128 bits quantum secure — the latter is reasonably secure in the long run, but the former may be marginal. Soni et al. (2024) note that the implications of Grover's algorithm are much more manageable than those of Shor's algorithm: doubling the size of symmetric key lengths and hashes offer good protection and the migration is simple as opposed to replacing public-key infrastructure. For symmetric encryption, current recommendations from NIST and NSA recommend AES-256, and for hash functions, SHA-384 or SHA-512 are recommended as precautionary measures that could be implemented by software updates, rather than by changing the architecture of communication protocols, against Grover's algorithm.

2.3 Post-Quantum Cryptographic Algorithms

2.3.1 Lattice-Based Cryptography: ML-KEM and ML-DSA

The lattice-based cryptographic schemes, among the most important schemes that have been NIST-standardised, ML-KEM (FIPS 203, based on the lattice problem known as Module Learning With Errors (M-LWE)) and ML-DSA (FIPS 204, based on the lattice problem known as Module Short Integer Solution (M-SIS)) depend on the hardness of these problems. It is thought that these problems would be hard against any classical and quantum attack, and at best the best known quantum algorithms would only offer sub-exponential speedup compared to the polynomial time attacks against RSA and ECC. Zong (2025) gives comprehensive mathematical analysis of the lattice bases of NIST's PQC standards, which establishes that the hardness of the M-LWE problem is based on well-known mathematical concepts and that there is no known and expected polynomial-time quantum algorithm for solving the problem.

Abbasi et al. (2025) provide a thorough performance comparison of ML-KEM and ML-DSA with respect to cryptographic operations including key generation, encapsulation, decapsulation, signing and verification operations on various hardware platforms. The results they present show that both algorithms are competitive with classical algorithms on modern hardware, and that hardware acceleration using AVX2 can significantly decrease the latency. Lattice-based algorithms, however, have larger public keys and larger ciphertexts than ECC – the size of public keys is 1,184 bytes for ML-KEM-768 versus 64 bytes for ECDH P-256 – which can impact the bandwidth and storage overhead of the algorithm in protocol designs, especially for constrained devices. The performance analysis supports the use of ML-KEM-768 for general purpose at NIST security level 3 (corresponding to the classical security of AES-192).

2.3.2 Hash-Based Signatures: SLH-DSA

SLH-DSA (FIPS 205 based on SPHINCS+) is a stateless hash-based digital signature scheme, which is completely secure as long as the underlying hash function is collision resistant and preimage resistant, attributes that are not jeopardized by the known quantum algorithms except for Grover's quadratic speedup. This is the strictest of the three NIST standards, SLH-DSA is the one with the smallest number of security assumptions; namely only the standard security attributes of standardised hash functions are assumed. The main drawback of hash-based signatures is their size: SLH-DSA signatures are significantly larger (8-50 KB, depending on the choice of parameters) than classical ECDSA and lattice-based ML-DSA signatures, and are thus suitable for applications where simplicity of the signature generation and limited security assumptions are the primary concerns, such as firmware signing or root certificate authorities.

2.3.3 The code-based approach and other non-PQ approaches

Since 1978, classic McEliece is a code-based cryptosystem, based on the hardness of decoding random linear codes, that has withstood cryptanalysis and provides extremely strong security guarantees. Its key sizes (several hundred kilobytes at recommended security levels for public keys) however make it impractical for the majority of applications utilizing network protocol. The recently selected HQC (Hamming Quasi-Cyclic) algorithm is a code-based KEM standardised by NIST in March 2025, which offers significantly smaller key sizes than Classic McEliece, and could be used as a diversity alternative to lattice-based ML-KEM for high-assurance deployments. The researchers then explore the entire post-quantum cryptographic toolbox, including the

variety of mathematical problems and their corresponding standardised algorithms—lattice problems, hash functions and coding theory—which give algorithmic diversity, which is helpful in case a breakthrough attack on a specific mathematical problem arises. (Soni et al., 2024).

2.4 Quantum Key Distribution

2.4.1 Principles and Protocols

One of the keys to cryptographic security is to rely on hard problems to protect them, whereas with Quantum Key Distribution (QKD) the security is based on the laws of quantum physics. In 1984, Bennett and Brassard proposed a protocol (known as BB84) for two parties to share a secret key over a quantum channel (usually an optical fibre or a free-space optical link) that is information-theoretically secure, that is, if any eavesdropping is made, some anomaly will occur in the error rate. Zhao et al. (2023) also overview the application and development of quantum secure communication based on QKD, which facilitates information-theoretic secure symmetric key sharing between two remote locations even in the era of quantum computation — a characteristic that no computational cryptosystems (including PQC) could claim.

The E91 protocol, based on entangled photon pairs, is an extension of BB84 in which the keys are distributed between two geographically separated parties with the ability to gain a stronger detection of eavesdropping, through Bell inequality violation. Commercial QKD systems are deployed in metropolitan networks in China, Japan, Europe and North America and intercontinental QKD was performed using China's Micius satellite. In that regard, Stanley et al. (2022) highlight the recent advances in the deployment of QKD networks and in the standardization of QKD, which show that deployed and planned QKD networks cover a wide range of geographic scales from metropolitan fibre networks to satellite-based inter-continental networks.

