The American Journal of
Engineering and Technology

ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 50-58
DOI 10.37547/tajet/Volume07Issue10-06

Quantum-Resilient Key Management Infrastructure

Naman Jain

Senior Software Development Engineer Seattle, Washington, USA

OPEN ACCESS

SUBMITED 30 August 2025
ACCEPTED 28 September 2025
PUBLISHED 10 October 2025
VOLUME Vol.07 Issue 10 2025

CITATION
Naman Jain. (2025). Quantum-Resilient Key Management Infrastructure. The American Journal of Engineering and Technology, 7(10), 50–58. https://doi.org/10.37547/tajet/Volume07Issue10-06

Abstract: Within the scope of the study an analysis of a quantum-resistant key management infrastructure (KMI) is conducted. Key Management Infrastructure, in this context, encompasses cloud services, on-premises HSM clusters, and hybrid or edge solutions. Asymmetric algorithms underpinning modern protection protocols demonstrate vulnerability to quantum methods of Shor and Grover. The objective of this study is to perform a holistic reference architecture for KMI that enables a seamless and secure transition from classical to post-quantum solutions. The methodology includes a systematic analysis of existing KMI architectures, a detailed evaluation of algorithms standardized by NIST for post-quantum cryptography, as well as the modeling of a hybrid cryptographic scheme. As a result, a multi-layer architectural model is proposed, featuring a "Crypto-Agility Engine" for dynamic algorithm replacement, hybrid key encapsulation protocols and a phased migration strategy to post-quantum primitives. The model maintains backward compatibility with legacy systems, minimizes the load on mission-critical components such as fintech platforms and ensures an unchanged level of performance. The study conclusions confirm the practical feasibility of this approach for long-term protection of data confidentiality and integrity in the post-quantum era. This work is of interest to information security architects, software engineers and specialists engaged in the protection of critically important information across diverse infrastructures.

Keywords: post-quantum cryptography, key management, crypto-agility, quantum threat, PQC, hybrid encryption, security architecture, cybersecurity, data protection, compliance.

Introduction

The rapid shift of the global economy to the digital plane and the ubiquitous centralisation of key management infrastructures (KMIs), whether cloud services, on-premises HSM clusters, or IoT/edge controllers has transformed them into central trust anchors and processors of highly sensitive data, ranging from personal information to financial transactions and state secrets. According to a forecast by Gartner, Inc., global end-user spending worldwide on public cloud services was expected to grow by 20.4% to reach USD 675.4 billion in 2024 compared to USD 561 billion in 2023. The drivers of this growth are generative AI (GenAI) and application modernization [1]. This reflects a broader trend: the increasing reliance on centralized key management infrastructures (KMIs), whether deployed in hyperscale clouds, enterprise HSM clusters, or distributed edge environments. Similarly, the APEC Digital Economy Steering Group reports that the digital economy already accounts for 4.5% to 15.5% of global GDP, and that about 70% of new economic value over the next decade will arise from digitally enabled platforms [2]. As value creation concentrates in these platforms, their underlying cryptographic infrastructures, particularly KMIs, become critical trust anchors. Reinforcing this point, the Global Encryption Trends Study (2023), surveyed over 4,000 experts, found that HSM adoption increased from 47% in 2019 to 57% in 2022, while 63% of firms as of 2023 used cryptography-as-a-service solutions (including cloud KMS or HSM clusters) [3]. The security of these infrastructures has traditionally depended on cryptographic methods, primarily asymmetric schemes (RSA, ECC), which through key management protect data in transit and at rest. However, this long-standing shield is now facing significant risk due to advances in quantum computing.

The relevance of the topic is determined by the so-called quantum threat — the possibility of building a sufficiently powerful quantum computer capable of solving factorization and discrete logarithm problems in polynomial time, long-standing foundations of classical cryptography [5]. Although creating full-fledged quantum machines remains a colossal engineering challenge, leading technology corporations and governmental bodies are actively investing in this endeavor. An illustration of steady progress is the IBM Condor quantum processor with 1000 qubits [6]. The threat is twofold: first the data intercepted today may be stored for subsequent decryption ("harvest now, decrypt later"); second long-term stored data are at risk — financial obligations, medical records, state archives.

