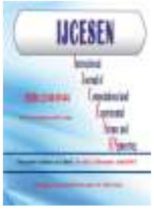
International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.3 (2025) pp. 6910-6917
http://www.ijcesen.com

Research Article



ISSN: 2149-9144

Safeguarding Next-Generation Cloud Infrastructure through Quantum-Resistant Security Protocols

Harsh Kaushikbhai Patel*

Independent Researcher, USA
* **Corresponding Author Email:** harshkp011@gmail.com-**ORCID:** 0000-0002-3519-8000

Article Info:

DOI: 10.22399/ijcesen.3938
Received : 25 July 2025
Accepted : 11 September 2025

Keywords

Post-Quantum Cryptography
Cloud Security
Lattice-Based Cryptography
Cryptographic Agility
Quantum Threat Mitigation

Abstract:

The hyperbolic progression of quantum computing technology poses challenges that the modern cryptographic standards have never seen before to secure the infrastructures of clouds around the world. The quantum version of such vulnerabilities exists with respect to quantum-based attacks using algorithms such as the Shor algorithm, potentially attacking the current cryptographic tools that preserve data integrity and confidentiality. The present technical overview discusses the imperative need to adopt quantum-resistant security protocols, otherwise known as post-quantum cryptography, as cloud security infrastructures of the future. It carries out an in-depth analysis of key principles of quantum-resistant cryptography, such as the mathematical underpinnings that can guarantee security, and how they are applied to safeguard cloud infrastructure in particular. In addition, the article discusses the developments of these cryptographic methods, their technical requirements, and implementation issues as well. Different post-quantum cryptographic strategies such as lattice-based systems, hash-based signature schemes, code-based cryptography, and multivariate quadratic equation-based approaches are analyzed in a detailed discussion of strengths, barriers, and applicability in the cloud. The article is concluded with the evaluation of the overall impact of such adoption of quantum-resistant protocols, including environmental, economic, and societal ones, providing strategic advice to stakeholders available to achieve a secure cloud infrastructure throughout quantum computing.

1. Introduction

1.1 Current Cloud Computing Landscape

The cloud computing infrastructure has also developed as the backbone behind modern digital services, with the capability to allow organizations and individuals to remotely access, store, and process large volumes of data. As the industry analysis shows, the dynamics of cloud services adoption in the enterprise environment have a stable increasing trend of growth with a significant increase in spending on public clouds over the past year in Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) segments. The studies by Gartner show that the same business trends are causing organizations to rapidly increase their cloud-first approaches due to digital transformation efforts, a distributed workforce, and the necessity of business responsiveness in an unstable economy [1]. This is a migration that reflects not only the maturity of the cloud-based technologies, but also the growing centrality of cloud technologies within enterprise IT architectures. The current proliferation of cloud data centers around the world has turned into massive data stores of sensitive information attached to cryptographic protocols safeguarding the data confidentiality, integrity, and secure authentication procedures across a sprawling digitalized environment that stretches far beyond financial services to health records and intellectual property.

Yet quantum computing technology is coming along too fast and is potentially a fatal blow to these security measures. Quantum computers exploit the quantum mechanical phenomena of superposition and entanglement in order to accelerate the completion of particular computational tasks exponentially compared with their classical counterparts. Larger technology firms and research organizations keep rolling out progress on quantum processors; each new generation has more qubits and a longer coherence length. The theoretical underpinnings of this threat were in place with Peter Shor and his seminal work on the quantum algorithms, which showed that quantum computers could efficiently factor integers and calculate discrete logarithms - the mathematical problem bases of many highly-deployed cryptographic algorithms such as RSA (Rivest-Shamir-Adleman) and Elliptic curve cryptography [2]. Shor presented the algorithm of quantum methods finding the solutions to some mathematical problems that could be considered solvable only by means of classical methods in exponential time, which was the fundamental shift in the security of public-key cryptography. Although massive quantum computers able to break present-day cryptographic measures have yet to be created, the curve is shifting closer to them being developed, thereby undermining, in the long term, the security model of the present-day cloud infrastructure and actively requiring the development and adoption of quantum-resistant security protocols.

