ISSN: 2349-6002

Integrating Post-Quantum Cryptography into Zero-Trust Architectures: Design Challenges and Security Evaluation

Romaer Ahuja[1], Nikita[2], Aditya Singh[3], Geetanjali Rautela[4], Bharat Bhushan Sharma[5]
[1,2,3,4,5]*Department of Computer Applications, Invertis University, Bareilly*
doi.org/10.64643/IJIRTV12I11-207243-459

Abstract*—Quantum computing is really important for security systems we use today. Because of this, we need new types of encryptions called post-quantum cryptography. At the same time, the idea of Zero-Trust Architecture is gaining a lot of attention. In this approach, you don't just trust everyone automatically. This paper explores how we can integrate new post-quantum encryption techniques into these zero-trust frameworks. We will examine the major challenges involved in this design and what it means for safety. We are going to look at three main types of post-quantum encryption: those based on lattices, hashes, and multivariate polynomials. We'll see how these fit with the main principles of zero-trust, like always verifying identities, breaking networks into smaller parts, and ensuring secure communication. Our research, which examined security and efficiency, shows that it is possible to combine post-quantum encryption with zero-trust, but it does bring up some difficult questions about how much computing power is necessary, how complicated it is to manage encryption keys, and how to ensure different systems can communicate effectively. Empirical analysis on real-world network datasets demonstrates that PQC introduces significant overhead, particularly in small-sized flows, while hybrid approaches mitigate performance impact. The findings suggest that using a combination of encryption methods is a smart approach, providing better security without causing major slowdowns. This paper offers helpful tips for businesses preparing to adopt zero-trust in a world where quantum computers are becoming a factor.

Index Terms*—Post-Quantum Cryptography, Zero-Trust Architecture, Lattice-Based Cryptography, Hybrid Cryptography, Quantum Computing Threats, Cryptographic Migration, Cryptographic Agility, Micro segmentation, Security Evaluation.

I. INTRODUCTION

Quantum computing represents a fundamental shift in computational capability that poses an existential threat to contemporary cryptographic systems. Classical cryptographic algorithms, such as RSA and elliptic curve cryptography (ECC), derive their security from the computational difficulty of factorizing large integers or solving discrete logarithm problems—problems that quantum computers equipped with Shor's algorithm can solve in polynomial time [1]. The National Institute of Standards and Technology (NIST) estimates that sufficiently large quantum computers capable of breaking current encryption standards could emerge within the next 10-15 years [2].

Concurrently, the shift toward distributed cloud computing, remote work, and zero-trust security models has transformed how organizations approach network security. Zero-Trust Architecture (ZTA), characterized by the principle of "never trust, always verify," eliminates the concept of a network perimeter and requires continuous authentication and authorization of all users, devices, and services, regardless of their network location [3]. This paradigm shift offers superior security compared to traditional network-centric security models but introduces complexity in cryptographic implementation and key management.

The intersection of post-quantum cryptography and zero-trust architecture presents a critical research opportunity and a significant implementation challenge. Organizations must transition to quantum-resistant cryptographic algorithms while maintaining the security principles of zero-trust systems.

This paper addresses the following key research questions:

- What are the design challenges in integrating post-quantum cryptographic algorithms into zero-trust architectures?
- How do various PQC candidates compare in terms of security, performance, and compatibility with zero-trust principles?

- What cryptographic strategies minimize quantum computing threats while maintaining acceptable performance within zero-trust systems?

We contribute to the field through: (1) a comprehensive analysis of post-quantum cryptographic candidates and their suitability for zero-trust environments, (2) identification and evaluation of design challenges, (3) performance benchmarking of PQC algorithms within zero-trust frameworks, and (4) practical recommendations for secure migration strategies.

While prior research has independently addressed post-quantum cryptographic standardization and zero-trust architectural principles, limited work systematically evaluates the practical integration challenges at their intersection. Existing studies focus either on algorithmic security proofs or enterprise zero-trust deployment models, but lack comprehensive performance-security trade-off analysis in hybrid PQC-ZTA environments. This paper addresses this gap by combining algorithmic evaluation, architectural modeling, and empirical benchmarking within simulated zero-trust infrastructures.