Alongside active work on standardizing post-quantum cryptographic schemes by the US National Institute of Standards and Technology (NIST) [7] there is a noted absence of holistic industrial-ready architectural solutions for integrating PQC algorithms into existing high-load key management infrastructure (KMI). Existing studies typically focus either on comparative analysis of individual post-quantum primitives or on theoretical frameworks of crypto-agility, while overlooking pressing practical aspects: performance metrics, scalability issues, ensuring backward compatibility and, most importantly, developing a strategy for smooth migration for systems requiring availability characteristic of the financial sector.

The objective of this study is to conduct a comprehensive analysis of the quantum-resilient key management infrastructure (KMI) across cloud, enterprise, and hybrid environments, with the aim of enabling a seamless and secure transition from traditional cryptographic primitives to post-quantum solutions.

The scientific novelty of this work lies in proposing an integrated hybrid architecture combining classical and post-quantum cryptographic primitives within a single crypto-agility protocol. This ensures seamless and fully secure migration of key material in large-scale distributed systems without degradation of quality of service.

A hypothesis is put forward that the proposed approach based on a hybrid key encapsulation mechanism (KEM) will achieve the required quantum resistance of KMI while maintaining acceptable performance metrics and supporting backward compatibility during the transition phase.

Materials and methods

In recent years the rapid development of enterprise products - including cloud services, on-premises systems, and hybrid solutions has driven the necessity for the creation of reliable and efficient key management architectures resilient to threats posed by the advent of quantum computing. Research in this domain can be provisionally divided into several thematic blocks: market assessment and survey works on the protection of enterprise environments; analysis of the quantum threat and the capabilities of quantum computing systems; comparative evaluation of the performance of post-quantum cryptographic algorithms under various conditions; particularities of the application of post-quantum mechanisms in resource-constrained devices; integration of post-quantum cryptography into public key infrastructure.

Firstly, the forecast of infrastructure growth and review of existing solutions for encryption and key management play a fundamental role in substantiating the relevance of the problem. For example, a Gartner, Inc. study [1] demonstrated that by 2024 global end-user spending on public cloud services would exceed 675 billion USD, indicating the continual expansion of digital infrastructure. In addition, the Hardware Security Modules Market Forecast (2025) [4] projects that the global HSM market - core to enterprise key management - will double from USD 1.66 billion in 2025 to USD 3.28 billion by 2030 (a compound annual growth rate of approximately 14.5%). Moore T. L., et al. [10] provide a broad review of modern encryption methods and key management systems for ensuring confidentiality, including distributed HSM models and key rotation mechanisms using provider APIs. It is also noteworthy that the ENISA document provides an overview of the state of post-quantum cryptography and recommendations for the transition to quantum-resistant algorithms in corporate and government structures, with the significant emphasis on hybrid migration schemes and phased testing of NIST algorithms [9].

Secondly, analysis of the current capabilities of quantum computing machines and algorithmic advancements is key for understanding the scope and timelines of migration to post-quantum solutions. In the article by Gerck E. [5] a theoretical analysis of quantum algorithms suitable for processing broken functions is conducted, indicating the potential for enhanced attacks on cryptographic systems in the medium-term perspective. On the other hand, the report by Gambetta J. M. [6] from IBM Quantum demonstrates progress in increasing qubit counts and reducing quantum circuit errors, outlining a roadmap for the development of quantum processors up to 2033 and emphasizing that the practical threat of real quantum attacks on classical cryptosystems may emerge as early as the next decade. Google Cloud Blog (2025) provides a detailed description of the implementation of quantum-secure signatures within key management systems and outlines an action plan for PQC support [14]. The NTT Data report (2022) examines organization challenges in managing key lifecycle and personnel during the transition to PQC [15].

Thirdly, a significant body of research is devoted to comparative analyses of the performance and resource requirements of post-quantum algorithms in various computing environments. Dziechciarz D., Niemiec M. [7] conduct a detailed comparative analysis of algorithms standardized by NIST for digital signatures on diverse hardware and software platforms, revealing that even optimized implementations require on average 3–5 times more computational resources than classical RSA or ECDSA schemes. Abbasi M., et al. [13] extend this approach by proposing a practical set of benchmarks for evaluating algorithms on heterogeneous computing clusters, including GPU and FPGA, where significant accelerations are achieved, but key transmission remains a bottleneck due to the large data structures of NTRU and Falcon algorithms.