1.2 Identified Security Gaps

In spite of recent innovations in cloud security solutions, the majority of infrastructure cannot be secure against adversaries that have access to quantum-based computing. There is also a large discrepancy between the theoretical foundations of quantum-safe algorithms and the implementation of such schemes at the scale needed in the public clouds. There is a consistent lack of organizational preparedness in the face of quantum threats, as documented by security researchers, with a small number of enterprises carrying out detailed quantum risk assessments or developing coherent quantum-safe transition plans. The issues facing organization are many-fold: post-quantum cryptographic mechanisms typically need much more computing resources than what is necessary in their current forms, thus inevitably pose a performance challenge in resources-constrained settings, integrating the designs with incumbent systems will necessitate potentially complicated changes both to deeply embedded protocols and cryptographic libraries, and there remains uncertainty as to which of the large number being considered will become standardized as the currently ongoing evaluation process concludes. Migration plans are also further complicated by the necessity to support backward compatibility through long transition periods and the availability of helping them to adopt quantum-safe protocols before a quantum computer of significant scale becomes available. Most organizations are unlikely to have complete quantum resistance of their cloud infrastructure over the next several years.

1.3 Article Scope and Objectives

This technical analysis aims to elucidate the foundational concepts of quantum-resistant cryptography and their specific application to securing next-generation cloud infrastructure. The discussion focuses on explaining core cryptographic principles, tracing their historical development trajectory from Shor's groundbreaking algorithm through the launch of NIST's Post-Quantum Cryptography Standardization process to the selection of the first standardized algorithms. Technical specifications and implementation requirements are examined, including computational efficiency considerations for various post-quantum approaches, key size implications for storage and transmission, and integration pathways with existing public key infrastructure systems. The analysis provides a detailed assessment of the mathematical foundations of leading quantum-resistant candidates, including lattice-based cryptography, hash-based signature schemes, code-based cryptography, and multivariate quadratic equation systems, evaluating their relative strengths and implementation challenges. Additionally, the article highlights the practical relevance of these protocols in operational cloud environments and examines their broader implications for technology ecosystems and society, including economic considerations of early adoption versus delayed implementation, regulatory compliance requirements, and the potential consequences of quantum-related data breaches if mitigation strategies are not implemented before quantum computing reaches cryptographically relevant capabilities.

2. Core Technical Concepts

2.1 Quantum Computing Threat Analysis

Quantum computers make use of quantum parallelism and entanglement to perform calculations that would still be computationally hard for classical computing systems. As opposed to the classical bits, which can be only in the state of 0 or 1, quantum bits (qubits) can be both in the state of 0 or the state of 1 at the same time, and that results in the capability of quantum computers to find the way through hundreds of solution paths simultaneously. This fundamental capability directly threatens cryptographic protocols dependent on the computational difficulty of specific mathematical problems. The RSA algorithm, which secures numerous internet communications channels, including financial transactions, healthcare data exchanges, and governmental communications, relies on the practical impossibility of factoring extremely large integers using classical computing approaches. The security guarantee diminishes exponentially when quantum computing enters the equation, as demonstrated by extensive theoretical analysis in the field of quantum algorithmics [3]. Similarly, elliptic curve cryptography depends on the difficulty of solving discrete logarithm problems within elliptic curve structures, providing equivalent security to RSA with significantly smaller key sizes, yet it remains equally vulnerable to quantum computational approaches.

Such mathematical problems can be readily solved by quantum algorithms, notably Shor's algorithm in 1999, due to the ability of quantum Fourier transforms to determine periodic patterns in apparently random mathematical data, effectively nullifying classical cryptographic applications. It is the Shor algorithm, when run on a quantum computer powerful enough to carry it out, and factorization is being taken to run in polynomial time rather than the exponential time that is exceedingly difficult to realize in normal algorithms. The issue is not only confined to those cryptographical implementations, but applies to more core protocols to secure cloud services infrastructure like TLS (Transport Layer Security), SSL (Secure Sockets Layer) and VPN (Virtual Private Network) technologies, all of which use these classical algorithms to accomplish the transfer of secure key exchanges and verification of digital signatures. The practical implication is that the encrypted message sent or stored now may be decrypted later when quantum computers become large enough and stable enough to achieve useful performance, forming a kind of harvest-now-decrypt-later threat scenario that must be taken seriously by the security architect communities in cloud environments.