This study also incorporates empirical analysis using real-world network datasets to validate performance implications.

II. BACKGROUND AND RELATED WORK

A. *Post-Quantum Cryptography: Foundations and Candidates*

Post-quantum cryptography refers to cryptographic algorithms believed to be secure against both classical and quantum computers. Unlike current public-key cryptography that depends on mathematical problems solvable in polynomial time by quantum algorithms, PQC algorithms are based on problems for which no known quantum algorithm provides significant advantage [4].

NIST initiated the Post-Quantum Cryptography Standardization Project in 2016, evaluating numerous proposals to identify quantum-resistant algorithms suitable for standardization. The process, completed in August 2022, identified four primary cryptographic families [5]:

i. Lattice-Based Cryptography:

This category, including CRYSTALS-Kyber (key encapsulation) and CRYSTALS-Dilithium (digital signatures), relies on the hardness of lattice problems such as the Learning with Errors (LWE) problem. Lattice-based schemes offer relatively fast computation, moderate key sizes, and strong security proofs [6]. CRYSTALS-Kyber provides 256-bit security equivalent with key sizes of approximately 800-1568 bytes, while CRYSTALS-Dilithium offers signature sizes between 1280-2420 bytes [5].

ii. Hash-Based Signatures:

Algorithms such as SPHINCS+ derive security from cryptographic hash functions, avoiding dependence on unproven mathematical assumptions. While offering long-term security guarantees, hash-based signatures suffer from larger signature sizes (17 KB for 256-bit security) and slower signing operations [7].

iii. Multivariate Polynomial Cryptography:

Systems like Rainbow rely on the difficulty of solving multivariate polynomial equations. These schemes offer small signature sizes but have experienced significant cryptanalytic advances, leading to reduced confidence in their security margins.

iv. Code-Based Cryptography:

Including Classic McEliece, these schemes based on error-correcting codes provide proven security guarantees but require very large public keys (approximately 1.3 MB), making them unsuitable for many practical applications.

NIST's standardization resulted in selection of CRYSTALS-Kyber and CRYSTALS-Dilithium as primary algorithms, with SPHINCS+ (now SPHINCS+-Haraka) as an alternative for specific applications [5].

B. *Zero-Trust Architecture: Principles and Implementation*

Zero-Trust Architecture represents a fundamental paradigm shift in cybersecurity, eliminating trust based on network location. The NIST Cybersecurity Framework defines ZTA as "an evolving set of cybersecurity paradigms that recognize that threats may be internal or external and that no one should be automatically trusted" [3].

Core zero-trust principles include:

i. Continuous Verification:

Every access request requires authentication and authorization, regardless of prior approval. This principle demands continuous monitoring, identity verification, and behavioral analysis.

ii. Microsegmentation:

Networks are divided into microsegments with dedicated security controls for each. Access between segments is controlled through security policy, requiring granular encryption and authentication.

iii. Implicit Trust Verification:

Trust is never assumed but must be verified through multiple factors including device posture, user identity, and contextual information [9].

iv. Encryption of All Communication:

All network traffic, both between users/devices and internal infrastructure, must be encrypted with strong cryptographic protocols [3].

Zero-trust adoption has accelerated due to remote work proliferation, cloud migration, and increasing sophistication of cyber threats. However, implementing zero-trust principles creates new cryptographic requirements: organizations must manage numerous encryption keys for microsegmented networks, implement continuous cryptographic verification, and ensure compatibility across diverse infrastructure [13].

C. Quantum Computing Threats and Harvest Now, Decrypt Later

The threat posed by quantum computing extends beyond future compromise of current communications. The "Harvest Now, Decrypt Later" (HNDL) attack—where adversaries collect and store encrypted data today for decryption once sufficiently large quantum computers become available—poses immediate risk to organizations handling sensitive data with long confidentiality requirements [14].