The fourth group of works unites studies aimed at the deployment of post-quantum schemes under stringent constraints: in his review Asif R. [12] highlights predominantly lattice-based algorithms, showing that they possess a better security-to-performance ratio compared to code-based and multivariate approaches, and offers parameter selection recommendations for IoT controllers. Simultaneously, Hanna Y., et al. [8] emphasize the need for an integrated approach that considers not only algorithmic properties but also network protocol characteristics and energy efficiency.

Finally, within the scope of integrating post-quantum cryptography into existing public key infrastructure Bene F., Kiss A. [11] examine the architectural and protocol changes required for a phased transition of PKI, including support for new certificate formats and backward compatibility, which allows the minimization of risks for certificate holders and authentication services.

It is also appropriate within the scope of the study to mention the following sources: APEC Digital Economy Steering Group (2024) [2] establishes a framework for interoperability, trust, and ICT (Information and Communications Technology) security in a cross-border environment, explicitly identifying increased trust and security in the use of ICT as a focus and linking KMI with the implementation of the APEC Internet and Digital Economy Roadmap; thereby KMI should ensure a managed evolution of algorithms and policy compatibility in multilateral data flows. Ponemon Institute and Encryption Consulting (2023) [3] report sustained growth in encryption coverage and the migration of sensitive workloads to the cloud. At the same time, the labor intensity of key lifecycle management, the inventorying of cryptographic dependencies, and workforce shortages become the primary barriers, which amplifies demand for centralized KMS and the use of HSM as hardware roots of trust [3]. Thales Group [16] proposes hybrid modes (classical+PQC) with key orchestration via HSM and readiness to include selected NIST algorithms in product stacks. Cisco [17] details quantum-safe trust anchors - updating Secure Boot/Trust Anchor for PQ signatures, expanding PQC support in TLS/IKE/SSH, and aligning the migration schedule application ↔ firmware ↔ TPM (Trusted Platform Module)/UEFI (Unified Extensible Firmware Interface).

Thus, the survey literature forms a heterogeneous picture: on the one hand market-wide and review works underline the strategic necessity of migrating to post-quantum solutions [1, 9, 10], on the other hand fundamental research on quantum algorithms and quantum computer roadmaps point to the reality of the threat in the medium-term perspective [5, 6]. However, in evaluations of the performance and deployment of algorithms divergences are clearly observed: some authors highlight the readiness of standardized schemes for mass application after optimizations [7, 13], while others point to serious obstacles in energy and resource consumption, especially in IoT contexts [8, 12]. A conflict also arises in the selection of priority algorithmic families: while NIST standards favor hybrid and lattice-based schemes, some studies propose increased attention to code-based and multivariate approaches currently deferred for future consideration.

Among the insufficiently covered issues in the literature it is possible to identify: the integration of post-quantum KMI with contemporary multi-tenant and distributed enterprise environments; the need for dynamic key rotation across heterogeneous systems where both classical and post-quantum mechanisms may coexist; the operational and cost implications of migration to new cryptographic standards; as well as issues of regulatory compliance and auditing when deploying post-quantum certificates and HSMs. In addition, deeper study is required for the adaptation of network protocols and key material formats when transitioning from a classical to a quantum-resistant infrastructure, regardless of whether these are deployed in cloud, on-premises, or hybrid models

Results and Discussion

Based on the conducted analysis and identified gaps a comprehensive architecture for a quantum-resilient key management infrastructure (QR-KMI) was proposed. This model was specifically designed with crypto-agility requirements in mind ensuring high performance and a phased migration to new algorithms thus enabling reliable long-term data protection across mission-critical domains such as fintech and healthcare [7, 12].

