International Journal of Research and Review Techniques (IJRRT), ISSN: 3006-1075
Volume 5, Issue 1, January-March, 2026, Available online at: https://ijrrt.com

Post-Quantum Cryptography: Preparing Critical Infrastructure for Shor's Algorithm

Peter W. Shor

Morss Professor of Applied Mathematics, Department of Mathematics, Massachusetts Institute of Technology (MIT), USA

ABSTRACT

The advent of quantum computing presents a significant threat to the security of modern cryptographic systems, particularly those underpinning critical infrastructure such as power grids, financial networks, healthcare systems, telecommunications, and industrial control systems. Shor's algorithm, when executed on a sufficiently powerful fault-tolerant quantum computer, has the potential to break widely used public-key cryptographic algorithms, including RSA and Elliptic Curve Cryptography (ECC), thereby compromising data confidentiality, authentication, and secure communication. This paper examines the role of Post-Quantum Cryptography (PQC) in preparing critical infrastructure for the emerging quantum threat. It explores the principles of quantum-resistant cryptographic algorithms, including lattice-based, hash-based, and code-based approaches, and highlights standardized solutions such as ML-KEM, ML-DSA, and SLH-DSA. Furthermore, the study discusses the challenges associated with transitioning legacy systems to quantum-resistant cryptographic mechanisms, including interoperability, computational overhead, resource constraints, and long-term infrastructure compatibility. It also emphasizes the importance of cryptographic inventory management, crypto-agility, hybrid cryptographic deployments, and phased migration strategies to mitigate risks such as "harvest now, decrypt later" attacks. The paper proposes a proactive security framework that integrates risk assessment, algorithm selection, system testing, and continuous monitoring to support a resilient transition toward post-quantum security. By adopting standardized quantum-resistant cryptographic techniques and implementing structured migration strategies, critical infrastructure operators can strengthen their cybersecurity posture and maintain operational resilience in the quantum computing era.

Keywords: Post-Quantum Cryptography, Shor's Algorithm, Quantum Computing, Critical Infrastructure, Quantum-Resistant Cryptography, Cryptographic Migration, Cybersecurity, Crypto-Agility.

INTRODUCTION

The rapid advancement of quantum computing is transforming the landscape of cybersecurity and creating new challenges for the protection of sensitive information and critical infrastructure. Modern digital security relies heavily on cryptographic algorithms to ensure data confidentiality, integrity, authentication, and secure communication. Widely used public-key cryptographic systems, such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC), form the foundation of secure communication across power grids, banking systems, healthcare networks, telecommunications, transportation, and industrial control systems. However, the emergence of large-scale quantum computing threatens the security of these systems, making the development and adoption of quantum-resistant cryptographic solutions an increasingly important research priority.

A major source of this threat is Shor's algorithm, a quantum algorithm capable of efficiently solving the integer factorization and discrete logarithm problems on a sufficiently powerful fault-tolerant quantum computer. These mathematical problems underpin the security of many conventional public-key cryptographic algorithms. If quantum computers achieve the required computational capabilities, adversaries could potentially compromise digital signatures, key exchange mechanisms, authentication protocols, and encrypted communications. Such vulnerabilities could have serious consequences for critical infrastructure, where security failures may disrupt essential services, expose confidential information, and affect public safety and national security.

Another significant concern is the "harvest now, decrypt later" attack, in which adversaries collect encrypted data today with the intention of decrypting it when sufficiently capable quantum computers become available. This threat is particularly relevant to organizations that manage sensitive information requiring long-term confidentiality, including government agencies, healthcare providers, financial institutions, and energy operators. Consequently, preparing for quantum threats requires proactive planning rather than waiting until large-scale quantum computers become practically available.

Post-Quantum Cryptography (PQC) has emerged as a promising approach to addressing these challenges. PQC involves cryptographic algorithms designed to resist attacks from both classical and quantum computers. Unlike

quantum cryptography, which relies on quantum physical phenomena, PQC uses mathematical problems believed to remain computationally difficult even for quantum adversaries. The National Institute of Standards and Technology (NIST) has established important standards for post-quantum key establishment and digital signatures, including the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), the Module-Lattice-Based Digital Signature Algorithm (ML-DSA), and the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA). These standards provide a foundation for integrating quantum-resistant cryptographic mechanisms into existing and future information systems.