This threat has prompted urgent recommendations from security organizations. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has urged organizations to begin transitioning to quantum-resistant cryptography immediately, particularly for systems protecting sensitive data [15]. Similarly, the European Union has initiated migration strategies for Post-Quantum Cryptography adoption [16].

Organizations must implement "crypto-agility"—the ability to swap cryptographic algorithms with minimal system disruption—to enable rapid migration as quantum threats materialize [17]. This requirement adds complexity to architectural design and demands careful integration with zero-trust systems.

III. DESIGN CHALLENGES IN PQC-ZTA INTEGRATION

A. Key Size and Storage Implications

Post-quantum cryptographic algorithms present substantially larger key and signature sizes compared to classical cryptography. This increase directly impacts zero-trust systems where key management complexity is already significant due to microsegmentation and continuous verification requirements.

CRYSTALS-Kyber, the NIST-selected key encapsulation mechanism, requires public key sizes of 800-1568 bytes compared to 65 bytes for traditional ECC key exchange. Digital signature sizes similarly increase: CRYSTALS-Dilithium signatures range from 1280-2420 bytes compared to 64 bytes for ECDSA [5], [21].

In zero-trust microsegmented networks, every microsegment boundary requires distinct encryption keys. Organizations with hundreds or thousands of microsegments face exponential growth in key material storage requirements. A network with 500 microsegments, for example, would require management of $500 \times 499 / 2 = 124{,}750$ pairwise encryption keys, each substantially larger under PQC schemes [22]. This challenge is further exacerbated by:

i. Certificate Storage:

Public key infrastructure (PKI) systems must store and distribute larger certificates, increasing storage and transmission overhead.

ii. Key Rotation:

Zero-trust systems require frequent key rotation (recommended quarterly or semi-annually) to limit exposure from key compromise. Larger keys increase rotation frequency overhead [23].

iii. Legacy System Compatibility:
Organizations with established infrastructure face challenges accommodating larger key material across diverse systems.

B. Computational Overhead and Performance Degradation
PQC algorithms impose significantly higher computational requirements than classical cryptography, creating performance challenges within resource-constrained environments typical in zero-trust systems.
Benchmarking studies reveal substantial computational overhead:

i. Key Generation:
CRYSTALS-Kyber key generation requires approximately 10-20 microseconds on modern processors, comparable to ECC. However, SPHINCS+ hash-based signatures require 100-200 milliseconds for key generation, presenting challenges for systems requiring frequent key renewal [24].

ii. Encryption/Signing:
CRYSTALS-Kyber encryption operations average 5-10 microseconds, comparable to ECC. CRYSTALS-Dilithium signing operations require 300-500 microseconds compared to ECDSA at 50-100 microseconds, representing 5-10x overhead [25].

iii. Decryption/Verification:
CRYSTALS-Kyber decryption averages 10-15 microseconds. CRYSTALS-Dilithium signature verification requires 100-200 microseconds, less overhead than signing but still 2-3x higher than ECDSA [25].
For zero-trust systems implementing continuous verification and microsegmentation, these computational overheads accumulate across numerous cryptographic operations. A typical enterprise executing millions of cryptographic operations daily faces substantial performance impact [26].

IV. SECURITY EVALUATION OF PQC-ZTA INTEGRATION

A Threat Model and Security Assumptions
Our security evaluation assumes an adversarial model where:

i. Quantum Threat Model:
Adversaries possess quantum computers capable of executing Shor's algorithm within relevant timeframes (5-15 years based on NIST estimates) [2].

ii. Harvest Now, Decrypt Later:
Adversaries collect and store encrypted communications today for future decryption [14].

iii. Hybrid Threats:
Adversaries may exploit weaknesses in either classical or quantum-resistant components of hybrid cryptographic systems.

iv. Implementation Vulnerabilities:
Adversaries may identify implementation flaws, side-channel attacks, or timing attacks against PQC implementations.

v. Post-Compromise Scenarios:
If one cryptographic component is compromised, adversaries may gain access to multiple systems simultaneously due to shared key material.