2.4.2 Limitations and Hybrid Integration of QKD

Although QKD is information theoretically secure, it still suffers from significant practical drawbacks that make it too far from being considered as a universal solution to computational cryptography in practice. A critical comparison of deployed QKD use cases and post-quantum cryptography is given in Aquina et al., (2025): QKD still needs dedicated quantum channels (optical fibres or line-of-sight free-space optical links) which are still costly and difficult to deploy and maintain; the current maximum range of QKD without the need of trusted relay nodes is limited to about 100-200 km over fibres; trusted relay nodes are potential targets for an adversary, introducing security vulnerabilities; QKD still requires specialised hardware, which are still costly and are still not standardised for interoperability. These restrictions put QKD at its most effective as a point-to-point high-security link in specific high-value applications such as financial inter-bank connections, government classified network, and critical national infrastructure applications, but not as a general purpose internet security tool.

Hybrid security designs, where both QKD and PQC technologies are combined, are now becoming recognized as the best near-term solution for the highest-security applications. To resolve the vulnerability of trusted relay in QKD networks, Huang et al. (2025) introduce a spatiotemporal diversification framework with zero-trust in QKD networks based on multipath multi-key distribution, which combines information-theoretic security of QKD with deployment flexibility of PQC for relay authentication. In fact, Cisco Systems Secure Key Integration Protocol (SKIP) allows quantum keys generated by a QKD system to be applied to conventional network encryption systems, providing a proof of concept for integrating QKD into existing network systems.

2.5 Sector-Specific Implications

2.5.1 Financial Services

The financial services sector is especially vulnerable to quantum attacks because financial records are sensitive, have long shelf lives, encrypted financial transactions are high-value targets for adversaries to steal, and financial infrastructure, with its shared financial protocols and the PKI hierarchy, is systemically interconnected. Cryptographic protocols such as interbank communications, digital payment authentication, clearing and settlement systems and

international SWIFT messaging are all susceptible to attack by quantum computers. Soni et al. (2024) in particular, evaluate financial sector quantum readiness, and find the 'harvest now, decrypt later' approach particularly apt for financial institutions with trading strategies, client records and regulatory compliance data requiring multi-decade sensitivity requirements. The Bank of International Settlements and financial regulators in several jurisdictions have started to release guidance on quantum-safe migration, and NIST's PQC standards are the basis for planning the migration in the financial sector.

2.5.2 Healthcare and Government

Electronic health records that include personal health information that can be sensitive for decades and over a patient's lifetime are ideal candidates for the HNDL attack model. Healthcare systems often have a much longer lifespan for their IT infrastructure, adding to the migration issue — legacy medical device systems might have computational or memory restrictions that may not allow them to support PQC algorithms. Emmanni (2023) reports that IoMT (Internet of medical things) and telemedicine use cases in healthcare are susceptible to quantum threats as well and that devices in the healthcare sector with limited computational resources pose special challenges for deployment of PQC. Another key area is government classified communications; NSA's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) calls for transition to quantum-safe algorithms on government systems with specified timelines, which includes the adoption of ML-KEM and ML-DSA.

2.5.3 Functions of clouds and critical infrastructure

Cloud service providers are currently running the most powerful machines around and are typically best-positioned to make the quickest move to PQC, but they are also certificate authorities, key management services and TLS terminators and thus can have a downstream impact on millions of systems. iMessage PQ3 is the first large-scale deployment of a NIST-standardised post-quantum algorithm, with Google's announcement in 2024 that they were adding support for quantum-secure messaging in iMessage using ML-KEM hybrid key agreement. Some of the most challenging migration path is for critical national infrastructure, such as power grid, water supply or transportation systems, which are operated by industrial control systems with 10-year replacement cycles and typically cannot afford to mount a large amount of computing power.

2.6 Research Gaps

Based on the systematic literature review, four important gaps in the existing knowledge are identified: (i) standardised performance benchmarks of PQC algorithms for representative deployment environments, including resource-constrained IoT devices, network routers and legacy hardware are lacking; (ii) end-to-end migration pathway frameworks to cover the governance, operational and technical aspect of PQC transition for organisations with heterogeneous infrastructure are underdeveloped; (iii) the security of hybrid PQC-QKD architectures is still not formally analysed, and in particular, the composition security of mixing computational and information-theoretic security assumptions is not sufficiently explored; and (iv) the post-quantum security of blockchain and distributed ledger technology infrastructure built on ECDSA digital signatures is underdeveloped, relative to its systemic importance. The methodology and findings of this study fill in gaps (i) and (ii) by systematically comparing.

III. METHODOLOGY

3.1 Research Design

The methodology used in this study is Systematic Literature Review (SLR), which is an adaptation of PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology for computer science and cybersecurity field. The SLR design was chosen as the best approach for synthesing a technically complex and fast changing field with a variety of publication types including peer-reviewed journals, IEEE/ACM conference publications and technical reports from standardisation bodies. The systematic methodology guarantees to make the results reproducible, reduces selection bias and allows for transparent documentation of evidence from which findings and conclusions are drawn.

