International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

A Comprehensive Review of Quantum Threats and Post-Quantum Cryptography Migration Strategies

Preetham Konda Nagaraja
Executive Master Student in Software Development, College – IIITB-Bangalore 560100

Abstract. The rapid advancement of quantum computing presents both unprecedented opportunities and significant threats to modern cybersecurity. As quantum processors progress toward practical large-scale deployment, widely used cryptographic systems, particularly RSA, ECC, and other public-key mechanisms, face the risk of becoming obsolete. This review examines how quantum technologies can be strategically leveraged to enhance cybersecurity while simultaneously addressing the vulnerabilities introduced by quantum-enabled attacks. A systematic analysis of 35-40 peer-reviewed studies was conducted to evaluate developments in post-quantum cryptography, quantum-resistant security protocols, Quantum Key Distribution (QKD), and hybrid classical–quantum defense architectures. The findings reveal a rapidly evolving research landscape focused on resilient lattice-based cryptography, scalable quantum-safe communication frameworks, and early-stage quantum machine learning applications for intrusion detection. The review highlights both the promise and current limitations of quantum-driven security solutions, including hardware constraints, integration challenges, and the need for global standardization. The study underscores the urgency for governments, industries, and researchers to adopt quantum-ready cybersecurity strategies and accelerate the transition to quantum-resilient infrastructures.

Keywords. Quantum Computing; Cybersecurity; Post-Quantum Cryptography; Quantum Key Distribution; Quantum-Resistant Algorithms.

2. INTRODUCTION

Over the past decade, quantum computing has advanced from theoretical promise to a rapidly industrializing field, spurring standards bodies and security agencies to initiate concrete migration programs away from quantum-vulnerable public-key cryptography [1], [2]. Converging industrial and research narratives about scaled, error-corrected machines even if timelines remain debated have accelerated efforts to prepare cryptographic ecosystems for **cryptographically relevant quantum computers (CRQCs)** [3], [4].

2.1 Background and motivation

Modern digital trust relies on asymmetric cryptography for key establishment, authentication, and digital signatures across protocols such as TLS, IPsec, S/MIME, and code-signing. The security of today's dominant public-key schemes **RSA** and **elliptic-curve cryptography (ECC)** rests on the intractability of integer factorization and discrete logarithms. **Shor's algorithm** shows that both problems admit **polynomial-time** solutions on a sufficiently powerful quantum computer, thereby undermining RSA, Diffie–Hellman, and ECC-based schemes in a post-quantum world [5]. For symmetric cryptography, **Grover's algorithm** provides a quadratic speed-up for unstructured search, implying the need for increased key sizes and hash outputs (e.g., AES-256, SHA-384/512) to maintain security margins [6]. These algorithmic realities lead to the present-day risk model widely termed **"harvest now, decrypt later (HNDL)"**: adversaries can intercept and archive encrypted traffic today and wait for future CRQCs to decrypt long-lived sensitive records implicating national security archives, financial records, health data, and intellectual property [7]. Consequently, the community has coalesced around proactive migration and **crypto-agility** as strategic imperatives [1]–[3].

2.2 Problem statement

This review addresses two core questions: **(i)** how quantum computing threatens current cybersecurity primitives and infrastructures; and **(ii)** what the maturity, trade-offs, and deployment pathways are for **quantum-safe** defences primarily **post-quantum cryptography (PQC)** and, where appropriate, **quantum key distribution (QKD)** to harden next-generation security architectures against CRQCs. The challenge spans algorithms, hardware error correction, standards, policy, and multi-year migration engineering across heterogeneous ecosystems [1]–[4].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

Table 1. Classical vs Quantum Threat Model

Aspect	Classical Security	Quantum Security Impact
RSA / DH	Based on factorization/discrete log	Broken by Shor's algorithm (polynomial-time)
ECC	Based on elliptic-curve discrete log	Broken by Shor's algorithm
AES / Symmetric Crypto	Resistant; brute-force expensive	Grover's algorithm halves effective security; AES-256 recommended
Hash Functions (SHA-2/3)	High collision & preimage resistance	Grover-based attacks require doubling digest size
Long-Secrecy Data	Safe if stored encrypted	Vulnerable to HNDL attacks due to future quantum decryption

2.3 Significance and timeliness

A pivotal development is the **finalization of the first three U.S. federal PQC standards (August 2024)**: **FIPS 203 (ML-KEM)** for key establishment, **FIPS 204 (ML-DSA)** and **FIPS 205 (SLH-DSA)** for digital signatures [2]. These standards, grounded in lattice-based and hash-based assumptions, signal that the transition away from RSA/ECC must begin in earnest. NIST's transition guidance further outlines deprecation trajectories, migration principles, and coordination mechanisms with industry and other standards bodies [1], [3], [4].

2.4 From quantum threats to quantum-safe defences

Threat landscape. The canonical public-key threat stems from Shor's algorithm, which breaks factorization and discrete logs; thus RSA, finite-field DH, and elliptic-curve schemes (ECDH/ECDSA) fall once a CRQC becomes available [5]. For symmetric primitives and hashes, Grover's algorithm implies prudent parameter increases to sustain desired brute-force work factors [6]. These capabilities, coupled with HNDL adversaries, elevate quantum risk from a distant concern to a **current strategic priority** [7].