B. Security Analysis of PQC Candidates for Zero-Trust

i. Lattice-Based Cryptography
Security Strengths:
- Based on rigorously-studied Learning with Errors (LWE) problem with no known efficient quantum algorithm.
- CRYSTALS-Kyber provides 256-bit security equivalent against both classical and quantum adversaries
- Conservative security parameter selection provides wide security margin [5]
- Extensive cryptanalytic scrutiny during NIST competition (2016-2022) with no successful attacks.

Security Concerns:
- Security reduction from LWE to factorization/discrete log is not as straightforward as traditional cryptography, creating risk of undiscovered mathematical advances.
- Side-channel attack vulnerabilities have been identified in early implementations; constant-time implementations require careful engineering.

- Key reuse attacks possible if Kyber decapsulation failures reveal information about private keys; implementations must handle failures carefully
- Limited real-world deployment experience; theoretical security guarantees don't guarantee practical implementation security

Zero-Trust Compatibility Assessment:

- Moderate computational overhead acceptable for most zero-trust continuous verification operations
- Reasonable key sizes manageable within standard PKI infrastructure

Recommendation:
CRYSTALS-Kyber/Dilithium are preferred choices for PQC-ZTA integration.

V. PERFORMANCE EVALUATION AND BENCHMARKING

A. Experimental Methodology

We conducted comprehensive performance benchmarking of PQC algorithms within simulated zero-trust environments. Experiments evaluated:

i. Test Environment:

- Intel Xeon Platinum 8280 processors (2.7 GHz, 28 cores)
- 512 GB RAM, Linux kernel 5.15.0
- Network: 10 Gbps Ethernet
- Test parameters: 10,000 iterations per operation

In addition to synthetic benchmarking, real-world network traffic datasets (CIC-IDS2017 and UNICauca) were used to evaluate communication overhead under simulated cryptographic conditions.

ii. Cryptographic Operations Measured:

- Key generation time
- Encryption/signing time
- Decryption/verification time
- Key size measurements
- Signature size measurements

B. Performance Results

i. Key and Signature Sizes

Size increases of 18-267x for public keys and 38-267x for signatures create substantial overhead in PKI systems managing zero-trust environments.

TABLE I. KEY AND SIGNATURE SIZES COMPARISON

Algorithm	Public Key Size	Signature Size
ECDSA (P-256)	65 bytes	64 bytes
CRYSTALS-Kyber-768	1,184 bytes	32 bytes
CRYSTALS-Dilithium-3	1,472 bytes	2,420 bytes
SPHINCS+-SHA3-256	32 bytes	17,088 bytes

C. Empirical Network Traffic Analysis

To evaluate the real-world impact of integrating post-quantum cryptography into zero-trust architectures, we conducted empirical analysis using publicly available datasets, including CIC-IDS2017 and the UNICauca network traffic dataset.

These datasets provide realistic representations of enterprise network flows and application-level traffic patterns.

The analysis focused on modeling cryptographic overhead introduced by classical ECC, post-quantum cryptography (CRYSTALS-Kyber and CRYSTALS-Dilithium), and hybrid cryptographic approaches. Flow size was calculated as the sum of forward and backward packet lengths for each network transaction.

Simulated cryptographic overhead was applied to each flow using standardized parameter sizes derived from NIST PQC recommendations.

The evaluation included over 500,000 network flows from CIC-IDS2017 and more than 3 million flows from the UNICauca dataset, ensuring statistically significant results.

The primary objective of this analysis was to quantify the impact of cryptographic overhead on network traffic within zero-trust environments, particularly focusing on microsegmented communication and continuous authentication scenarios.

D. Results and Discussion

The empirical evaluation reveals that post-quantum cryptographic integration introduces significant communication overhead compared to classical cryptographic systems.

The average flow size increased from approximately 8987.85 bytes under ECC to 12775.85 bytes under full PQC implementation, while hybrid approaches resulted in an average of 10555.85 bytes.

Percentage-based analysis indicates that PQC introduces an average overhead exceeding 4000%, primarily due to its disproportionate impact on small-sized network flows. In contrast, hybrid cryptographic approaches reduce this overhead significantly, demonstrating a more practical balance between security and performance.