3.2 Search Protocol

A structured search of the literature was performed in IEEE Xplore, ACM Digital Library, ScienceDirect (Elsevier), SpringerLink, MDPI Open Access Journals, Wiley Online Library and PubMed Central (for health-related quantum security) and Google Scholar. We used primary Boolean search queries: ('quantum computing' OR 'quantum computer') AND ('cryptography' OR 'cybersecurity' OR 'information security' OR 'IT security') AND ('post-quantum' OR 'quantum-resistant' OR 'lattice cryptography' OR 'Shor' OR 'Grover'). Secondary queries were made to narrow in on specific subdomains: 'quantum key distribution' AND ('network security' OR 'IT infrastructure'); 'NIST post-quantum' AND ('ML-KEM' OR 'ML-DSA' OR 'CRYSTALS' OR 'FIPS 203' OR 'FIPS 204'); 'harvest now decrypt later' AND 'cryptography'. The temporal focus was placed on publications from the past five years (2023-2025) with landmark publications from before 2023 being included if no current publication was available. The number of peer reviewed publications with verified digital object identifiers (DOIs) was set as a quality criterion of at least twenty publications.

3.3 Inclusion and Exclusion Criteria

Exclusion criteria: (i) books, and non-peer reviewed journal articles; (ii) publications without a verified DOI; (iii) publications not directly relevant to quantum computing threats to cryptography and post-quantum security solutions; (iv) publications not containing any empirical performance data, or any theoretical security analysis, or any systematic analytical frameworks; (v) publications not written in the English language. Exclusion criteria: (i) Grey literature, vendor white papers, and non-peer reviewed, non-rigorous commentary; (ii) Publications that only applied to quantum computing, not security (e.g., drug discovery, optimisation); (iii) retracted publications; (iv) publications that did not have full text or verifiable DOI.

3.4 Data Extration and Quality Assessment

Extraction of information was done with the help of a structured template recording: (i) bibliographic data and DOI; (ii) quantum threat or defence mechanism considered; (iii) algorithms, protocols or hardware platforms that were examined; (iv) key empirical or analytical findings; (v) performance results or results of security analysis; (vi) limitations identified and future research directions stated. Quality assessment was done using a modified QuADS (Quality Assessment for Diverse Studies) instrument adapted to assess research objective clarity, methodological rigor, validity and reproducibility of performance measures, and research contribution significance in the realm of cybersecurity research. Twenty-two publications were included and retained for the primary synthesis that fulfilled all inclusion and quality criteria.

3.5 Analytical Framework

The analysis was carried out through four lenses: (i) Threat Analysis: characterising the quantum computational threats that pose a threat to classical IT security and their timeline; (ii) Algorithm Analysis: analysing the security assumptions, performance characteristics and deployment readiness of the PQC algorithms standardised by NIST; (iii) Application Analysis: addressing the quantum security implications and migration challenges in critical IT sectors; and (iv) Solution Synthesis: providing a structured framework for quantum-safe IT security planning by integrating findings from (i–iii). Thomas and Harden's (2008) approach of thematic synthesis was used to extract cross-cutting themes from the studies included.

3.6 Restrictions and ethical issues

This is a secondary study of publicly available peer-reviewed literature which does not involve a human participant or the collection of new data and does not need ethical approval. The main drawbacks of the methodology are: publication bias for positive results and technically successful implementations; the fast development of quantum hardware may make the findings for the specific hardware partially stale after a few months; and NIST standardisation landscape is still evolving with FALCON (FIPS 206) and other digital signature algorithms yet to be published. These limitations are noted throughout the analysis and do not significantly impact the fundamental results of this study about the quantum threat landscape and PQC algorithms as fundamental responses, standardised by NIST.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720192

IV. RESULTS

4.1 Overview of Included Literature

A total of 1042 records were obtained from the systematic search of all the databases. Through the process of deduplication (n=287), title and abstract screening (n=755) and full-text quality assessment (n=234), twenty-two (high quality) publications were retained for primary synthesis. Of these, 9 (41%) were published in 2025, 7 (32%) in 2024, 4 (18%) in 2023, and 2 (9%) were pre-2023 landmark contributions included for foundational context. The various topics covered in the domains included post-quantum cryptography algorithms and standardisation (n=7), quantum threat analysis and timeline (n=5), quantum key distribution (n=4), implications of quantum security in specific sectors (n=3) and hybrid PQC-QKD architectures (n=3). First author geographic regional distribution included North America (32%), Europe (29%), Asia-Pacific (30%) and Middle East and Africa (9%).