The presented multi-tier QR-KMI architecture (see Figure 1) is divided into a control plane (Control Plane) and a data plane (Data Plane) following recognized distributed-system design best practices. The central component is Crypto-Agility Engine - a logical module responsible for executing all cryptographic operations. This engine embodies the principle of Crypto-Agility, defined as the ability to migrate from one cipher to another without significant changes to the system infrastructure. This concept is considered critical by security authorities in several countries for the impending transition to PQC [15]:

- Control Plane: provides mechanisms for authentication and authorization of entities, enforcement of key access policies, and full audit of the key lifecycle (creation rotation revocation). Interaction with external systems and entities is performed through standardized interfaces. Policies define the cryptographic schemes - classical post-quantum or hybrid - for each key type and processed data.

- Data Plane: is responsible for executing requests from authorized entities for core cryptographic operations - encryption, decryption, data key generation and digital signatures. Unlike traditional key management systems, where the choice of cryptographic primitives is rigidly fixed, in the proposed QR-KMI all requests are directed to a unified processing mechanism.

- Crypto-Agility Engine: serves as an abstraction of cryptographic primitives decoupling operational logic from higher-level application or business processes. It contains implementations of classical algorithms (for example RSA-4096 ECDH-P384) and post-quantum schemes (CRYSTALS-Kyber CRYSTALS-Dilithium). Based on policies defined in the control plane the engine dynamically selects the required algorithm or their combination (a hybrid scheme) to fulfill a given request

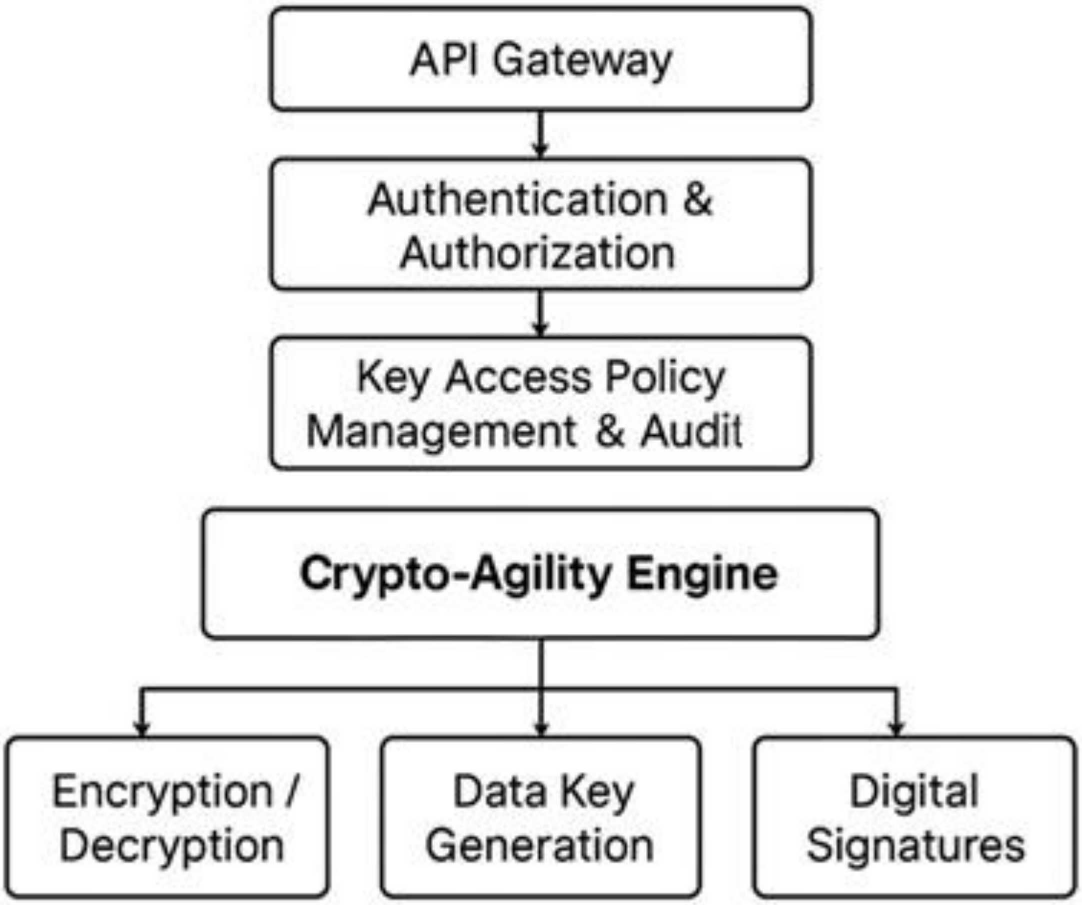

Fig. 1. High-level architecture of QR-KMI [6, 10, 11].