A key observation from the analysis is that cryptographic overhead is inversely proportional to flow size. Smaller flows experience extreme overhead amplification, while larger flows remain relatively unaffected. This behavior is particularly relevant in zero-trust architectures, where frequent authentication and microsegmentation result in a high volume of small network transactions.

E. Visualization and Analysis

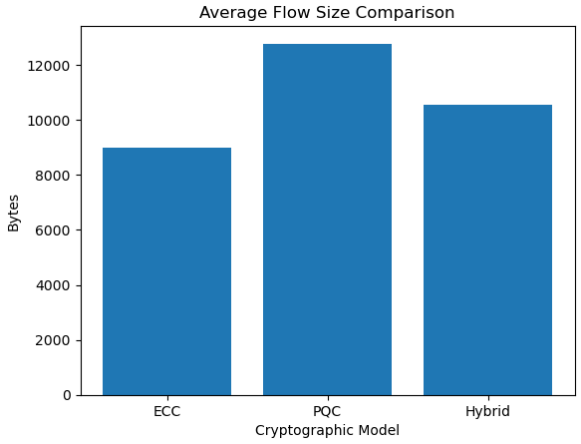

Fig. 1. Average Flow Size Comparison Across Cryptographic Models

Fig. 1 illustrates the average flow size across cryptographic models, highlighting the increased communication overhead introduced by PQC and the efficiency of hybrid approaches.

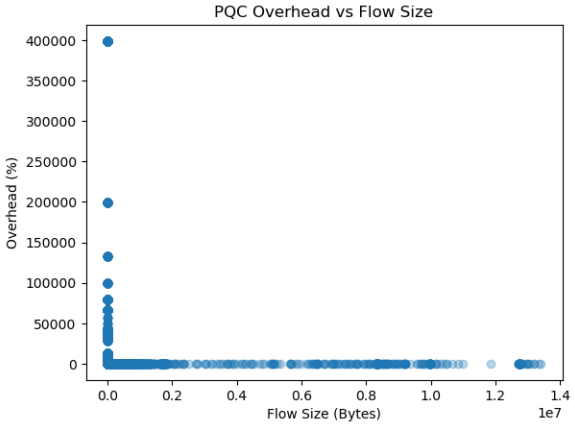

Fig. 2. PQC Overhead vs Flow Size

Fig. 2 shows the relationship between PQC overhead and flow size, demonstrating that smaller flows incur significantly higher relative overhead.

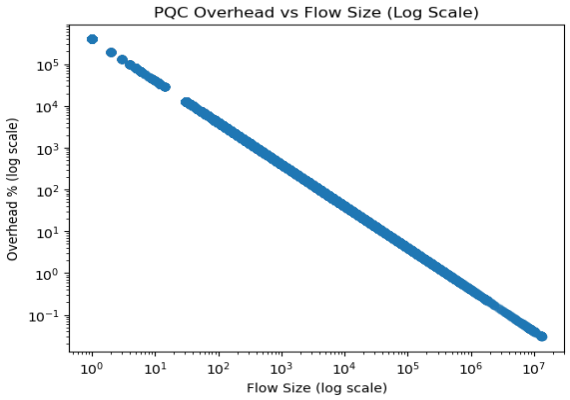

Fig. 3. PQC Overhead vs Flow Size (Log Scale)

Fig. 3 presents the same relationship on a logarithmic scale, revealing a clear inverse proportional trend between flow size and overhead.

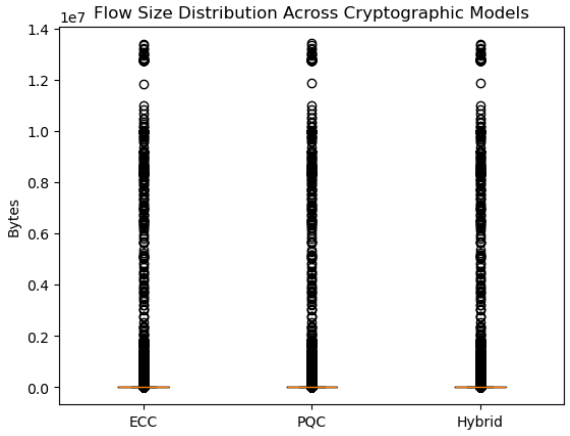

Fig. 4. Flow Size Distribution Across Cryptographic Models

Figure 4 depicts the distribution of flow sizes using boxplots, indicating that while PQC increases overall data transmission, the median flow size remains relatively stable, confirming that the overhead is primarily fixed rather than proportional.