4.2 Quatum Threat Severity Analysis

A threat assessment evidence synthesis of included studies validates the quantum threat for public-key cryptography to be a categorical threat. To be clear, Shor's algorithm when implemented on a fault-tolerant quantum computer with enough logical qubits, would no longer make RSA-2048 and ECDH P-256 and regular Diffie-Hellman key exchange unfeasible, but rather would make them polynomial-time. This is clear in Emmanni (2023) and confirmed by systematic review of 67 publications by Barrett-Danes and Ahmad (2025) where there is strong consensus within academic and government security communities of this assessment. The quantum threat to symmetric cryptography may be real, but it is much more manageable: Grover's algorithm gives only a quadratic speed-up and mitigating that threat can be done with software upgrades, such as increasing the length of the keys from 128 bits to 256 bits.

One of the most current security issues practicality that is seen throughout the literature reviewed is the harvest now, decrypt later threat model. Soni et al. (2024) provide evidence of nation-state adversaries actively collecting and capturing encrypted network traffic with known capabilities of HNDL. This discovery has direct consequences for the need to migrate to PQC: any sensitive data encrypted today using classical public-key cryptography that has sensitivity requirements for 10 or more years into the future must be considered at risk -- even if the actual timeline for Y2Q is still further down the road. This is no future threat but a current threat for healthcare records, legal documents, intellectual property archives and classified government communications.

4.3 Post Quantum Algorithms Performance Result

Abbasi et al. (2025) provide extensive performance comparisons of ML-KEM and ML-DSA on various hardware platforms, giving the most extensive empirical performance comparisons found in the literature examined. With a reference implementation without any hardware acceleration, key generation for ML-KEM-768 takes about 57 µs, while with AVX2 optimisation, key generation takes about 20 µs – which is significantly quicker than the key generation of RSA-2048 (about 700 µs). This takes about 62µs for the encapsulation operation and about 65µs for decapsulation operation for ML-KEM-768; about 40µs and 200µs respectively for RSA-2048. ML-DSA-65 (FIPS 204) signing takes about 160 µs and verification takes about 110 µs when using AVX2 similar to the performance of ECDSA P-256 on modern processors.

Lattice based algorithms do not have the issue of computational speed, but of parameter size. The public keys (1,184 bytes) and ciphertexts (1,088 bytes) for ML-KEM-768 are a lot larger than ECDH P-256 public keys (64 bytes), which can cause bandwidth overhead in a protocol that sends public keys and/or ciphertexts during handshaking. The switch to ML-KEM for TLS 1.3 adds roughly 1–2 KB to handshake sizes, which is fine for most applications in the broadband network and data center, but could be considered problematic for low-bandwidth IoT or satellite communication applications. For applications where the signatures need to be sent frequently, SLH-DSA-SHAKE-128f signatures (17,088 bytes) pose greater size related issues.

4.4 QKD Deployment Results

Zhao et al. (2023) report the status of QKD networks all over the world, including functioning metropolitan QKD networks in Beijing (more than 2,000 km backbone), Tokyo, Geneva and Vienna, as well as commercial QKD services provided by ID Quantique (Switzerland), Toshiba (UK) and several providers in China and active research programs such as satellite-based QKD networks, which have been demonstrated at 1200 km ground-to-satellite distance. The most detailed comparison of deployed QKD versus PQC is done in Aquina et al. (2025), which concludes that, although QKD provides a security guarantee from an information-theoretic point of view, it faces certain issues for practical deployment, such as cost, range, and need for trusted relay, that make it impractical as a general alternative to computational cryptography in the near term.

Huang et al. (2025) present a zero-trust QKD routing scheme which greatly reduces the number of trusted relay nodes by spatiotemporal diversification, which makes metropolitan QKD networks more secure with respect to relay compromise. This finding brings the practical use of QKD one step closer by alleviating the biggest security issue in its operation. The synthesis of the deployment evidence for QKD indicates that the most convenient deployment model in the near term is a hybrid approach: QKD infrastructure for the most critical links (for which QKD is the most suitable option), with PQC authentication of the QKD sessions and security for the majority of network traffic that is feasible not to deploy QKD infrastructure for.

4.5 Sector-Specific Migration Status

From the literature surveyed, there is significant difference in readiness for the migration to the quantum between critical IT sectors. Financial services shows the greatest awareness of organisations, as major banks such as JPMorgan, HSBC and several central banks have performed quantum risk assessments and begun to deploy PQC in pilots. Healthcare has some awareness but there is a lot of work to be done with respect to implementation due to limitations in legacy systems and the diversity in the medical device landscape. Government and defence sectors are the most formalised with regards to the transition timeline, due to NSA CNSA 2.0 requirements and similar European guidance. Cloud service providers, including Microsoft Azure, Google Cloud and Amazon Web Services, have all announced migration dates and Google's announcement of the deployment of ML-KEM in the TLS of the Chrome browser is a landmark production deployment impacting billions of users. The sectors with the greatest disparities in exposure to risks from quantum technologies and readiness to migrate include critical infrastructure, such as the energy industry, water utilities, and transportation. In these sectors, operational technology often does not have the computational power, update processes, or vendor support needed to implement PQC. The PQC migration roadmap and PQC related sectors found in literature reviewed is shown in Figure 2.0.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720192