Table 1. *Computational Complexity Comparison: Classical vs. Quantum Computing [3, 4]*

Cryptographic Problem	Classical Computing Complexity	Quantum Computing Complexity	Vulnerability Level
Integer Factorization (RSA)	Exponential Time	Polynomial Time	Severe
Discrete Logarithm (ECC)	Exponential Time	Polynomial Time	Severe
Symmetric Encryption (AES-256)	Exponential Time	Sub-exponential Time	Moderate
Hash Functions (SHA-256)	Exponential Time	Quadratic Speedup	Moderate

2.2 Post-Quantum Cryptographic Approaches

Post-quantum cryptography is cryptographic algorithms aimed at remaining secure even to both classical and quantum computational attacks. Such algorithms depend on the mathematical problems which are conjectured not to be vulnerable to attacks with quantum computers since they are fundamentally different from the mathematical structures of integer factorisation and discrete logarithm. The National Institute of Standards and Technology has led a comprehensive multi-year evaluation process to identify promising candidates for standardization, with selection criteria emphasizing security, performance, and implementation characteristics across diverse computing environments [4]. The primary categories of post-quantum cryptographic algorithms include:

● **Lattice-Based Cryptography**: This approach relies on the computational hardness of lattice problems, such as the Learning With Errors (LWE) problem and its ring-based variants. Lattices represent multidimensional mathematical structures where finding the closest vector or shortest vector presents extreme computational difficulty, even for quantum algorithms. Notable implementations include NTRUEncrypt, which has withstood over two decades of cryptanalysis, CRYSTALS-Kyber, selected by NIST for key encapsulation standardization, and CRYSTALS-DILITHIUM, selected for digital signature applications. Lattice-based schemes effectively support encryption, digital signatures, and key exchange operations with relatively efficient performance characteristics and robust security guarantees derived from worst-case hardness assumptions. Their mathematical foundation provides strong security assurances while maintaining practical operational characteristics, including reasonable key sizes and computational efficiency compared to other post-quantum approaches. The versatility of lattice-based approaches enables implementations across various cloud security contexts, from secure communications channels to authenticated API gateways and encrypted data storage systems.

● **Hash-Based Signature Schemes:** An implementation using the security features of cryptographic hash functions to provide a digital signature whose security does not depend on structured mathematical problems, but solely on the collision resistance of the underlying hash function. Representative ones are XMSS (eXtended Merkle Signature Scheme) and LMS (Leighton-Micali Signature Scheme), and have been standardized respectively in IETF RFC 8391 and NIST SP 800-208. Merkle-tree-based. The ideas behind these schemes generalize the original tree-based signature concept in two ways by building hierarchical structures of authentication that efficiently verify digital signatures and have certain properties of forward security.. While offering strong security assurances with the simplest security proofs among post-quantum approaches, hash-based signatures typically generate larger signature sizes compared to classical cryptographic methods and face challenges related to state management requirements. Their implementation proves particularly valuable for firmware signing, software update authentication, and other applications where signature generation frequency remains limited but verification security is paramount.