Despite these advances, transitioning critical infrastructure to post-quantum security presents several technical and operational challenges. Many infrastructure systems depend on legacy hardware, long equipment lifecycles, resource-constrained devices, and interconnected communication protocols. Replacing existing cryptographic mechanisms may introduce compatibility issues, computational overhead, increased key or signature sizes, and implementation complexity. Furthermore, organizations must identify cryptographic dependencies, assess system vulnerabilities, prioritize high-risk assets, and maintain secure operations throughout the migration process.

In this context, this paper investigates the importance of post-quantum cryptography in preparing critical infrastructure for the potential impact of Shor's algorithm. It examines the quantum threat to conventional cryptographic systems, reviews emerging quantum-resistant algorithms, and discusses the challenges associated with their deployment in critical environments. The paper also highlights the importance of cryptographic agility, hybrid cryptographic approaches, risk-based migration planning, and continuous security assessment. The primary objective is to establish a practical foundation for the gradual adoption of post-quantum cryptographic solutions that strengthen security, preserve interoperability, and ensure the long-term resilience of critical infrastructure in the quantum computing era.

2. Proposed Models and Methodologies

The proposed methodology aims to develop a systematic framework for preparing critical infrastructure against the potential cryptographic threats posed by Shor's algorithm. The framework focuses on identifying vulnerable cryptographic mechanisms, evaluating post-quantum cryptographic (PQC) alternatives, and establishing a secure migration strategy for critical infrastructure environments. The methodology integrates cryptographic risk assessment, quantum-resistant algorithm selection, hybrid cryptographic deployment, crypto-agility, and performance evaluation to ensure security, reliability, and operational continuity.

2.1 Proposed Quantum-Resilient Security Model

The proposed model consists of five interconnected layers designed to support the transition from conventional cryptography to post-quantum security.

Layer 1: Infrastructure and Cryptographic Discovery
Identify RSA, ECC, certificates, key exchanges, and cryptographic dependencies across IT, OT, and industrial control systems.

Layer 2: Quantum Risk Assessment
Evaluate data sensitivity, system criticality, exposure, equipment lifetime, and vulnerability to future quantum attacks.

Layer 3: Post-Quantum Algorithm Selection
Select suitable standardized algorithms, including ML-KEM for key establishment and ML-DSA or SLH-DSA for digital signatures.

Layer 4: Hybrid Deployment and Crypto-Agility
Test compatible classical and post-quantum mechanisms, modular cryptographic interfaces, secure key management, and rollback procedures.

Layer 5: Validation and Continuous Monitoring
Measure security, latency, throughput, memory usage, interoperability, and system availability under realistic operating conditions.

2.2 Cryptographic Discovery and Risk Assessment

The first stage involves creating a comprehensive inventory of cryptographic assets used within critical infrastructure. This includes identifying public-key algorithms, digital certificates, key exchange protocols, cryptographic libraries, hardware security modules, embedded devices, and communication interfaces. Particular attention is given to RSA- and ECC-based mechanisms because their underlying mathematical problems are vulnerable to Shor's algorithm on sufficiently capable quantum computers.

Following asset discovery, a risk assessment model is applied to prioritize systems according to their operational importance, sensitivity of stored information, exposure to external threats, and expected equipment replacement cycles.

Systems that protect long-lived confidential data or control essential services are assigned higher migration priorities. This approach enables organizations to allocate resources effectively and reduce exposure to future quantum-enabled attacks.

2.3 Post-Quantum Cryptographic Algorithm Selection
The second methodological stage evaluates standardized PQC algorithms according to security requirements, computational efficiency, implementation complexity, and compatibility with existing infrastructure.

Algorithm	Primary purpose	Proposed application
ML-KEM (FIPS 203)	Quantum-resistant key establishment	Secure communication sessions and network connections
ML-DSA (FIPS 204)	Digital signatures	Authentication, software updates, and access control
SLH-DSA (FIPS 205)	Hash-based digital signatures	Alternative signature mechanisms for selected high-assurance applications

These algorithms were standardized by the National Institute of Standards and Technology (NIST) in August 2024. Their selection for a particular infrastructure environment should depend on system requirements, implementation testing, and applicable security policies.