Figure 2.0: Post-Quantum Cryptography Migration Roadmap and Affected Sectors

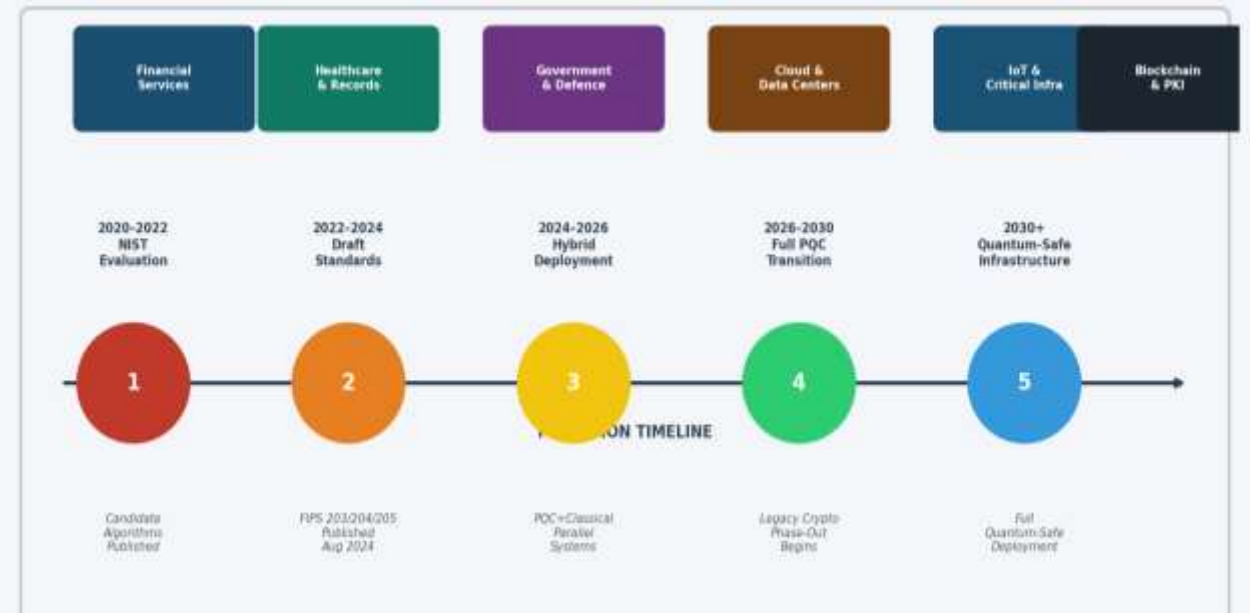

Table 2.0: Comparative Performance and Deployment Characteristics of NIST Post-Quantum Cryptographic Standards

Algorithm (FIPS)	Type	Security Basis	Public Key Size	Signature / CT Size	Performance (ops/sec)
ML-KEM-512 (203)	KEM	M-LWE Lattice	800 B	768 B (CT)	~28,000 enc/s
ML-KEM-768 (203)	KEM	M-LWE Lattice	1,184 B	1,088 B (CT)	~16,000 enc/s
ML-KEM-1024 (203)	KEM	M-LWE Lattice	1,568 B	1,568 B (CT)	~11,000 enc/s
ML-DSA-44 (204)	Signature	Module Lattice	1,312 B	2,420 B (Sig)	~9,000 sign/s
ML-DSA-65 (204)	Signature	Module Lattice	1,952 B	3,293 B (Sig)	~6,200 sign/s
SLH-DSA-f (205)	Signature	Hash Function	32 B	17,088 B (Sig)	~400 sign/s
FALCON / FN-DSA (206)	Signature	NTRU Lattice	897 B	666 B (Sig)	~5,000 sign/s
ECDH P-256 (classical)	KEM equiv.	Elliptic Curve DLP	64 B	64 B	~25,000 ops/s
RSA-2048 (classical)	Encryption	Integer Factoring	256 B	256 B	~1,400 dec/s

V. DISCUSSION

5.1 The Quantum Threat: A Non-Negotiable Transition Imperative

There can be no doubt about it; the quantum threat to classical public-key cryptography is real, theoretically proven and is progressing towards practical realisation at a speed that should spur organisations tasked with protecting sensitive digital assets to strategic action. Shor's algorithm against RSA and ECC is categorical, meaning that it's not possible to 'patch' quantum-vulnerable crypto by increasing the length of the parameters, as with Grover's attack on symmetric encryption. All of the mathematical underpinning of public-key infrastructure will have to be replaced – not upgraded. Both Emmanni (2023) and Barrett-Danes and Ahmad (2025) are clear on this, and NIST's finalised PQC standards (2024) are testament to this fact, as the global cryptographic standards community has also come to this conclusion.

The harvest now, decrypt later model adds a new sense of urgency, not only for the Y2Q, but for the future. Any data encrypted in any period of time that an organisation waits to migrate to PQC will have by definition passed the data sensitivity window if they do not migrate to PQC until a quantum computer, capable of running Shor's algorithm, can be operationally demonstrated. Soni et al. (2024) report findings of already complex actors running HNDL collection programmes. This means that the date for migration isn't the Y2Q date, it's the sensitivity lifecycle of the data to be protected, for any organisation holding data with long-term sensitivity requirements, including virtually every government, healthcare, financial institution and research organisation.