- **Code-Based Cryptography:** Based on error-correcting code mathematics developed initially for reliable communications over noisy channels, code-based cryptography provides substantial security assurances through the difficulty of decoding general linear codes. Classic McEliece, one of the oldest post-quantum systems dating to 1978 and remaining unbroken despite decades of cryptanalytic scrutiny, represents a significant implementation in this category. Their security is based on the NP-hardness of decoding random linear codes and thus poses challenging difficulties to both classical and quantum adversaries. Nevertheless, such schemes typically necessitate an exceptionally large size of the public keys with usually hundreds of kilobytes and even megabytes, which can be a problem with certain implementation requirements in resource-constrained settings, like IoT devices deployed in cloud-based infrastructure. Recent research has focused on reducing key sizes through alternative code structures while maintaining security margins, though these approaches often introduce additional cryptanalytic considerations requiring careful security analysis.
- **Multivariate Quadratic Equation-Based Schemes:** These cryptographic methods rely on the computational difficulty of solving systems of multivariate quadratic equations over finite fields, a problem proven to be NP-hard and resistant to known quantum algorithmic approaches. The mathematical foundation involves constructing systems with trapdoor functions that allow easy solution verification but extremely difficult solution generation without secret knowledge. Rainbow represents a notable implementation example, though recent cryptanalytic advances have identified specific vulnerabilities in its structure. These schemes offer remarkably rapid signature generation and verification capabilities but may require substantial key storage resources and face ongoing cryptanalytic challenges requiring regular parameter adjustments. Their implementation characteristics make them potentially suitable for authentication systems requiring minimal computational overhead but with sufficient storage capacity for large key structures.

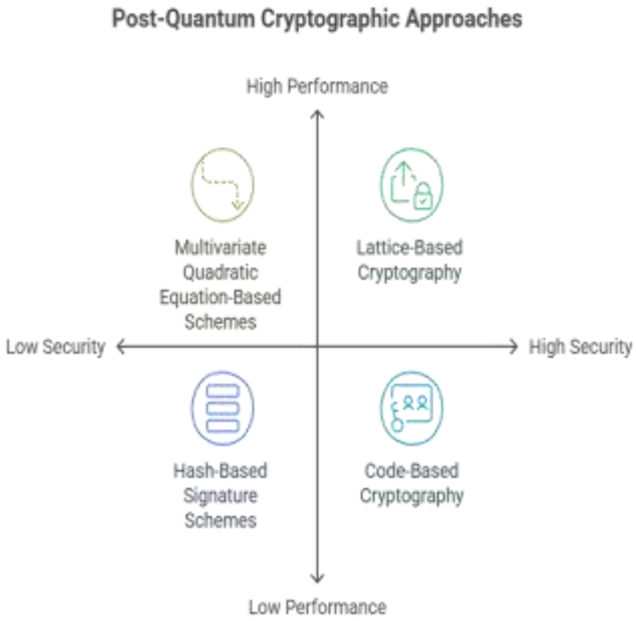

Post-Quantum Cryptographic Approaches
High Performance
Multivariate Quadratic Equation-Based Schemes
Lattice-Based Cryptography
Low Security
High Security
Hash-Based Signature Schemes
Code-Based Cryptography
Low Performance

Figure 1. *Post-Quantum Cryptographic Approaches: A Comparative Overview [3, 4]*

2.3 Historical Development Timeline

The area of quantum-resistant cryptography arose immediately once we found quantum algorithms that threatened classical cryptographic security. Since Peter Shor's pioneering research in 1994, for example, scientists have been seeking other types of problems that quantum computers are not able to solve efficiently. Early proposals remained largely theoretical, but over the past two decades, the field has matured significantly with practical algorithm candidates undergoing rigorous security evaluation and performance testing across diverse implementation environments. The initial academic exploration phase focused primarily on establishing theoretical security guarantees, followed by a subsequent engineering phase addressing practical implementation challenges related to computational efficiency, key size management, and integration with existing security infrastructure.

NIST (National Institute of Standards and Technology) has assumed a central role in this evolutionary process by initiating the Post-Quantum Cryptography Standardization project in 2016. This comprehensive initiative began with 69 candidate algorithms submitted for evaluation, progressing through multiple rounds of intense cryptanalytic scrutiny, performance benchmarking, and implementation testing across hardware and software platforms [4]. The selection process emphasizes security effectiveness against both known and anticipated attack vectors, computational efficiency across implementation environments, and implementation feasibility for diverse applications from embedded systems to high-performance cloud infrastructure. Their goal continues to define broadly used post-quantum cryptography standards that can be applied ahead of large-scale quantum computers becoming a reality, with initial standards for key encapsulation mechanisms and digital signatures already released in 2023, and more algorithms awaiting standardization.