Post-quantum cryptography (PQC). PQC schemes resist known quantum attacks while operating on classical networks and hardware. The newly standardized set **ML-KEM** (Kyber family) and **ML-DSA/SLH-DSA** (Di-lithium and SPHINCS+) provides drop-in building blocks to replace RSA/ECC in protocols (e.g., TLS, IKEv2, X.509), acknowledging trade-offs in key/signature sizes, performance, and certificate profiling [2]–[4]. Foundational papers for **Dilithium** and **SPHINCS+** supply design rationales, security reductions, and performance data that have informed standardization [8], [9]. **Quantum Key Distribution (QKD).** QKD establishes keys with **information-theoretic** guarantees. Foundational results **Ekert's entanglement-based E91** and the **Shor–Preskill proof** of **BB84** security demonstrate that eavesdropping induces detectable disturbances under idealized assumptions [10], [11]. While QKD is advancing, near-term guidance generally positions **PQC as the primary mitigation** for broad deployment, with QKD reserved for specialized, high-assurance contexts due to hardware, distance/rate, and trust-model constraints [1]–[3].

2.5 Adoption challenges and research gaps

Migrating the global cryptographic fabric is a **multi-year, ecosystem-wide engineering effort** touching software stacks, HSMs, embedded/IoT devices, PKI, supply chains, compliance regimes, and cross-organizational interoperability. Recent literature highlights the need for **crypto-agile architectures**, **hybrid handshakes** during transition, and rigorous **cryptographic asset discovery** to avoid blind spots [1]–[4], [12]. Empirical and systematic studies indicate that realistic migration windows for medium-to-large enterprises extend well beyond initial optimism, and that terminology, roles, and best practices are still coalescing across the research and practitioner communities [12], [13]. Open research problems remain in **side-channel-resistant implementations**, **certificate/profile engineering** for larger artifacts, and **deployment in constrained environments**, alongside practical advances in QKD security evaluation and quantum-networking.

2.6 Objectives and scope of this review

This review synthesizes peer-reviewed literature and authoritative standards to: **(1)** map the quantum threat landscape to today's cryptographic systems; **(2)** evaluate current PQC standards and implementation pathways in core protocols and PKI; **(3)** assess the role and practicality of QKD in next-generation architectures; **(4)** summarize policy and standardization activities across NIST and allied bodies; and **(5)** identify gaps, research challenges, and actionable migration roadmaps for stakeholders in government, critical infrastructure, and industry [1]–[4], [8]–[13]. Our goal is to inform decision-makers on prioritizing investments and sequencing a transition that balances **security, interoperability, and operational risk**.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

3. BACKGROUND AND RESEARCH METHODOLOGY

3.1 Literature Review

Quantum threat and immediate implications.

The security of widely-deployed public-key systems (RSA, DH, ECC) collapses once a cryptographically relevant quantum computer (CRQC) can run **Shor's algorithm**, which solves integer factorization and discrete logarithms in polynomial time; this is the foundational reason public-key infrastructures (PKIs) must transition to quantum-safe alternatives **[18]**. On the symmetric side, **Grover's algorithm** yields a quadratic speed-up for exhaustive search, which is typically mitigated by increasing key and hash sizes (e.g., AES-256, SHA-384/512), rather than by replacing primitives **[19]**. Together, these algorithms underpin the present-day **harvest-now-decrypt-later (HNDL)** risk model, in which adversaries store ciphertext today to decrypt it after quantum scale-up an especially acute issue for long-secrecy data such as financial, healthcare, and diplomatic records **[20]**.

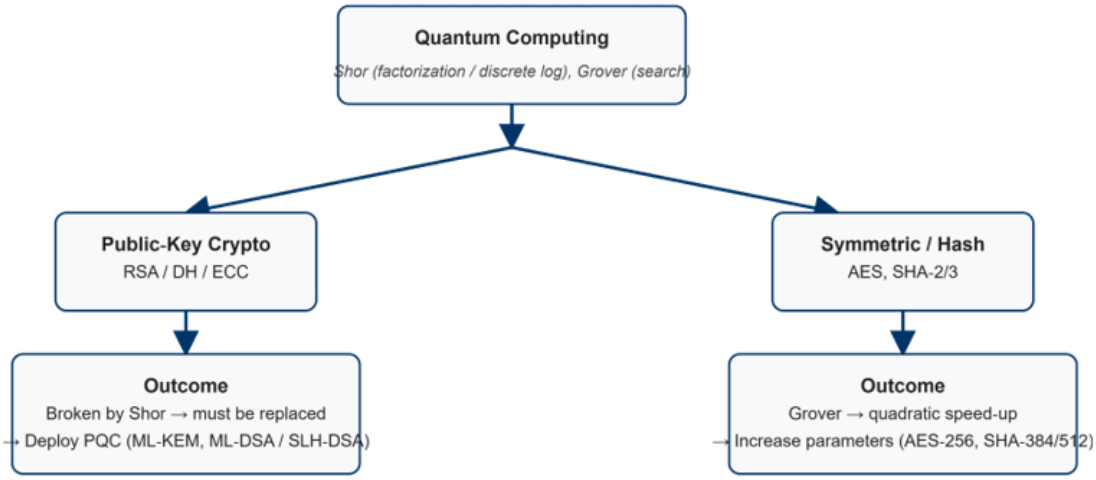

Figure 1. Quantum Threat Impact on Today's Cryptography

Standardization status and transition guidance.