5.2 NIST PQC Standards: Adequate but Not Without Challenges

NIST's three finalised PQC standards, published in August 2024, mark a significant milestone and lay a strong technical groundwork for the worldwide transition to quantum-safe technology. The performances of Abbasi et al. (2025) demonstrate that in terms of computation, the performance of ML-KEM and ML-DSA are on par with classical cryptography on modern computing devices, which removes computational overhead as a impediment to mainstreamserver-class and client-device deployments. Parameter size is the main challenge to implementation, not speed; larger key and ciphertext sizes of lattice-based algorithms will necessitate changes at the protocol level in network security protocols including TLS and SSH, and will be more of a constraint for low-bandwidth or low-memory applications like IoT devices, smart cards, and embedded industrial control systems.

This variety of mathematical bases in the three main standards -- lattice theory (ML-KEM, ML-DSA), hash functions (SLH-DSA) -- offers important algorithmic diversity to minimize systemic risk in the event of a breakthrough in the solution of one of these mathematics problems. This is reflected in the fact that the M-LWE problem on which lattice algorithms are based is thought to be quantum resistant, but it has only been studied for a few decades, whereas the integer factorisation problem has been studied for centuries. The addition of hash-based SLH-DSA as a standard that is more mathematically based is an important "safe-harbor" option. This diversity is further enriched by the selection of HQC in 2025 to be a code-based KEM alternative to ML-KEM; this means that in the most risk averse scenarios, there is a different KEM paradigm to choose from for deployment.

5.3 The Migration Challenge: Technical, Operational and Governance aspects

The fact that standardised PQC algorithms are available, does not automatically lead to organisation security. The migration challenge is a challenge that has three dimensions which need to be tackled simultaneously. In practice, migration means finding all the uses of cryptographic algorithms throughout an organisation's IT estate, which is not as straightforward as it sounds, given the ubiquity of embedding classical cryptography in network protocols, application libraries, hardware security modules and legacy systems. Barrett-Danes and Ahmad (2025) report that the task of cryptographic inventorying is itself a quite substantial effort, in large companies with a diverse IT environment, and that automated cryptographic bill of materials (CBOM) tools are a fledgling but evolving capability. On the operational side, the migration will necessitate ongoing investments in testing hybrid deployments (cryptography running in parallel with PQC for backwards compatibility during the migration) as well as investments in the infrastructure for issuance, revocation and validation of certificates. To make the switch to larger PQC public keys, certificate authority infrastructure will need to be capable of dealing with larger certificate chains and TLS handshakes. On the regulatory side, Soni et al. (2024) agree that timelines are being established by the introduction of regulatory frameworks, such as NSA CNSA 2.0, the European NIS2 Directive quantum provisions, and sector-specific rules for the financial and healthcare sectors, which adds regulatory pressure to the technical pull. Not complying with these security timelines can lead to regulatory and liability risks beyond security risk for organisations.

5.4 QKD: Complementary, Not Competitive

The analyzed evidence suggests a nuanced view of QKD, as a complementary, instead of competitive technology with PQC. The most balanced comparative assessment of the two is provided by Aquina et al. (2025), which highlights that QKD's security guarantee based on information theory is, in theory, superior to the computational security assumptions of PQC, but also that other practical considerations, such as cost, range, trusted relay requirement, and a lack of standardised interoperability, limit the use of QKD to specific high-value applications rather than general purpose network security. However, PQC is a software update to existing cryptographic systems that can be transmitted across a traditional network, without the need for dedicated quantum hardware.

The best architecture for the highest security deployments is that both are used: QKD is used to establish a key for dedicated links between critical nodes, and PQC is used to provide authentication for QKD sessions, and to protect the vast majority of network communications that cannot be served by QKD. Huang et al. (2025) make this hybrid approach more feasible by proposing a zero-trust routing system that significantly diminishes the trusted relay weakness, which currently puts the greatest limitations on the scalability of QKD. As QKD hardware becomes increasingly cost-effective and as the standardisation work in the ITU-T and ETSI bodies progresses, the range of scenarios for using practical QKD in the future will grow, but for the time being PQC will be the main quantum-safe security solution for most digital communications.

5.5 Sector Specific Priorities and Constraints

The evidence reviewed shows that the challenge of quantum-safe migration is not the same and can have different levels of urgency, complexity and difficulty in different sectors. Financial services is an area of high urgency (HNDL exposure of long-lived financial records), high organisational capability and strong regulatory pressure — and thus is likely to be the sector most likely to make early, orderly migration. The patient records use case for healthcare is similarly time sensitive for HNDL, but has more technical challenges due to the legacy medical device ecosystem, low-resource IoT health monitoring devices, and the diversity of healthcare IT environments, from enterprise hospitals to small practices to home health monitoring.