2.4 Technical Implementation Considerations

Implementing quantum-resistant protocols demands careful calibration between security requirements and performance characteristics across diverse operational environments. Lattice-based cryptographic schemes exemplify this challenge. Selecting parameters requires navigating complex tradeoffs between mathematical security margins, computational overhead, memory requirements, and communication bandwidth. Too conservative, and performance suffers unnecessarily; too aggressive, and subtle vulnerabilities might emerge under specialized attacks.

Parameter selection grows further complicated when considering the full spectrum of potential threats. Beyond theoretical attack complexities, practical implementation must account for side-channel vulnerabilities, fault injection techniques, and hybrid classical-quantum attack methodologies that could combine computing paradigms to reduce overall attack complexity. For instance, certain lattice parameters might resist pure quantum approaches but remain vulnerable to combined attacks leveraging classical preprocessing followed by targeted quantum operations.

Real-world integration presents even thornier challenges. Existing cloud infrastructure contains deeply embedded cryptographic dependencies across multiple architectural layers. From hardware security modules storing root keys to authentication frameworks handling identity verification, from certificate authorities managing trust chains to application interfaces consuming cryptographic services—each component requires careful modification. Legacy systems often present particularly vexing obstacles, with hardcoded cryptographic implementations and limited upgrade pathways.

Backwards compatibility demands clever engineering solutions. Hybrid implementation approaches have emerged as a practical transitional strategy, combining classical and quantum-resistant algorithms to provide dual security assurance. These hybrid schemes generally concatenate the outputs from both algorithms, so attackers have to break both to break the system. While this technique adds overhead in both computation and bandwidth, it provides a practical migration path that is compatible with existing systems but adds quantum resistance.

2.5 Practical Implementation Examples

Major cloud service providers have started developing quantum-resistant implementations. They provide important lessons for wider adoption. These early deployments strategically focus on protecting high-value assets facing "harvest now, decrypt later" threats—where encrypted data today could be stored until quantum computers become powerful enough to break the encryption.

The leading tech company’s experimental deployment of lattice-based key exchange within Transport Layer Security infrastructure demonstrated encouraging results. Their engineering team integrated the "New Hope" lattice-based key exchange alongside traditional elliptic curve mechanisms, creating a hybrid handshake resistant to both classical and quantum attacks. Performance monitoring revealed modest computational overhead—roughly 20% additional CPU utilization—while network bandwidth increased by approximately 3 kilobytes per connection. Latency impacts registered below typical human perception thresholds for most applications. Perhaps most significantly, this implementation proved backward-compatible with existing TLS infrastructure, requiring minimal changes to surrounding systems [3].

Microsoft's Azure Quantum program takes a multi-pronged approach, exploring both quantum-resistant algorithms and quantum key distribution technologies. Their platform allows enterprise customers to experiment with post-quantum cryptography in controlled environments before production deployment. Microsoft Research also developed specialized performance optimization techniques for lattice-based systems, creating assembly-level implementations that dramatically reduce computational overhead on modern processors. These optimizations leverage advanced vector instruction sets to parallelize cryptographic operations, achieving performance improvements of up to 270% compared to standard implementations.

AWS has integrated selected post-quantum algorithms into key management services, offering optional cryptographic layers for sensitive workloads. Their approach emphasizes cryptographic agility—developing a flexible infrastructure that can rapidly adopt new algorithms as standards evolve. This architectural approach separates cryptographic policy from implementation details, allowing seamless algorithm transitions without application modifications. AWS also created specialized hardware acceleration modules for selected lattice-based operations, demonstrating how custom silicon can mitigate performance concerns in high-throughput environments.

These industry implementations reveal practical considerations beyond theoretical cryptography. Integration testing exposed unexpected compatibility issues with load balancers, intrusion detection systems, and network monitoring tools. Certificate lifecycle management requires enhancements to handle larger key sizes and different validation procedures. Key generation ceremonies needed modification to accommodate post-quantum requirements. Performance optimization requires you to understand memory access patterns, instruction pipelining, and cache utilization. As reflected in these deployments, the insights gained during this transition can provide extremely valuable guidance for organizations crafting quantum-secure roadmaps, both from a technical solutions and an organizational perspective.