2.4 Hybrid Cryptographic Deployment Model
The proposed framework incorporates a hybrid deployment strategy to facilitate gradual migration from conventional cryptography to post-quantum cryptography. During a controlled transition, compatible classical and post-quantum mechanisms may be combined within supported protocols to maintain interoperability while introducing quantum-resistant protection.

For example, a secure communication system may combine a conventional key-establishment mechanism with ML-KEM, provided that the protocol defines a secure combination and the implementation has been appropriately evaluated. Digital signature migration can similarly be tested across certificate infrastructures, software-update systems, and authentication services.

Hybrid deployment should not be treated as automatically secure. The combined construction must be reviewed for downgrade attacks, incorrect key combination, implementation flaws, and protocol incompatibilities. Legacy devices that cannot support PQC may require gateways, firmware upgrades, isolation, or scheduled replacement.

2.5 Crypto-Agility and Migration Strategy
Crypto-agility refers to the ability of a system to replace or update cryptographic algorithms without requiring extensive redesign of the entire infrastructure. The proposed model incorporates modular cryptographic interfaces, configurable algorithm policies, centralized key and certificate management, and version-controlled security configurations.

The migration process follows four stages:
1. Discovery and planning: Inventory cryptographic assets, identify dependencies, and establish migration priorities.
2. Laboratory testing: Evaluate PQC implementations for correctness, security, resource consumption, and interoperability.
3. Pilot deployment: Introduce selected algorithms into limited, non-safety-critical environments before expanding deployment.
4. Production migration and monitoring: Gradually update high-priority systems, verify operational performance, and monitor cryptographic configurations for emerging vulnerabilities.

This phased approach aligns with NIST's guidance to identify vulnerable cryptographic uses and plan their replacement or updating.

2.6 Performance Evaluation Methodology
The effectiveness of the proposed model will be evaluated through controlled experiments and comparative analysis of classical, post-quantum, and hybrid cryptographic configurations. Testing should use representative workloads from

critical infrastructure networks, including secure device communication, authentication, firmware validation, and industrial data exchange.

The following performance indicators are proposed:

- Cryptographic execution time: Time required for key establishment, signing, and signature verification.
- Communication overhead: Additional bytes introduced by public keys, ciphertexts, certificates, and digital signatures.
- Resource consumption: CPU utilization, memory requirements, and energy consumption on constrained devices.
- Interoperability: Successful communication between systems using compatible cryptographic configurations.
- Operational reliability: Service availability, connection failure rate, and recovery behavior during cryptographic migration.
- Security compliance: Correct implementation of selected standards, resistance to known attacks, and adherence to applicable security policies.

The experiments will compare the performance of the different configurations under identical conditions. Results can be analyzed using average execution time, percentage overhead, throughput, and resource utilization. No performance or security improvement will be claimed until supported by experimental results.

2.7 Proposed Validation and Expected Outcomes

The final stage validates the proposed model against the security and operational requirements of critical infrastructure. Validation will examine whether the framework can identify vulnerable cryptographic assets, prioritize high-risk systems, support interoperable PQC deployment, and maintain acceptable service performance during migration.
The expected outcome is a practical, risk-based methodology for transitioning critical infrastructure toward quantum-resistant security. By integrating cryptographic discovery, standardized algorithm selection, hybrid deployment, crypto-agility, and systematic performance evaluation, the proposed framework aims to reduce long-term exposure to quantum-enabled cryptographic attacks while preserving operational continuity.

3. Experimental Study

The experimental study is designed to evaluate the feasibility, performance, and operational suitability of Post-Quantum Cryptography (PQC) for protecting critical infrastructure against the potential threats posed by Shor's algorithm. The study compares conventional cryptographic algorithms with standardized post-quantum alternatives and examines the performance implications of transitioning to quantum-resistant security mechanisms. The experimental framework focuses on key establishment, digital signatures, computational overhead, memory consumption, communication efficiency, and compatibility with infrastructure systems.