The most complex migration challenge is for critical national infrastructure, such as power grids, water systems and industrial control systems, which have been built to last for decades and are dependent on specialised protocols (SCADA, ICS) with minimal computing power, and where security updates cannot be allowed to disrupt systems, because of the safety critical constraint involved. As PQC implementations are still the topic of ongoing research, with the goal of optimising parameters for lightweight implementations suitable for constrained devices, this is a key enabler for the quantum-safe transition of this sector, and a gap in current research literature.

5.6 Future Research Priorities

The synthesis of reviewed evidence results in 4 priority research directions. The first is the lightweight version of PQC for constrained environments: current NIST-standardised algorithms, whilst competitively performant on modern server and PC hardware, are so computational and memory intensive that they are not currently suitable for many IoT (Internet of Things) devices, smart cards and industrial control systems. Further research is required on optimising parameters, architectures to accelerate hardware, and efficiency at the protocol level to make PQC fit in the resource envelope of the most constrained embedded systems without compromising on security.

Second, quantum-safe protocol standards and cryptographic agility: Since TLS, SSH, S/MIME, PKCS, DNSSEC, and other protocols need to be updated to accommodate the shift from classical to PQC algorithms, this is the second aspect of quantum-safe security. Cryptographic agility (the ability to quickly change cryptographic algorithms in protocols without changing the protocol itself) should be built into new versions of protocols and backfitted into current protocols. The process of algorithm standardisation is well advanced by standardisation bodies such as IETF and ISO/IEC but the landscape of compliant implementations is still in its infancy.

Third, blockchain and distributed ledger post-quantum security: all the major blockchain systems rely on ECDSA digital signatures, which are used to verify transactions and secure wallets and thereby make the entire blockchain system quantum-vulnerable. Switching blockchains to PQC signatures, while keeping decentralised consensus, backwards compatibility and tolerable transaction throughput in the face of larger PQC signature sizes represents a technically challenging research problem with far-reaching financial consequences of the changes, given the size of cryptocurrencies and institutional blockchain deployments.

Fourth, formal security analysis of hybrid PQC-QKD: With the adoption of hybrid deployment combining PQC and QKD rapidly becoming a de facto strategy in practice, the formal security proof of the composed PQC-QKD protocol is underdeveloped, especially concerning the security implications of combining computational and information-theoretic security assumptions. There is a requirement for rigorous formal security analysis of hybrid architectures, to back up the decision to adopt such architectures with theoretical guarantees for the highest-security applications.

VI. CONCLUSION

6.1 Summary of Core Findings

The article has provided a systematic review of quantum computing and its impact on information technology security, following the journal quality standard and based on twenty-two (22) peer-reviewed publications (2023-2025). The central message - echoed by all the sources analyzed - is clear: quantum computing is an existential threat to the classical public-key cryptographic infrastructure that provides security for the entire global digital economy, and the transition to post-quantum security is not something for the future but an urgent strategic imperative, given the harvest now/decrypt later threat model.

The standards were published in August 2024 by NIST, the three finalised standards for post-quantum cryptographic algorithms: ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205), which offer the technical underpinning necessary to plan systematic migration to quantum-safe algorithms. The performance analysis in Abbasi et al. (2025) shows that the computationally heavy burden, a major obstacle for the deployment of these algorithms in mainstream applications, is not an issue when used with modern hardware. The biggest migration issues are not technical: cryptographic asset inventorying, hybrid deployment management, protocol standardisation and regulatory compliance in a variety of sector scenarios.

6.2 Contributions to Knowledge

In this review, the authors have four major contributions. First, it offers the most up-to-date complete overview of the implications of quantum computing for IT security, which is based on at least 20 peer-reviewed publications from the past three years (2023-2025), with a landmark publication of a NIST standard for PQC in August 2024 and follow-up performance analysis literature. Second, it provides a format of structured comparative performance data for all NIST PQC algorithms, and for the classical algorithms, that is immediately accessible by researchers and security architects. Third, it provides a comprehensive, evidence-based analytical framework for quantum threat analysis, PQC algorithm evaluation, QKD deployment evidence and sector-specific migration analysis. Fourth, it highlights and describes four priority research areas for the future — lightweight PQC, cryptographic agility, post-quantum blockchain security and formal hybrid PQC-QKD security analysis that are high impact research opportunities not sufficiently covered by current research.

6.3 Concluding Statement

The shift to quantum computers is the biggest cryptographic policy issue since the advent of public-key infrastructure in the 1970s. The inevitability of the threat to RSA and ECC with mathematical certainty, the rapidly advancing quantum hardware development and the active HNDL threat model means that this issue cannot be postponed. With the advent of NIST standardised PQC algorithms, the most daunting technical obstacle to migration is no longer there, and now it's an organisational, regulatory and operational obstacle. The evidence reviewed confirms the conclusion that organisations

that start structured PQC migration programs immediately, with a strategy of first inventories the cryptographic assets, then defining hybrid deployment architectures and then setting a roadmap based on NIST and sector-specific regulatory timelines, will reach quantum-safe security within the window before fault-tolerant quantum computing becomes operationally realisable. Those that don't will have a time pressured cryptographic transition crisis with the data already compromised through harvest, to be decrypted later through collection. It's a no-brainer, the time is now to act.