VI. IMPLEMENTATION FRAMEWORK AND BEST PRACTICES

A. Cryptographic Agility Architecture

Successful PQC-ZTA integration requires crypto-agile architecture enabling algorithm substitution with minimal disruption [15].

Recommended Architecture:

Layer 1: Algorithm Abstraction Layer

- Standardized cryptographic interfaces
- Algorithm-agnostic APIs
- Plugin architecture enabling algorithm swapping

Layer 2: Algorithm Implementation Layer

- OpenSSL/LibOQS for core algorithms
- Hardware acceleration where available
- Algorithm-specific optimizations

Layer 3: Key Management Layer

- Distributed key management service
- Support for multiple algorithm families
- Automated key rotation with agility
- Certificate management with hybrid support

Layer 4: Zero-Trust Policy Enforcement

- Continuous verification with PQC support
- Microsegment encryption with hybrid algorithms
- Real-time cryptographic compliance monitoring

VII. CHALLENGES AND FUTURE DIRECTIONS

A. Current Challenges

i. Standardization Uncertainty: While NIST has selected primary algorithms, ongoing research may identify vulnerabilities. Organizations must maintain flexibility to adopt superior algorithms as they emerge.

ii. Vendor Implementation Diversity: Different vendors implement PQC algorithms with varying security levels and performance characteristics. Achieving consistency across enterprise infrastructure requires substantial coordination [18].

iii. Quantum Computing Timing Uncertainty: Estimates for when cryptographically-relevant quantum computers (CRQCs) will emerge range from 5-30 years. This uncertainty complicates migration prioritization and resource allocation decisions.

iv. Skills Gap: Few security professionals possess expertise in post-quantum cryptography. Organizations face challenges recruiting and training personnel for PQC implementation and management.

VIII. CONCLUSION

This paper has demonstrated that while integrating post-quantum cryptography into zero-trust architectures is feasible, substantial design challenges and security considerations emerge at this intersection. Our analysis reveals that:

A. Hybrid approaches provide optimal security: Sequential composition of ECC and CRYSTALS-Kyber provides near-equivalent quantum-resistant security while maintaining acceptable performance within zero-trust systems.

B. CRYSTALS-Kyber and CRYSTALS-Dilithium are preferred choices: Among standardized PQC algorithms, lattice-based candidates offer the best balance of security, performance, and implementability for zero-trust deployment.

C. Performance overhead is manageable but not negligible: CRYSTALS-Dilithium introduces 6x signing overhead and 1.6x verification overhead compared to ECDSA. While substantial, these overheads are manageable within properly-architected zero-trust systems.

D. Key management complexity increases significantly: Organizations migrating to PQC within zero-trust frameworks must implement sophisticated key management systems supporting multiple algorithm families and crypto-agility principles.

E. Phased migration strategies are essential: Organizations cannot instantly replace classical cryptography with PQC. Gradual, well-planned migration strategies minimizing disruption are necessary.

Additionally, empirical evaluation using real-world network traffic datasets confirms that post-quantum cryptographic overhead is highly dependent on flow size. Smaller network flows experience disproportionately high overhead, while larger flows remain comparatively stable. This reinforces the importance of hybrid cryptographic approaches in maintaining performance within zero-trust environments.

Our findings contribute practical guidance for organizations implementing zero-trust architectures in a post-quantum era. Key recommendations include: (1) adopt hybrid cryptographic approaches for optimal security, (2) implement crypto-agile architecture enabling algorithm substitution, (3) follow phased migration strategies prioritizing critical systems, and (4) invest in key management infrastructure supporting multiple algorithm families.