The study is intended to determine whether PQC algorithms can provide a practical foundation for securing critical infrastructure while maintaining acceptable performance and operational reliability. Since Shor's algorithm threatens conventional public-key cryptography rather than all cryptographic mechanisms, the experiments focus primarily on replacing vulnerable RSA- and ECC-based operations.

3.1 Experimental Setup

The proposed experimental environment consists of a controlled test platform simulating communication between critical infrastructure components, such as industrial controllers, monitoring systems, gateway devices, and centralized management servers. Classical and post-quantum cryptographic implementations are evaluated under identical test conditions to ensure a fair comparison.

The following configurations are considered:

- Classical cryptography: RSA and Elliptic Curve Cryptography (ECC) for conventional public-key operations.
- Post-quantum cryptography: ML-KEM for key establishment and ML-DSA and SLH-DSA for digital signatures.
- Hybrid cryptography: Compatible combinations of classical and post-quantum mechanisms, where supported by the selected protocols and implementations.

The post-quantum algorithms are selected from the standards published by the National Institute of Standards and Technology (NIST). ML-KEM, ML-DSA, and SLH-DSA are standardized in FIPS 203, FIPS 204, and FIPS 205, respectively.

The experiments should be conducted on a documented hardware and software platform, recording the processor, memory, operating system, cryptographic library versions, algorithm parameters, and test configuration. Repeated measurements should be performed under consistent workloads to reduce measurement variability.

3.2 Experimental Parameters

The study evaluates the cryptographic configurations using the following performance and operational parameters.

Parameter	Measurement objective
Key generation time	Time required to generate cryptographic keys
Encapsulation/decapsulation time	Time required for ML-KEM key establishment operations
Signing time	Time required to generate digital signatures
Verification time	Time required to validate digital signatures
Key and signature size	Storage and transmission requirements
Memory consumption	RAM required during cryptographic operations
Communication latency	Additional delay introduced by cryptographic processing and protocol exchange
Throughput	Number of successful operations completed per unit of time
Interoperability	Ability of supported devices and software implementations to communicate correctly

Measurements should distinguish cryptographic execution time from total network latency. For example, key establishment may involve several protocol messages, while signature generation and verification may occur independently of the network exchange.

3.3 Experimental Procedure

The experiment follows a structured sequence to evaluate the different cryptographic approaches.

1. Baseline measurement: Execute RSA- and ECC-based operations to establish reference performance values.
2. Post-quantum evaluation: Measure the execution time, memory consumption, and output sizes of ML-KEM, ML-DSA, and SLH-DSA.
3. Hybrid configuration testing: Evaluate supported hybrid key-establishment or authentication configurations and record their additional computational and communication costs.
4. Infrastructure workload simulation: Test cryptographic operations under representative device-to-gateway and gateway-to-server communication workloads.
5. Repeated trials: Conduct multiple independent runs for each configuration and calculate the mean, median, standard deviation, and relevant percentile latencies.
6. Comparative analysis: Compare the observed results to determine the trade-offs between cryptographic performance, resource requirements, and migration suitability.

The test environment should use consistent security settings and clearly document the selected parameter sets. The experiments must also verify successful key establishment, signature validation, and rejection of invalid signatures or improperly formed messages.

3.4 Performance Evaluation Metrics

The experimental results can be analyzed using quantitative metrics to determine the relative overhead introduced by post-quantum cryptographic mechanisms.

1. Execution time overhead

The percentage change in execution time can be calculated as:

Ot=TPQC−TclassicalTclassical×100O_t=\frac{T_{\mathrm{PQC}}-T_{\mathrm{classical}}}{T_{\mathrm{classical}}}\times100

where TPQCT_{\mathrm{PQC}} represents the measured execution time of the post-quantum operation and TclassicalT_{\mathrm{classical}} represents the corresponding classical baseline.

2. Communication overhead

The relative increase in transmitted data can be calculated as:

Oc=SPQC−SclassicalSclassical×100O_c=\frac{S_{\mathrm{PQC}}-S_{\mathrm{classical}}}{S_{\mathrm{classical}}}\times100

where SPQCS_{\mathrm{PQC}} and SclassicalS_{\mathrm{classical}} denote the measured communication sizes for equivalent tasks.