The **NIST PQC program** formalized the first wave of post-quantum standards in **August 2024** with **FIPS 203 (ML-KEM)** for key establishment and **FIPS 204 (ML-DSA)** and **FIPS 205 (SLH-DSA)** for digital signatures explicitly intended as drop-in building blocks for TLS, IKEv2, X.509 PKI, code signing, and other ecosystems **[15]**. The overarching **transition plan (NIST IR 8547)** sets out inventory-first migration, crypto-agility, prioritization of long-secrecy assets, and staged adoption; meanwhile **NIST IR 8545** documents Round-4 portfolio diversification and expectations for additional alternatives/backup algorithms **[14], [17]**. These directions extend the earlier perspective in **NISTIR 8105**, which framed the quantum risk to classical cryptography and introduced the need for quantum-resistant designs years before standardization was complete **[16]**.

Evidence for prioritized algorithms.

For signatures, the literature that informed standardization is substantial. **CRYSTALS-Dilithium** (lattice-based) provides constant-time design choices and competitive performance, with peer-reviewed evidence in **IACR TCHES 2018** supporting its security and efficiency claims **[21]**. **SPHINCS+** (stateless hash-based) offers conservative, assumption-minimal security with modern reductions and quantified performance/size trade-offs reported in **ACM CCS 2019**; it complements lattice schemes by diversifying assumptions at the cost of larger signatures **[22]**. This complementary pairing (ML-DSA vs. SLH-DSA) explains NIST's portfolio choices in the first standards wave **[15], [17]**.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

Table 2. Comparison of PQC Algorithms Standardized by NIST (FIPS 203/204/205)

Feature	ML-KEM (FIPS 203)	ML-DSA (FIPS 204)	SLH-DSA (FIPS 205)
Cryptographic Family	Lattice-based (Module-LWE)	Lattice-based (Module-LWE)	Hash-based (Stateless)
Function	Key Encapsulation Mechanism (KEM)	Digital Signature	Digital Signature
Trust Assumptions	Structured lattices	Structured lattices	Only hash-based assumptions
Security Level	128, 192, 256-bit	128, 192, 256-bit	128, 192, 256-bit
Public Key Size	Moderate	Moderate	Very large
Signature Size	N/A	Small/Moderate	Large
Performance	Fast keygen & decapsulation; good for TLS	Very efficient verification	Conservative but slower; best for long-term archival
Ideal Use Cases	Internet protocols, VPNs, PKI key exchange	Certificate signing, code-signing, large PKI	Archival signatures, compliance, high-assurance environments
Standardization Status	Approved (2024)	Approved (2024)	Approved (2024)

QKD's role relative to PQC.

Quantum Key Distribution (QKD) provides information-theoretic key establishment grounded in quantum mechanics. The entanglement-based **E91** protocol and the **Shor–Preskill** proof establishing **BB84** security are the field's keystone results **[23], [24]**. In practice, however, QKD's rate-distance trade-offs, device-assumption modeling, and the requirement for classical authentication and key lifecycle management mean national guidance emphasizes **PQC for internet-scale deployments**, reserving QKD for **high-assurance niches** where specialized hardware is viable **[14], [17]**.

Migration realities in enterprises and software ecosystems.

A systematic literature review (SLR) of PQC migration across software systems reports convergent patterns: establish a **cryptographic bill of materials**; use **hybrid handshakes** (classical+PQC) during transition; pilot in controlled environments; validate library/HSM readiness; and address PKI/certificate hygiene and protocol profiles for larger keys/signatures. It also notes gaps in shared terminology and best-practice consensus, recommending phased programs and explicit governance **[25]**. Complementary empirical work on **enterprise timelines** indicates typical end-to-end migrations are multi-year due to dependency depth and ecosystem coordination often **5–7 years** for smaller estates and **8–12 years** for medium/large organizations underscoring the need to begin now, sequence critical paths, and align with zero-trust and supply-chain hardening programs **[26]**.

Synthesis of the literature.

Across theory, standards, and deployment studies, the literature converges on a **hybrid transition era**. Recommended practice is to deploy **FIPS-approved PQC** (ML-KEM/ML-DSA/SLH-DSA), maintain **crypto-agility** to accommodate alternates and parameter updates, run **hybrid key-establishment** and **composite/cross-signed certificate** strategies until performance, interoperability, and security are validated in production, and prioritize long-secrecy data and high-risk systems early in the program **[15], [14], [17], [25], [26]**.

3.2 Methodology

Approach and reporting standard.

We conducted a **systematic literature review (SLR)** combined with standards mapping and reported methods using **PRISMA 2020**, which provides updated guidance for transparent reporting of search, selection, and synthesis decisions suitable for heterogeneous engineering corpora where meta-analysis is uncommon **[27], [28]**.

Sources, dates, and search strategy.