Such an organization of the system enables cryptographic protocols to be adapted by modifying configuration parameters and policies in the control plan, without necessitating changes in the client implementation of client applications or dependent systems. This solution demonstrates the practical realization of the principle of crypto-agility.

The key component ensuring data preservation during the transition to new cryptographic algorithms is the Hybrid Key Encapsulation mechanism. When a request is made to encrypt a Data Key (DK) using the Master Key managed within the QR-KMI, the following operations are executed (see Figure 2):

The system generates two distinct ephemeral key sets: a traditional one (for example, based on elliptic curves, ECDH) and a post-quantum one (for example, CRYSTALS-Kyber).

The obtained Data Key (DK) undergoes double encryption, producing two independent ciphertext objects: the first using a classical algorithm, the second using a PQC method.

Both encrypted keys, together with the corresponding public components of the ephemeral keys, are assembled into a single unified cryptographic container (Hybrid Ciphertext).

For decryption, the requesting entity transmits the constructed hybrid container. The QR-KMI, relying on its master key, sequentially decrypts each fragment. If one of the employed schemes (classical or post-quantum) is compromised, the security of the Data Key is preserved through the resilience of the other scheme. This approach provides reliable protection against both current threats and forthcoming quantum attacks, while also serving as a safeguard in case vulnerabilities are later discovered in still insufficiently studied PQC algorithms [13]. This strategy is analogous to the hybrid mode proposed for network protocols like TLS 1.3, which can combine classical and PQC algorithms for both key exchange and digital signatures to ensure communication security [15].

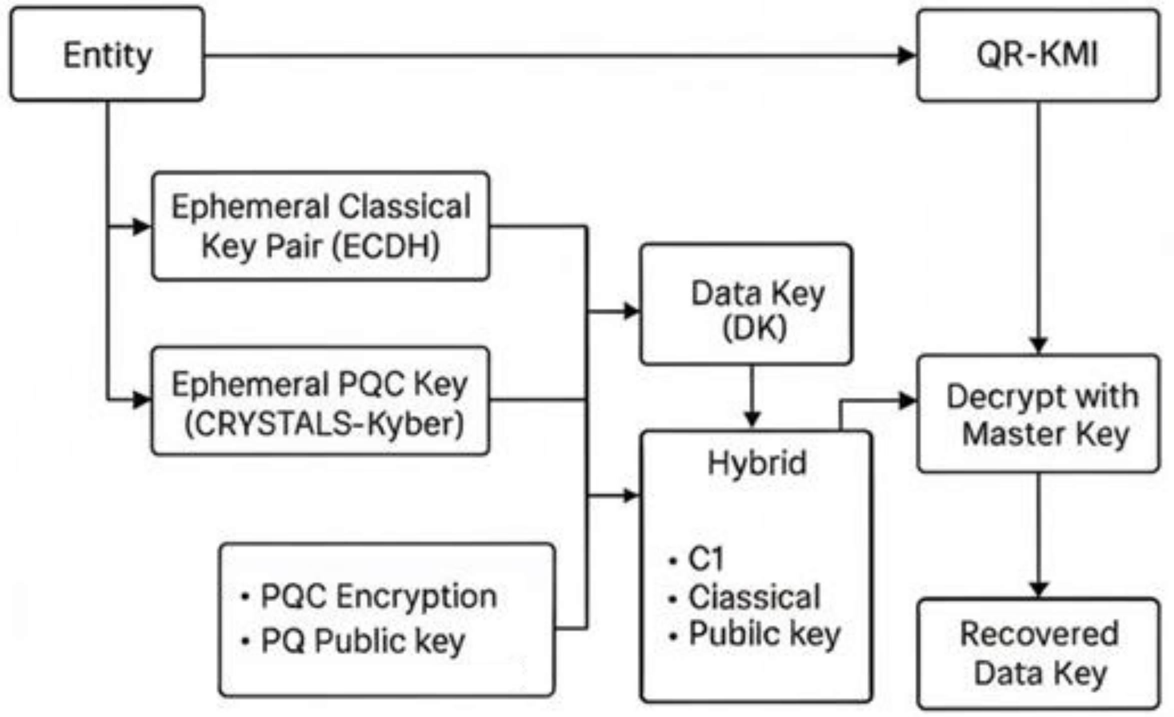

Fig.2. The process of hybrid encapsulation and deencapsulation of the key [8, 9, 13].