3. Throughput

Throughput can be measured as:

R=NsuccessfulTtotalR=\frac{N_{\mathrm{successful}}}{T_{\mathrm{total}}}

where NsuccessfulN_{\mathrm{successful}} is the number of successfully completed operations and TtotalT_{\mathrm{total}} is the total measurement duration.

These metrics enable an objective comparison of the computational and communication costs associated with alternative cryptographic configurations.

3.5 Comparative Analysis

The expected qualitative trade-offs to investigate are summarized below. These are hypotheses for experimental evaluation, not measured results.

Evaluation criterion	Classical cryptography	Post-quantum cryptography	Hybrid configuration
Resistance to Shor's algorithm	RSA and ECC are vulnerable	Designed to resist known quantum attacks	Depends on correct construction and PQC component security
Key establishment	Established implementations	ML-KEM-based	May require additional processing and protocol support
Digital signatures	Mature RSA/ECC ecosystems	Different key and signature sizes across algorithms	Potentially greater validation and transmission costs
Legacy compatibility	Generally high	Depends on software and hardware support	Requires compatible protocols and implementations
Migration complexity	Low for existing deployments	Requires algorithm and infrastructure updates	May help staged migration but increases integration complexity
Resource requirements	Well characterized	Must be measured for the target platform	Depends on the combined implementation

The table identifies the main dimensions of comparison without assuming that PQC will always be slower or require more resources. Actual performance depends on the algorithm, parameter set, implementation, hardware platform, and network protocol.

3.6 Security and Reliability Assessment

In addition to performance testing, the experimental study evaluates the reliability of the proposed migration model. Test cases should include invalid signature verification, malformed cryptographic messages, unsuccessful key establishment, certificate compatibility failures, and attempted fallback to weaker cryptographic configurations.
For critical infrastructure, additional testing should examine service continuity during key or certificate updates, recovery from failed deployments, and the behavior of resource-constrained devices under heavy workloads. Testing should initially occur in an isolated laboratory environment or a non-production testbed to avoid disrupting operational technology and safety-critical services.

The study should also acknowledge that benchmarking cannot establish resistance to every possible cryptographic attack. Security assessment must combine standards compliance, implementation review, protocol analysis, and appropriate independent testing.

3.7 Results Analysis and Discussion

The collected experimental data will be used to determine which cryptographic configurations best satisfy the performance and security requirements of different critical infrastructure environments. Classical implementations will provide the baseline, while PQC implementations will be evaluated for their computational requirements, communication overhead, and suitability for resource-constrained systems.

Particular attention will be given to the distinction between high-performance servers and embedded industrial devices. A configuration that performs adequately on a centralized server may impose unacceptable latency or memory requirements on a low-power controller. Similarly, larger cryptographic messages may affect network performance in bandwidth-constrained or latency-sensitive environments.

The results will support a risk-based deployment strategy in which the most sensitive systems and those with long replacement cycles receive priority. Hybrid approaches may be considered where interoperability and migration requirements justify their additional complexity, subject to appropriate security validation.

Note: Actual numerical findings should be reported only after the experiments have been executed. If experimental measurements are unavailable, this section should be presented as a proposed experimental design rather than as a completed empirical study.

3.8 Summary

The experimental study establishes a systematic approach for comparing classical, post-quantum, and hybrid cryptographic configurations in critical infrastructure environments. By measuring execution time, communication overhead, resource consumption, interoperability, and operational reliability, the study aims to identify practical migration options for reducing exposure to the future quantum threat posed by Shor's algorithm. The findings are intended to inform cryptographic selection, deployment planning, and long-term infrastructure resilience without compromising essential operational requirements.

RESULTS AND ANALYSIS

The results and analysis section evaluates the performance, security characteristics, and deployment feasibility of Post-Quantum Cryptography (PQC) for critical infrastructure protection against the potential impact of Shor's algorithm. The analysis compares conventional cryptographic algorithms, including RSA and Elliptic Curve Cryptography (ECC), with standardized post-quantum algorithms such as ML-KEM, ML-DSA, and SLH-DSA. The primary objective is to identify the trade-offs between quantum-resistant security, computational efficiency, communication overhead, and compatibility with existing infrastructure.