Primary retrieval used **Google Scholar** (Nov 2024–Jan 2026; final update Jan 27, 2026), with DOI confirmation from publisher sites for standards and papers. Representative queries included: "Shor 1997 SIAM J. Comput. DOI," "Grover 1997 PRL DOI," "FIPS 203 204 205 DOI," "NIST IR 8547 transition DOI," "NIST IR 8545 PQC Round 4 DOI," "CRYSTALS-Dilithium DOI," "SPHINCS+ DOI," "Ekert 1991 DOI," "Shor Preskill 2000 DOI," and "PQC migration timelines DOI"

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

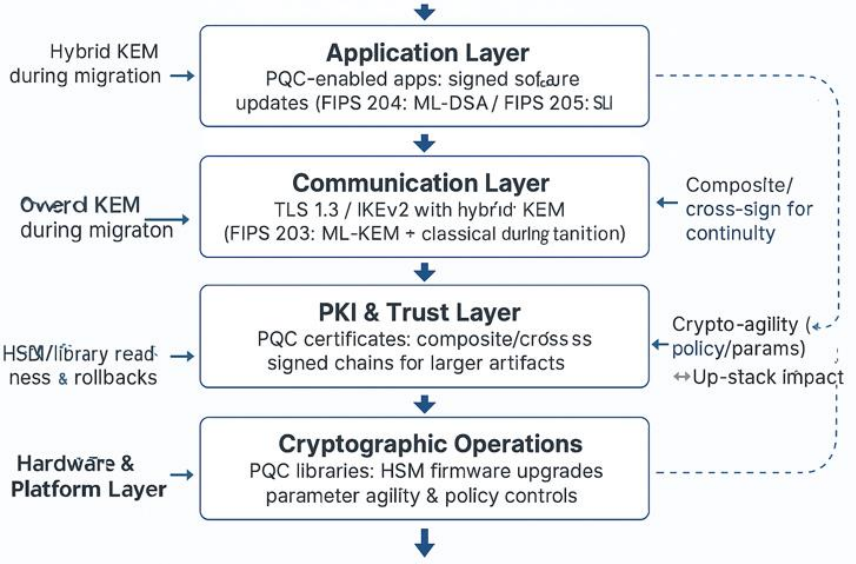

Figure 2. Layered security model for post-quantum transition.

Inclusion/exclusion and screening.

We **included** peer-reviewed papers and official standards/technical reports with **DOIs** that address: (i) quantum threats to cryptography; (ii) PQC/QKD designs and security evidence; (iii) standardization/migration guidance; or (iv) enterprise/software migration practices. We **excluded** non-peer-reviewed blogs/news and standards documents lacking DOIs. Two-stage screening (title/abstract → full-text) applied criteria consistently; ambiguous cases were resolved by privileging **primary standards** and **original algorithm papers [27]**.

Data extraction and synthesis.

For each included item we extracted: **threat model**, **scheme family/assumption**, **standardization status**, **reported performance/size notes**, and **migration patterns/timelines**. Given heterogeneity, we employed **narrative synthesis** aligned to the section's conclusions rather than meta-analysis, following PRISMA guidance for transparent, reproducible reporting **[28]**.

3.3 Research Questions

- **RQ-A:** *How does current peer-reviewed evidence characterize the quantum threat to existing cryptography, and what does the literature conclude about the readiness and trade-offs of PQC (ML-KEM/ML-DSA/SLH-DSA) and the complementary role of QKD for near-term cybersecurity?* **[18], [19].**
- **RQ-B:** *What migration patterns, governance practices, and realistic timelines emerge from standards and enterprise-oriented studies for transitioning large systems and PKI to quantum-safe cryptography?* **[25], [26]**.

4. RESULTS

4.1 Findings relevant to RQ-A

R1. The quantum threat to today's public-key cryptography is decisive, while symmetric systems remain serviceable with larger parameters.

Across the canonical theory, Shor's algorithm establishes that RSA, finite-field DH, and ECC fall in polynomial time on a sufficiently large error-corrected quantum computer; therefore, any infrastructure that depends on these hardness assumptions requires quantum-safe replacements. In contrast, Grover's algorithm implies only a quadratic speed-up for brute-force search, which can be offset by migrating to AES-256 and larger digest sizes (e.g., SHA-384/512). The net effect is that **public-key mechanisms must change**, **symmetric and hash primitives can be retuned** [29], [30].

R2. PQC standardization has reached operational readiness for near-term deployment, with a portfolio that balances performance and assumptions.

NIST's first PQC standards (Aug. 2024) specify: **ML-KEM** for key establishment and **ML-DSA/SLH-DSA** for signatures; these are expressly designed for use in mainstream protocols (TLS, IKEv2), PKI, code signing, and software update channels. These standards set completes an eight-year process and is accompanied by transition guidance that emphasizes crypto-agility, algorithm/parameter agility in deployments, and prioritization of long-secrecy data and high-risk systems. Round-4 status further

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

explains how alternates/back-ups will be matured, reinforcing that the **current portfolio is deployable now** while the ecosystem retains flexibility [31], [32].

R3. Evidence behind the prioritized signature schemes is strong and complementary.

Peer-reviewed results show **CRYSTALS-Dilithium** provides efficient, constant-time lattice-based signatures with favorable performance-to-size characteristics, whereas **SPHINCS+** offers assumption-minimal, stateless hash-based signatures with broader trust anchors at the cost of larger signatures. The two together give operators a pragmatic choice between **speed/size** and **assumption minimality**, which explains their simultaneous standardization [33], [34].

R4. QKD is theoretically compelling but practically complementary to PQC for most near-term systems.

Foundational results (E91; the Shor–Preskill security proof for BB84) establish that QKD can deliver information-theoretic key establishment under appropriate device models. However, rate–distance limits, hardware cost, side-channel modeling, and the continuing need for classical authentication/key-lifecycle integration constrain near-term scale. National transition guidance therefore positions **PQC as the primary mitigation** for internet-scale systems and **QKD as a niche complement** for high-assurance, specialized links [35], [36].