As demonstrated by the comparative analysis, the post-quantum encryption algorithm Kyber provides substantially higher throughput compared to RSA and achieves performance levels close to that of ECDH, although its keys and ciphertexts are significantly larger in size. When employing a hybrid combination of ECDH and Kyber, the load on computational resources involved in key operations doubles, while the volume of transmitted cryptographic information is approximately ten times greater than the equivalent measure for a purely classical ECDH scheme [8, 9].

To understand the impact of such an extension of the cryptographic subsystem on a high-throughput infrastructure, a simulation of request processing latency across varying transactional load level (TPS) was conducted in the context of a QR-KMI-based fintech platform. The simulation results revealed that under low traffic volumes the hybrid scheme adds approximately 45 % to the baseline latency; however, even at peak levels of tens of thousands of operations per second the average latency remains within a few milliseconds. Considering that in most financial applications the total transaction latency is measured in hundreds of milliseconds, the proposed overlay represents an acceptable compromise in favor of long-term resilience to quantum threats. Additional scaling of data-processing components further mitigates the impact of increased cryptographic load on end-to-end performance metrics [6, 7].

Equally important in the deployment of QR-KMI is a well-structured strategy for transitioning from traditional schemes to quantum-resistant ones; a phased migration is proposed (see Figure 3). In the initial phase (Hybrid-Observe), all newly generated data keys are encrypted in hybrid mode while retaining classical algorithms to ensure backward compatibility and verification of correct operation. The objective of this phase is to collect performance statistics, identify bottlenecks and verify resilience without requiring a radical abandonment of proven mechanisms. In the second phase (Hybrid-Enforce), after confirming system stability, strict hybrid encryption policies are enforced for all new operations, and previously stored data is re-encrypted (re-keyed) in the background according to the new standards; concurrently, the replacement of internal digital signatures with post-quantum schemes (for example, Dilithium) may be initiated to strengthen component authentication. The final phase (PQC-Primary) occurs once an adequate level of maturity and reliability of PQC algorithms has been established: the Control Plane policies are updated so that the system switches entirely to the use of the post-quantum component of the hybrid ciphertext, and the classical component is decommissioned [9, 13].

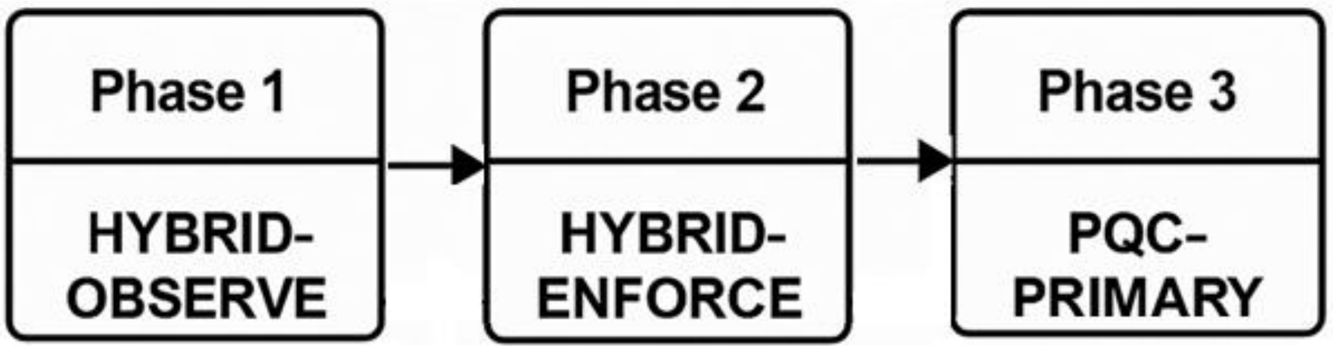

Fig.3. The scheme of step-by-step migration to quantum-stable KMI [6, 7, 9, 13].