3. Broader Implications and Future Outlook

3.1 Environmental, Economic, and Social Impacts

Adopting quantum-resistant cryptography carries significant environmental considerations. Post-quantum algorithms demand increased computational resources due to complex operations and larger key sizes. Research indicates transitional energy requirements could rise between 7-19% depending on algorithm choice and implementation efficiency. Hash-based signatures show modest increases, while multivariate systems demand substantially more resources. Without optimization, this shift might increase data center energy consumption by several terawatt-hours annually, though representing a small fraction of total usage [5].

These environmental factors must be weighed against the potential catastrophic consequences of quantum-enabled security breaches. Economic implications extend beyond immediate financial losses to systemic risks across multiple sectors. World Economic Forum analysis suggests inadequate protection could expose significant portions of global GDP to cryptographic vulnerabilities by 2035, with financial services, healthcare, and government facing acute exposure. Early adoption offers competitive advantages through enhanced security, intellectual property protection, and reduced future remediation costs. Forward-thinking organizations gain strategic market positioning, particularly in regulated industries where security drives procurement decisions [6].

Societal implications span both domestic and international dimensions. Quantum security impacts power relations between nations. Countries that develop quantum technology early, without a matching global effort in quantum-resistant cryptography, could gain advantages in intelligence and cybersecurity. This situation has increased national investments in major economies, including the European Quantum Flagship, China's National Quantum Initiative, and similar U.S. programs. Equity concerns emerge regarding technology accessibility across nations with varying resources, potentially widening digital divides without international cooperation facilitating technology transfer. Protection of privacy, essential services, and democratic processes depends on widespread quantum-resistant security implementation [5].

***Table 2.** Sector-Based Vulnerability Assessment to Quantum Computing Threats [5, 6]*

Sector	Vulnerability Level	Data Longevity Requirements	Potential Economic Impact
Financial Services	High	Medium	Severe
Healthcare	High	Long	Severe
Government	Very High	Very Long	Critical
Energy/Utilities	High	Medium	Severe
Telecommunications	Medium-High	Medium	Significant
Retail	Medium	Short	Moderate

3.2 Strategic Implementation Timeline

Transitioning to quantum-resistant protocols requires decades of coordinated effort across research, standardization, and implementation. Global Risk Institute's analysis suggests approximately 50% probability that quantum computers capable of breaking 2048-bit RSA will emerge between 2030-2035, increasing to 80% by 2040 [6]. This timeline drives implementation planning, particularly for critical infrastructure and systems handling sensitive data.

Implementation follows distinct phases: inventory assessment (8-16 months), planning and preparation (12-24 months), transitional implementation with hybrid approaches (2-4 years), and migration completion (1-3 additional years). Each phase presents unique challenges depending on organizational complexity and technology environments [5].

Collaborative efforts between academia, industry, and government are crucial. NIST's standardization process is a key effort, with 82 initial submissions from 25 countries going through rigorous evaluation. Industry consortia have emerged across sectors, developing implementation guidance for specific domains. Government initiatives like DHS's Post-Quantum Cryptography Roadmap and European cybersecurity recommendations provide frameworks informing both public and private planning [6].

3.3 Strategic Recommendations

Five core strategic elements have emerged as essential for successful quantum security transitions:

- Cryptographic agility provides a foundation for algorithm transitions. Microsoft Research indicates organizations with high cryptographic agility reduced transition costs by 30-45% compared to rigid implementations [5]. Successful implementation requires clear abstraction layers between cryptographic functions and business logic, flexible configuration management, and certificate systems supporting multiple algorithm types simultaneously.
- Standards participation accelerates robust, interoperable solutions development. Cloud Security Alliance documented organizations actively participating in standards development achieve compliance 40% faster than those adopting standards after finalization [6]. Participation options include technical committee membership, public comment contributions, implementation testing, and sharing non-sensitive experiences through industry consortia.
- Education programs establish crucial awareness foundations. Organizations with structured quantum security education achieved 55% higher executive sponsorship and 70% higher implementation funding compared to organizations without such programs [5]. Effective education addresses different stakeholder groups with tailored content explaining threats in contextually relevant terms.
- Legacy system migration pathways address challenges of systems with limited upgrade capabilities. Industrial Internet Consortium identifies four primary migration patterns: system replacement, cryptographic module replacement, cryptographic proxy implementation, and compensating control implementation [6]. Risk-based timelines must balance security requirements against operational constraints.
- Procurement requirement integration ensures new systems support transition objectives. Implementing specific contractual language requiring vendors to document cryptographic implementations, demonstrate agility capabilities, and commit to migration timelines prevents expanding legacy vulnerabilities [5].