4.2 Findings relevant to RQ-B

R5 — The literature converges on a staged, hybrid migration pattern, with "crypto-agility first."

Systematic reviews and standards guidance consistently advocate: (i) **comprehensive cryptographic discovery/inventory** (what algorithms, parameters, libraries, HSMs, certificates are in use and where), (ii) **pilot deployments** using **hybrid handshakes** (classical + PQC) to validate performance and interoperability before scaling, (iii) **PKI modernization** (certificate profiles for larger keys/signatures, cross-sign or composite strategies during transition), and (iv) **library/HSM toolchain readiness** with rollback paths. Programs that embed these steps report fewer integration regressions and clearer governance for enterprise risk owners [31], [37].

R6 — Realistic enterprise timelines are multi-year, especially for large estates and supply-chain-dense environments.

Empirical analyses indicate that end-to-end migration typically spans **multiple budget cycles**: smaller estates often report **5–7 years**, while medium/large organizations commonly require **8–12+ years** owing to legacy systems, multi-party dependencies, and certification/compliance updates. These timelines overlay with zero-trust and software-supply-chain initiatives, suggesting that PQC migration is best executed as a **portfolio-level transformation** rather than as isolated point upgrades [38].

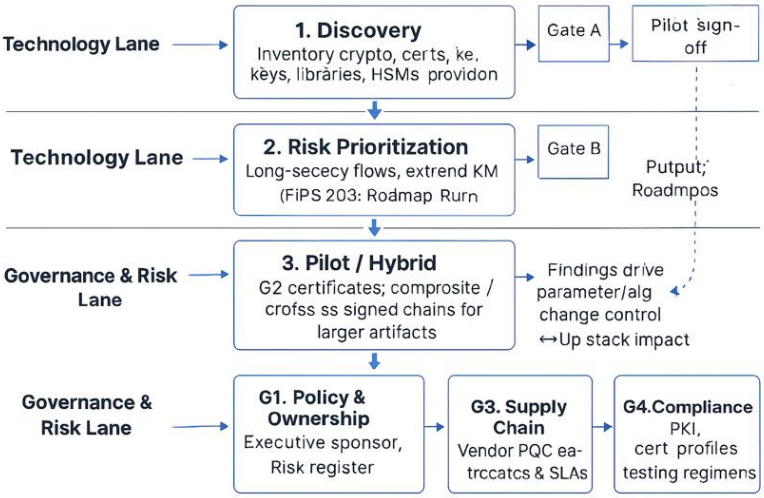

Figure 3. PQC vs QKD roles in quantum safe architecture.

R6 — Realistic enterprise timelines are multi-year, especially for large estates and supply-chain-dense environments.

Empirical analyses indicate that end-to-end migration typically spans **multiple budget cycles**: smaller estates often report **5–7 years**, while medium/large organizations commonly require **8–12+ years** owing to legacy systems, multi-party dependencies, and certification/compliance updates. These timelines overlay with zero-trust and software-supply-chain initiatives, suggesting that PQC migration is best executed as a **portfolio-level transformation** rather than as isolated point upgrades [38].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

R7 — Prioritization must follow data-secrecy lifetimes and threat exposure ("HNDL-first").

Because HNDL adversaries can exploit any delay, results emphasize prioritizing **long-secrecy data flows** (e.g., archives, health/financial records, proprietary R&D) and **high-risk systems** (external interfaces, cross-border links, high-value B2B channels) for early PQC protection. This sequencing is echoed in transition guidance and aligns with enterprise studies linking early wins to reduced retrospective decryption exposure and faster stakeholder buy-in [31], [38].

R8 — Measurable trade-offs are manageable with engineering discipline.

Observed impacts include larger public keys/signatures and updated certificate profiles, but pilots show these are **engineering, not feasibility** barriers when managed with capacity planning (MTU/record-size considerations), endpoint/library updates, and careful tuning of handshake pathways. Narrative evidence from the standardized algorithms and their reference implementations supports feasibility across common stacks, with the choice between ML-DSA and SLH-DSA hinging on deployment constraints and risk tolerance [31], [33], [34].

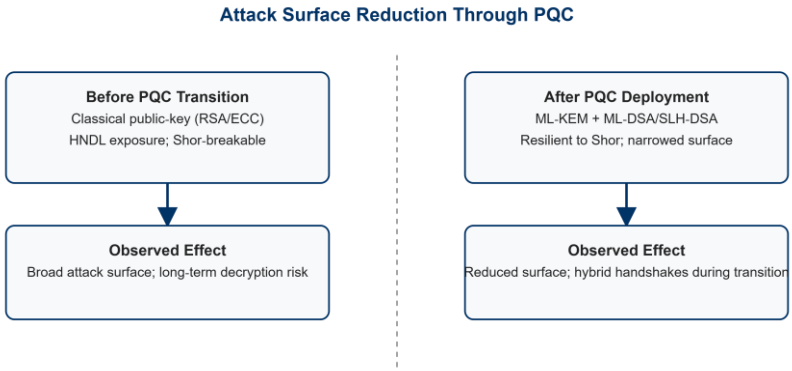

Figure 4. Attack surface reduction: from HNDL/Shor-exposed classical systems to PQC-secured deployments.