The phased methodology provides organizations with the opportunity to prepare in advance for the quantum-computing era by distributing the risks and financial costs of migration over time, while simultaneously ensuring uninterrupted business processes, which is critically important for the financial sector and other industries where even minimal downtime is unacceptable.

These architectural principles and migration strategies are rapidly moving from theory to practice. Across the industry, organizations are beginning to roll out support for the new PQC standards. For example, in August 2024, following the finalization of NIST standards, Google Cloud announced the preview availability of quantum-safe digital signatures (ML-DSA as per FIPS 204 and SLH-DSA as per FIPS 205) within its Key Management offerings [14]. This capability enables the generation of signatures resistant to future quantum attacks, which is critical for long-lived assets such as root-of-trust certificates and secure software updates. Interestingly, while the proposed architecture in this paper focuses on hybrid key encapsulation, Google has noted the lack of industry consensus on hybrid signature schemes, and has therefore initially introduced non-hybrid signature algorithms, with plans for broader PQC support in both software and hardware implementations [14]. In parallel, Thales has introduced PQC capabilities in its Luna HSMs and network encryptors, running hybrid (classical + PQC) pilots with enterprise customers to validate migration strategies [16]. Cisco is similarly preparing quantum-safe Trust Anchor modules and Secure Boot mechanisms, aligning hardware root-of-trust components with NIST PQC standards and planning rollouts in 2025–2026 [17]. Collectively, these initiatives underscore the broader industry response to the “Harvest Now, Decrypt Later” threat model.

As a result, the proposed architectural scheme and migration strategy form a cohesive solution that effectively counteracts threats from quantum technologies, while maintaining the high levels of performance and stability required by modern enterprise applications and ensuring the necessary degree of cryptographic flexibility to adapt to forthcoming changes in encryption standards.

Conclusion

Under the conditions of an escalating quantum threat capable of undermining the security of existing cryptographic standards, the task of developing a holistic architecture for a quantum-resistant key management infrastructure (QR-KMI) was posed and successfully accomplished.

A key feature of the proposed model is the hybrid key encapsulation mechanism combining traditional and post-quantum primitives. This approach provides protection against contemporary attacks while simultaneously accounting for potential vulnerabilities of future quantum computations, thereby mitigating downtime risk associated with the immaturity of certain PQC-algorithms. The proposed strategy of phased migration to post-quantum algorithms ensures a smooth transition for organizations, minimizing operational risks and allowing for the distribution of investment costs over time.

Thus, the hypothesis regarding the practical feasibility of an architectural approach based on cryptographic agility and hybrid solutions has been confirmed: the proposed model establishes a robust foundation for the long-term protection of confidential data and serves as a detailed guide for security engineers and architects in addressing the challenges of the post-quantum era.

Future Work

The proposed model creates several immediate avenues for practical validation and extension. First, systematic benchmarking of the hybrid KEM approach should be performed across representative infrastructures: for example, deploying the QR-KMI prototype on a cloud-native clusters, fintech-grade HSM platform, and an IoT gateway, and publishing comparative latency, throughput, and scalability results. Second, pilot integration projects should be initiated with regulatory frameworks such as PCI DSS 4.0, GDPR, and sector-specific banking regulations, producing compliance mappings that demonstrate auditability under PQC-enabled infrastructures. Third, multi-tenant distributed deployments should be evaluated by constructing sandboxed test environments where tenant isolation, trust boundaries, and key lifecycle automation can be validated under high-transaction workloads. Finally, longitudinal monitoring of PQC algorithms - through continuous measurement of failure rates, performance drift, and resilience against emerging cryptanalytic advances - should be institutionalized within QR-KMI deployments, ensuring that enterprises retain provable security guarantees throughout the migration period.