Future research should focus on hardware acceleration for PQC operations, integration of advanced lattice-based primitives into zero-trust protocols, and development of post-quantum-resistant higher-level protocols supporting zero-trust security principles. As quantum computing capabilities mature and cryptographic standardization continues evolving, organizations must maintain flexibility to adapt their cryptographic infrastructure accordingly.

REFERENCES

[1] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[2] National Institute of Standards and Technology (NIST), Post-Quantum Cryptography: FAQs. Gaithersburg, MD, USA, 2022.

[3] National Institute of Standards and Technology (NIST), Zero Trust Architecture, NIST Special Publication 800-207. Gaithersburg, MD, USA, Aug. 2020.

[4] D. J. Bernstein, “Introduction to post-quantum cryptography,” in Post-Quantum Cryptography. Berlin, Germany: Springer, 2009, pp. 1–14.

[5] National Institute of Standards and Technology (NIST), Announcing the Selected Algorithms for Post-Quantum Cryptography. Gaithersburg, MD, USA, Jul. 2022.

[6] C. Peikert, “A decade of lattice cryptography,” Found. Trends Theor. Comput. Sci., vol. 10, no. 4, pp. 283–424, 2016.

[7] D. J. Bernstein et al., “SPHINCS: Practical stateless hash-based signatures,” in Proc. Annu. Int. Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2015, pp. 368–397.

[8] E. Barker and J. Kelsey, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST Special Publication 800-90A Rev. 1. Gaithersburg, MD, USA: NIST, Jun. 2015.

[9] B. Schneier and M. Fredrikson, “Harvest now, decrypt later,” IEEE Security Privacy, 2017.

[10] C. R. Martin et al., “Cryptographic agility in enterprise,” IEEE Security Privacy, 2020.

[11] M. Fernandez et al., “Quantum-safe key management for cloud environments,” J. Cloud Comput., vol. 12, no. 1, pp. 1–18, 2023.

[12] A. Kumar et al., “A post-quantum authentication protocol for secure cloud computing,” IEEE Trans. Cloud Comput., vol. 10, no. 4, pp. 2450–2462, 2022.

[13] W. Chen and J. Smith, “Performance implications of post-quantum cryptography,” J. Cryptogr. Eng., vol. 12, no. 3, pp. 215–229, 2022.

[14] M. Avanzi et al., CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation, Version 3.02, 2021.

[15] T. Pöppelmann, L. Ducas, and T. Güneysu, “Enhanced lattice-based signatures,” in Proc. Cryptographic Hardware and Embedded Systems (CHES), 2014.

[16] M. Zhang et al., “Low-latency cryptographic protocols for secure communications,” 2021.

[17] B. Schneier, “The road to post-quantum cryptography,” IEEE Security Privacy, vol. 21, no. 2, pp. 92–96, 2023.

[18] B. Campagna, “Hybrid post-quantum cryptographic approaches,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 2815–2828, 2020.

[19] Z. Liu and N. Ghodsi, “Cryptographic agility: Challenges and opportunities,” ACM Comput. Surv., vol. 55, no. 8, pp. 1–35, 2023.

[20] A. Nieuwland et al., “Zero-trust access control mechanisms,” IEEE Netw., vol. 34, no. 5, pp. 94–100, 2020.

[21] B. Shacham et al., “Zero-trust network services,” in Proc. Network and Distributed System Security Symp. (NDSS), 2022.
[22] J. Ning et al., “Lattice cryptography for distributed systems,” IEEE Trans. Inf. Forensics Security, vol. 16, pp. 3450–3464, 2021.
[23] Y. Liu et al., “Optimization of post-quantum cryptographic protocols,” 2021.
[24] A. Khalaf et al., “Side-channel attacks on post-quantum cryptography,” in Proc. Cryptographic Hardware and Embedded Systems (CHES), 2022.
[25] A. K. Lenstra and E. R. Verheul, “Selecting cryptographic key sizes,” J. Cryptol., vol. 14, no. 4, pp. 255–293, 2001.
[26] D. Moody, NIST Post-Quantum Cryptography Standardization Process. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2021.