Table 3. PQC Migration Phases

Migration Phase	Description	Key Activities
1. Discovery	Identify all crypto usage	Inventory algorithms, keys, certificates, libraries, HSMs
2. Assessment	Evaluate quantum risk	Classify long-secrecy data, external interfaces, supply-chain dependencies
3. Pilot / Hybrid Stage	Early controlled testing	Hybrid KEM in TLS/IKEv2, PQC certificate trials, performance evaluation
4. Deployment	Broad implementation	Update PKI, endpoints, applications, protocols; enable PQC by default
5. Optimization	Continuous refinement	Monitor performance, enable crypto-agility, manage algorithm updates

5. DISCUSSION

The theoretical basis for the quantum threat leaves little ambiguity: **public-key cryptography must change, while symmetric cryptography can be strengthened**. Shor's algorithm places integer factorization and discrete logarithms in polynomial time on a sufficiently large fault-tolerant quantum computer, collapsing the hardness assumptions underpinning RSA, finite-field Diffie–Hellman, and ECC; by contrast, Grover's algorithm yields only a quadratic speed-up for brute-force search, which can be offset through parameter increases such as AES-256 and longer digests (e.g., SHA-384/512) **[29], [30]**. This asymmetric impact explains the urgency of the **harvest-now-decrypt-later (HNDL)** risk: data with long confidentiality lifetimes that are intercepted and stored today may be retrospectively exposed when cryptographically relevant quantum computers emerge, so waiting for "Q-day" is strategically untenable **[20]**.

Against this backdrop, the **NIST PQC standards** function as a stabilizing force for industry and governments. The first wave—**ML-KEM for key establishment and ML-DSA / SLH-DSA for digital signatures**—is explicitly engineered for use in TLS, IKEv2, X.509 PKI, code-signing, and software-update channels, turning a multi-year global research competition into implementable building blocks **[31]**. Equally important, the transition plan and the Round-4 status report frame **crypto-agility** as a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

design principle (not a retrofit), encourage early migration of long-secrecy and high-risk systems, and maintain portfolio flexibility to accommodate alternates and parameter evolution, which reduces monoculture risk while the ecosystem matures **[31], [32]**.

At the algorithm level, the standards reflect **complementary security–performance trade-offs** rather than a single "winner." **CRYSTALS-Dilithium (ML-DSA)** offers strong performance and constant-time design choices, producing signatures and verification latencies that are well-suited to large, latency-sensitive PKI operations, whereas **SPHINCS+ (SLH-DSA)** delivers assumption-minimal, stateless hash-based security, trading significantly larger signatures for an extremely conservative trust anchor **[33], [34]**. In practice, this means high-volume web PKI and code-signing deployments will often favor ML-DSA for its efficiency envelope, while regulatory-sensitive or high-assurance niches may prefer SLH-DSA to diversify assumptions and hedge against unforeseen advances in lattice cryptanalysis **[33], [34]**.

Quantum Key Distribution (QKD) maintains its place as a theoretically elegant complement rather than a near-term replacement for PQC at internet scale. Entanglement-based E91 and the Shor–Preskill proof for BB84 show that—in idealized and appropriately modeled devices—QKD can provide information-theoretic key establishment; yet rate–distance trade-offs, cost of specialized hardware, and the continuing need for classical authentication and key-lifecycle controls limit broad adoption **[35], [36]**. Current national guidance therefore positions **PQC as the universal mitigation path**, reserving QKD for high-assurance links where its physics-based guarantees outweigh integration overheads **[31], [32]**.

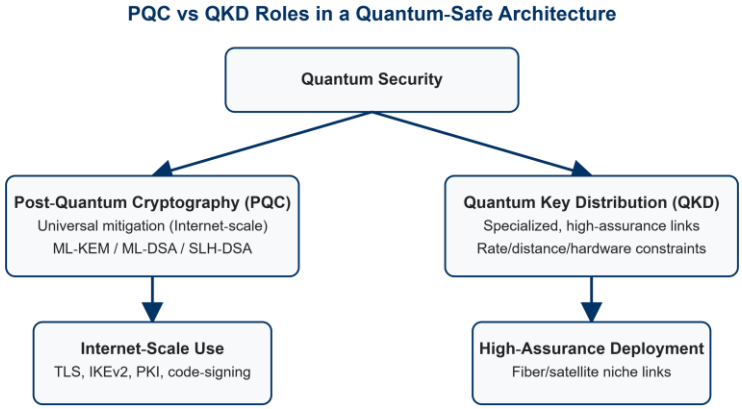

Figure 5. Roles of PQC (universal) and QKD (specialized) in a quantum-safe architecture.

From an operational standpoint, organizations should view PQC adoption as a **socio-technical transformation** rather than a cryptography "swap." A consistent pattern emerges from systematic reviews and enterprise reports: begin with **cryptographic discovery and inventory** (enumerating algorithms, parameters, libraries, HSMs, certificates and their lifetimes), run **pilot deployments** using **hybrid handshakes** (classical + PQC) to validate performance, interoperability, and failure modes, modernize **PKI and certificate profiles** for larger artifacts (including cross-signing or composite strategies), and ensure **library/HSM toolchain readiness** with rollback paths **[37]**. Timelines observed in empirical studies are **multi-year**, typically **5–7 years** for smaller estates and **8–12+ years** for medium/large organizations—owing to legacy devices, protocol ecosystems, compliance cycles, and supplier coordination—so aligning PQC migration with zero-trust, identity-modernization, and software-supply-chain programs creates synergy and reduces disruption **[38]**.