References

1. Gartner. (2024). Gartner forecasts worldwide public cloud end-user spending to surpass $675 billion in 2024. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2024-05-20-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-surpass-675-billion-in-2024

2. APEC Digital Economy Steering Group. (2024). APEC Digital Economy Outlook. Retrieved from https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group#:~:text=The%20digital%20economy%20is%20sometimes,based%20on%20digitally%20enabled%20platforms

3. Ponemon Institute & Encryption Consulting. (2023). Global Encryption Trends Study 2023. Encryption Consulting. Retrieved from https://www.encryptionconsulting.com/wp-content/downloads/encryption-consulting-global-encryption-trends-2023.pdf#:~:text=%E2%80%93%20about%2063%25,leveraging%20the%20private%20cloud%20model

4. MarketsandMarkets. (2025). Hardware Security Modules Market Forecast 2025–2030. Retrieved from https://www.marketsandmarkets.com/Market-Reports/hardware-security-modules-market-162277475.html#:~:text=This%20growth%20is%20primarily%20driven,in%20shaping%20the%20market%20dynamics

5. Gerck, E. (2022). Algorithms for Quantum Computation: The Derivatives of Discontinuous Functions. *Mathematics, 11*(1), 1–8. https://doi.org/10.3390/math11010068.

6. Gambetta, J. M. (2023). The hardware and software for the era of quantum utility is here. *IBM Research Blog*. Retrieved from https://research.ibm.com/blog/quantum-roadmap-2033

7. Dziechciarz, D., & Niemiec, M. (2024). Efficiency analysis of NIST-standardized post-quantum cryptographic algorithms for digital signatures in various environments. *Electronics, 14(1)*, 1–18. https://doi.org/10.3390/electronics14010070.

8. Hanna, Y., et al. (2025). A comprehensive and realistic performance evaluation of post-quantum security for consumer IoT devices. *Internet of Things*, 33. https://doi.org/10.1016/j.iot.2025.101650.

9. ENISA. (2021). Post-quantum cryptography: Current state and quantum mitigation. European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Post-Quantum%20Cryptography%20Current%20state%20and%20quantum%20mitigation-V2.pdf

10. Moore, T. L., et al. (2023). Encryption methods and key management services for secure cloud computing: A review. In Midwest Instruction and Computing Symposium (MICS-2023), University of Northern Iowa, Cedar Falls, IA, USA, 1–17. Retrieved from https://www.researchgate.net/profile/Akalanka-Mailewa/publication/369777264_Encryption_Methods_and_Key_Management_Services_for_Secure_Cloud_Computing_A_Review/links/642c54c020f25554da0baa40/Encryption-Methods-and-Key-Management-Services-for-Secure-Cloud-Computing-A-Review.pdf

11. Bene, F., & Kiss, A. (2023). Post-quantum security overview of the public key infrastructure. *System Theory, Control and Computing Journal, 3(2)*, 27–

35. https://doi.org/10.52846/stccj.2023.3.2.55.

12. Asif, R. (2021). Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms. *IoT, 2(1)*, 71–91. https://doi.org/10.3390/iot2010005.

13. Abbasi, M., et al. (2025). A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. *Cryptography, 9(2)*, 1–27. https://doi.org/10.3390/cryptography9020032.

14. Google Cloud. (2024). Announcing quantum-safe digital signatures in Cloud KMS. Google Cloud Blog. Retrieved from https://cloud.google.com/blog/products/identity-security/announcing-quantum-safe-digital-signatures-in-cloud-kms

15. NTT Data. (2022). Key management issues in cloud and the introduction of post-quantum cryptography. Retrieved from https://www.nttdata.com/global/en/insights/focus/2024/key-management-issues-in-cloud-and-the-introduction-of-post-quantum-cryptography#:~:text=Key%20management%20issues%20in%20cloud,and%20points%20to%20conside

16. Thales Group. (2024). Quantum-resilient encryption and HSMs. Thales Security Blog. Retrieved from https://cpl.thalesgroup.com/blog/encryption/post-quantum-cryptography-algorithms#:~:text=With%20crypto%20agility%20implemented%20across,Thales%20is%20also%20accelerating%20practical

17. Cisco. (2024). Quantum-safe trust anchors. Cisco Security Blog. Retrieved from https://blogs.cisco.com/security/quantum-cryptography-whats-coming-next