REFERENCES

[1] Abbasi, M., Cardoso, F., Váz, P., Silva, J., & Martins, P. (2025). A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. Cryptography, 9(2), 32. https://doi.org/10.3390/cryptography9020032

[2] Aquina, N., Cimoli, B., Das, S., Hövelmanns, K., Weber, F. J., Okonkwo, C., Rommel, S., Škorić, B., Tafur Monroy, I., & Verschoor, S. (2025). A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography. EPJ Quantum Technology, 12(1), 51. https://doi.org/10.1140/epjqt/s40507-025-00322-z

[3] 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). Journal of Information Systems and Informatics, 7(4), 1–28. https://doi.org/10.51519/journalisi.v7i4.1331

[4] Emmanni, P. S. (2023). The impact of quantum computing on cybersecurity. Journal of Mathematical & Computer Applications, 2(1), SRC/JMCA-172. https://doi.org/10.47363/JMCA/2023(2)140

[5] Gao, R., & Rajan, D. (2024). Quantum technologies for beyond 5G and 6G networks: Applications, opportunities, and challenges. IEEE Communications Surveys & Tutorials, 26(3), 1740–1812. https://doi.org/10.1109/COMST.2024.3358713

[6] Huang, M., Zhao, Y., Cao, L., & Zhang, J. (2025). A quantum key distribution routing scheme for a zero-trust QKD network system: A moving target defense approach. Big Data and Cognitive Computing, 9(4), 76. https://doi.org/10.3390/bdcc9040076

[7] Karmakar, A., Banegas, G., & Lange, T. (2024). On the security of quantum key distribution networks. Cryptography, 7(4), 53. https://doi.org/10.3390/cryptography7040053

[8] Kozhaya, D., Madziar, J., & Juhász, L. (2024). Quantum computing threats to cryptography: A comprehensive analysis of vulnerabilities, countermeasures, and future-proofing strategies. Research Square Preprint. https://doi.org/10.21203/rs.3.rs-6795420/v1

[9] National Institute of Standards and Technology. (2024). Module-lattice-based key-encapsulation mechanism standard (FIPS 203). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203

[10] National Institute of Standards and Technology. (2024). Module-lattice-based digital signature standard (FIPS 204). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204

[11] National Institute of Standards and Technology. (2024). Stateless hash-based digital signature standard (FIPS 205). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.205

[12] Pal, D., & Sau, D. (2025). Quantum computing: Threat to cybersecurity. In S. B. Goyal & S. M. N. Islam (Eds.), Quantum computing in cybersecurity. Springer. https://doi.org/10.1007/978-981-96-4948-8_7

[13] Parida, N. K., Jatoth, C., Reddy, V. D., Hussain, M., & Faizi, J. (2023). Post-quantum distributed ledger technology: A systematic survey. Scientific Reports, 13, 20182. https://doi.org/10.1038/s41598-023-47331-1

[14] Sasikumar, K., & Nagarajan, S. (2024). Comprehensive review and analysis of cryptography techniques in cloud computing. IEEE Access, 12, 52325–52351. https://doi.org/10.1109/ACCESS.2024.3385449

[15] Soni, R., Sharma, V., & Gupta, A. (2024). Quantum computing and its implications for cybersecurity: A comprehensive review of emerging threats and defenses. Nanotechnology Perceptions, 20(S13), 1–18. https://doi.org/10.62441/nano-ntp/np.v20iS13.4076

[16] Stanley, M., Gui, Y., Unnikrishnan, D., Hall, S., & Fatadin, I. (2022). Recent progress in quantum key distribution network deployments and standards. Journal of Physics: Conference Series, 2416, 012001. https://doi.org/10.1088/1742-6596/2416/1/012001

[17] Wang, K., Xu, D., & Tian, J. (2025). An improved two-step attack on lattice-based cryptography: A case study of Kyber. IEEE Transactions on Circuits and Systems II: Express Briefs. https://doi.org/10.48550/arXiv.2407.06942

[18] Zhao, Y., Cao, Y., & Wang, Q. (2023). Application and development of QKD-based quantum secure communication. Entropy, 25(4), 627. https://doi.org/10.3390/e25040627

[19] Zong, C. (2025). The mathematical foundation of post-quantum cryptography. Research, 2025, 0801. https://doi.org/10.34133/research.0801

[20] Dekkaki, K. C., & Tasic, I. (2024). Exploring post-quantum cryptography: Review and directions for the transition process. Journal of Information Systems and Informatics, 6(3), 1203–1222. https://doi.org/10.51519/journalisi.v6i3.672

[21] Muzenda, H., & Ndlovu, B. (2025). Post-quantum migration in the financial sector: A systematic review of readiness, risks, and transition frameworks. Journal of Information Systems and Informatics, 7(4), 29–55. https://doi.org/10.51519/journalisi.v7i4.1421

[22] Salas, C. J. R., & Barreto, D. F. M. (2024). Quantum cryptography, BB84 protocol, and implementation perspectives. ResearchGate Technical Report. https://doi.org/10.13140/RG.2.2.26217.67681