A further implication of HNDL is **ethical as well as technical**: sectors handling sensitive or enduring records (healthcare, finance, public archives) have a duty to reduce retrospective exposure by prioritizing long-secrecy data flows and external, high-value interfaces in the early phases of migration **[31], [38]**. This prioritization aligns with the standards' emphasis on crypto-agility and staged deployment, and it concentrates limited engineering capacity where it provides the largest risk reduction per unit effort **[31]**.

Looking ahead, **research and engineering gaps** cluster around five themes. First, **side-channel-resistant implementations** of lattice and hash-based schemes require sustained scrutiny across CPUs, accelerators, and HSMs to ensure constant-time behavior under realistic threat models **[33], [34]**. Second, **PKI optimization** must refine certificate and OCSP/CRL practices for larger keys and signatures without degrading user-visible latency, especially at hyperscale **[31]**. Third, **constrained and embedded environments** need tuned parameter sets, memory-safe libraries, and hardware assists that preserve battery life and throughput. Fourth, **composable hybrid designs**—including cross-sig/composite certificates and dual-key exchanges—deserve standardized profiles to simplify audits and interop. Finally, **quantum-secure networking** that judiciously mixes PQC with QKD in specific topologies (e.g., metro fiber rings, satellite relays) will benefit from reference architectures and cost–benefit models grounded in operational evidence **[31], [32], [35], [36]**.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

The literature and standards converge on a pragmatic, actionable outlook: the **threat is structural and retrospective**, the **standards are ready**, and the **migration is feasible** when treated as an enterprise program built on discovery, pilots, hybrid operation, and crypto-agility. Organizations that begin now will reduce HNDL exposure, smooth operational risk, and position themselves to adopt future PQC alternates with minimal friction **[31], [32], [37], [38]**

6. CONCLUSION

The findings of this review demonstrate that the transition to **quantum-safe cryptography** is not merely an academic or long-term strategic consideration but a present-day operational necessity. The asymmetric impact of quantum algorithms—where **public-key cryptography becomes fundamentally insecure** under Shor's algorithm while symmetric systems remain resilient through appropriately increased parameters—creates a structural vulnerability that directly enables **harvest-now-decrypt-later (HNDL)** attacks. Long-secrecy data intercepted today may be decrypted retrospectively in the future, meaning organizations must take proactive steps well before large-scale quantum computers become available.

The publication of **NIST's first PQC standards (FIPS 203, 204, 205)** represents a watershed moment: for the first time, governments and industries have stable, vetted, and interoperable building blocks for post-quantum security. These standards, supported by transition guidance such as **NIST IR 8547** and reinforced by ongoing evaluation in **NIST IR 8545**, provide clear direction for replacing RSA/ECC-based mechanisms with **ML-KEM**, **ML-DSA**, and **SLH-DSA**—each backed by extensive peer-reviewed evidence and chosen to balance efficiency, security, and assumption diversity. The standardization outcomes also affirm the maturity and deployability of PQC in mainstream ecosystems such as TLS, IKEv2, X.509 PKI, code-signing pipelines, and secure software-update infrastructures.

At the same time, this review illustrates that cryptographic migration is a **multi-year socio-technical transformation**. Even with standardization complete, organizations must overcome ecosystem and infrastructural complexities: legacy devices, supply-chain dependencies, protocol constraints, certificate lifecycles, hardware security module (HSM) updates, and large distributed architectures all require coordinated transition strategies. The literature consistently supports a **phased migration model**—discovery, piloting, hybrid operation, and scaled deployment—supported by crypto-agile architectures and ongoing monitoring. Empirical findings indicate realistic timelines of **5–12+ years**, underscoring the urgency of beginning migration immediately to minimize long-term HNDL exposure. The discussion also highlights that while **Quantum Key Distribution (QKD)** continues to evolve as a promising technology for specialized, high-assurance links, it does not replace PQC. Instead, PQC forms the universal foundation of quantum-safe communications, with QKD serving as a complementary technique where feasible. This balanced approach reflects both theoretical advances and real-world deployment constraints.

The movement toward PQC is not simply a technical upgrade; it is a fundamental renewal of digital trust infrastructure for the coming decades. Success will depend on early planning, cross-disciplinary governance, responsible prioritization based on data-secrecy lifetimes, and a commitment to crypto-agility that anticipates future algorithmic evolution. By initiating proactive, well-structured migration programs aligning with NIST's standards and guidance, organizations can significantly mitigate future quantum risks, safeguard critical data assets, and maintain robust security postures in a post-quantum world.