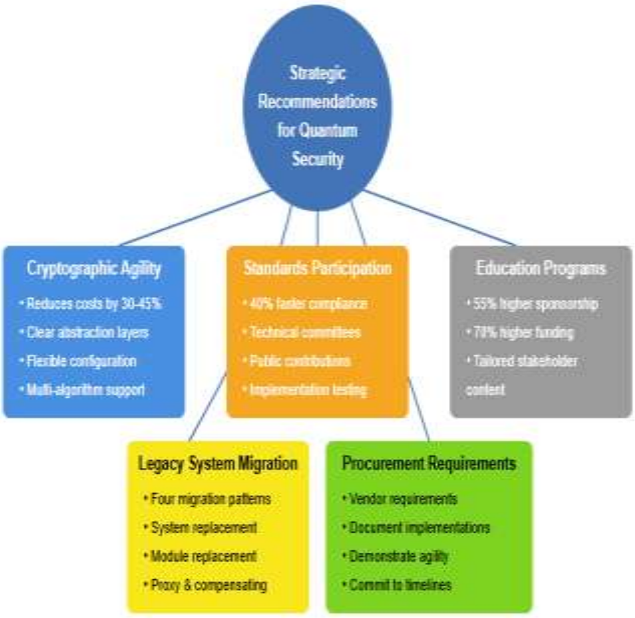


Figure 2. *Five Core Strategic Elements for Quantum Security Transition [5, 6]*

Conclusion

The emergence of quantum computing represents both a revolutionary technological advancement and a fundamental challenge to the security foundations that protect modern cloud infrastructure. Quantum-resistant cryptography has evolved from theoretical concepts to practical implementations as the reality of quantum computing capabilities draws closer. The transition to quantum-resistant security protocols for cloud infrastructure requires a multifaceted approach encompassing technical, organizational, and strategic considerations across the global technology ecosystem. This transition extends beyond simply replacing algorithms to fundamentally reimagining cryptographic architectures with agility as a core design principle. Successful implementation strategies must balance immediate security requirements with long-term sustainability, ensuring that infrastructure remains resistant to both classical and quantum threats throughout extended transition periods. The collaborative efforts among standards bodies, technology providers, researchers, and policy makers have established frameworks for this transition, though significant work remains to achieve widespread implementation. Organizations that proactively develop quantum-resistant security strategies will not only protect their sensitive data from future threats but also gain competitive advantages through enhanced security postures and operational resilience. As quantum computing advances from research laboratories toward practical applications, quantum-resistant security protocols will transition from forward-looking preparations to essential components of baseline security requirements. The protection of cloud infrastructure from quantum threats ultimately requires commitment to continuous evolution of security practices, embracing both the challenges and opportunities presented by this technological transformation. The security of our digital future depends on the decisions and investments made today to prepare cloud infrastructure for the quantum computing era.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Gartner, (2022). Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023. https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023

[2] Peter W. Shor, Algorithms for Quantum Computation: Discrete Log and Factoring. https://users.cs.duke.edu/~reif/courses/randlectures/Quantum.papers/shor.factoring.pdf

[3] Matt Braithwaite, (2016). Experimenting with Post-Quantum Cryptography, *Google Security Blog*. https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html

[4] National Institute of Standards and Technology, Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[5] William Barker et al., (2021). Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, *National Institute of Standards and Technology*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

[6] Babatunde Ojetunde et al., (2025). A Practical Implementation of Post-Quantum Cryptography for Secure Wireless Communication, *Network*. https://www.mdpi.com/2673-8732/5/2/20