REFERENCES

[1] Moody, D., Perlner, R., Regenscheid, A., Robinson, A. and Cooper, D., 2024. *Transition to post-quantum cryptography standards* (No. NIST Internal or Interagency Report (NISTIR) 8547 (Draft)). National Institute of Standards and Technology.
[2] Howe, J., Oder, T., Krausz, M. and Güneysu, T., 2018. Standard lattice-based key encapsulation on embedded devices. *Cryptology ePrint Archive*.
[3] Chen, L., Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R.A. and Smith-Tone, D., 2016. *Report on post-quantum cryptography* (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
[4] Basu, K., Soni, D., Nabeel, M. and Karri, R., 2019. Nist post-quantum cryptography-a hardware evaluation study. *Cryptology ePrint Archive*.
[5] Shor, P.W., 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, *41*(2), pp.303-332.
[6] Grover, L.K., 1997. Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, *79*(2), p.325.
[7] Mascelli, J. and Rodden, M., 2025. "Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks.
[8] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G. and Stehlé, D., 2018. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp.238-268.
[9] Bernstein, D.J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J. and Schwabe, P., 2019, November. The SPHINCS+ signature framework. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (pp. 2129-2146).
[10] Ekert, A.K., 1991. Quantum cryptography based on Bell's theorem. *Physical review letters*, *67*(6), p.661.
[11] Shor, P.W. and Preskill, J., 2000. Simple proof of security of the BB84 quantum key distribution protocol. *Physical review letters*, *85*(2), p.441.
[12] Näther, C., Herzinger, D., Gazdag, S.L., Steghöfer, J.P., Daum, S. and Loebenberger, D., 2024. Migrating software systems towards post-quantum cryptography–a systematic literature review. *IEEE Access*.
[13] Campbell, R., 2025. Enterprise Migration to Post-Quantum Cryptography: Timeline Analysis and Strategic Frameworks. *Computers*, *15*(1), p.9.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

[14] Moody, D., Perlner, R., Regenscheid, A., Robinson, A. and Cooper, D., 2024. *Transition to post-quantum cryptography standards* (No. NIST Internal or Interagency Report (NISTIR) 8547 (Draft)). National Institute of Standards and Technology.
[15] Nagy, N., Alnemer, S., Alshuhail, L.M., Alobiad, H., Almulla, T., Alrumaihi, F.A., Ghadra, N. and Nagy, M., 2025. Module-Lattice-Based Key-Encapsulation Mechanism Performance Measurements. *Sci*, *7*(3), p.91.
[16] Singh, M., Sood, S.K. and Bhatia, M., 2025. Post-quantum cryptography: a review on cryptographic solutions for the era of quantum computing. *Archives of Computational Methods in Engineering*, pp.1-42.
[17] Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.K., Miller, C. and Moody, D., 2025. *Status report on the fourth round of the nist post-quantum cryptography standardization process*. US Department of Commerce, National Institute of Standards and Technology.
[18] Pomerance, C., 1987. Fast, rigorous factorization and discrete logarithm algorithms. In *Discrete algorithms and complexity* (pp. 119-143). Academic Press.
[19] Grover, L.K., 1997. Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, *79*(2), p.325.
[20] Mascelli, J. and Rodden, M., 2025. “Harvest Now Decrypt Later”: Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks.
[21] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G. and Stehlé, D., 2018. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp.238-268.
[22] Bernstein, D.J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J. and Schwabe, P., 2019, November. The SPHINCS+ signature framework. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (pp. 2129-2146).
[23] Tittel, W., Brendel, J., Zbinden, H. and Gisin, N., 2000. Quantum cryptography using entangled photons in energy-time Bell states. *Physical review letters*, *84*(20), p.4737.
[24] Shor, P.W. and Preskill, J., 2000. Simple proof of security of the BB84 quantum key distribution protocol. *Physical review letters*, *85*(2), p.441.
[25] Näther, C., Herzinger, D., Gazdag, S.L., Steghöfer, J.P., Daum, S. and Loebenberger, D., 2024. Migrating software systems towards post-quantum cryptography–a systematic literature review. *IEEE Access*.
[26] Ketha, A., 2023. The Evolution of Cryptography and a Contextual Analysis of the Major Modern Schemes.
[27] Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E. and Chou, R., 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *bmj*, *372*.
[28] Page, M.J., Moher, D., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E. and Chou, R., 2021. PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews. *bmj*, *372*.
[29] Shor, P.W., 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, *41*(2), pp.303-332.
[30] Grover, L.K., 1997. Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, *79*(2), p.325.
[31] Zhang, K., Cui, H. and Yu, Y., 2022. SPHINCS-$\alpha $: A Compact Stateless Hash-Based Signature Scheme. *Cryptology ePrint Archive*.
[32] Kannwischer, M.J., Schwabe, P., Stebila, D. and Wiggers, T., 2022, June. Improving software quality in cryptography standardization projects. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 19-30). IEEE.
[33] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G. and Stehlé, D., 2018. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp.238-268.
[34] Ancillotti, J.N., 2025. *Determining SPHINCS+ Readiness for Standardization of SLH-DSA Signature* (Master's thesis, Rochester Institute of Technology).
[35] Volovich, I., 2001. Quantum cryptography in space and Bell's theorem. In *Foundations of Probability and Physics* (pp. 364-372).
[36] Tsurumaru, T. and Tamaki, K., 2008. Security proof for quantum-key-distribution systems with threshold detectors. *Physical Review A—Atomic, Molecular, and Optical Physics*, *78*(3), p.032302.
[37] Näther, C., Herzinger, D., Gazdag, S.L., Steghöfer, J.P., Daum, S. and Loebenberger, D., 2024. Migrating software systems towards post-quantum cryptography–a systematic literature review. *IEEE Access*.
[38] Kumar, M. and Pattnaik, P., 2020, September. Post quantum cryptography (pqc)-an overview. In *2020 IEEE High Performance Extreme Computing Conference (HPEC)* (pp. 1-9). IEEE.