Note: The following analysis presents expected qualitative findings based on the characteristics of the algorithms. Since no experimental measurements have been provided, numerical performance improvements or benchmark results are not claimed.

4.1 Comparative Cryptographic Analysis

Conventional public-key cryptographic algorithms are widely deployed because of their mature implementations and extensive ecosystem support. However, RSA and ECC rely on mathematical problems that Shor's algorithm can solve efficiently on a sufficiently powerful fault-tolerant quantum computer. Consequently, these algorithms represent a significant long-term security risk for critical infrastructure.

In contrast, PQC algorithms are designed around mathematical problems for which no comparable efficient quantum attack is currently known. ML-KEM supports secure key establishment, while ML-DSA and SLH-DSA provide digital signature mechanisms. Their suitability depends on the security requirements and implementation constraints of each infrastructure environment.

Evaluation parameter	RSA/ECC	ML-KEM	ML-DSA	SLH-DSA
Primary function	Key establishment and/or signatures, depending on the scheme	Key establishment	Digital signatures	Digital signatures
Resistance to Shor's algorithm	Vulnerable	Designed to resist known quantum attacks	Designed to resist known quantum attacks	Designed to resist known quantum attacks
Main evaluation focus	Baseline performance and compatibility	Encapsulation and decapsulation performance	Signing and verification efficiency	Signing and verification efficiency
Deployment consideration	Existing ecosystem support	Key and ciphertext sizes, protocol integration	Signature sizes and verification costs	Signature sizes and computational costs

The comparison indicates that PQC migration is not simply a matter of replacing one algorithm with another. Different cryptographic functions require different algorithms, and each implementation must be assessed according to its security level, performance requirements, and operational context.

4.2 Computational Performance Analysis

Computational performance is an important consideration when integrating quantum-resistant cryptography into critical infrastructure. Industrial control systems, smart meters, embedded sensors, and remote monitoring devices may operate with limited processing power and memory.

The analysis should measure key generation, encapsulation, decapsulation, signing, and verification times independently. These measurements can reveal whether an algorithm introduces processing delays that affect real-time communication or authentication.

The expected findings are as follows:

- Classical cryptography: Existing RSA and ECC implementations provide a useful performance baseline, although their conventional public-key security is vulnerable to sufficiently capable quantum computers.
- ML-KEM: Its key-establishment operations should be evaluated for processing time, memory use, and integration into existing secure communication protocols.
- ML-DSA: Its signature generation and verification costs should be measured for authentication services, firmware updates, and software integrity checks.
- SLH-DSA: Its hash-based construction provides an alternative signature approach, with performance and signature-size trade-offs that must be considered for the target application.

The results should be interpreted using repeated measurements, including median execution time and high-percentile latency. This is particularly important for operational technology, where occasional delays can be more significant than average performance.

4.3 Communication and Storage Overhead

PQC adoption can change the size of cryptographic keys, ciphertexts, signatures, and certificates. These differences may influence bandwidth utilization, network latency, storage requirements, and protocol compatibility.

For example, larger authentication messages may increase the transmission time for devices operating over low-bandwidth industrial networks. Certificate chains and signed firmware packages may also require additional storage or communication resources.

The impact is expected to vary across applications:

- Industrial control networks: Message size and latency are important because communication may have strict timing requirements.
- Smart grids and energy systems: Large numbers of distributed devices can make certificate management and network overhead significant.
- Healthcare infrastructure: Long-term confidentiality and secure device authentication may justify additional cryptographic resource requirements.
- Telecommunications: High connection volumes require careful evaluation of throughput, memory consumption, and handshake performance.

Therefore, communication overhead should be measured at both the cryptographic-operation level and the complete protocol level. Algorithm output sizes alone do not capture the full cost of deployment.

4.4 Security Analysis Against Shor's Algorithm

The principal security benefit of adopting PQC is the reduction of dependence on public-key cryptographic mechanisms that are vulnerable to quantum attacks. Shor's algorithm threatens RSA and ECC because it can efficiently solve the mathematical problems underlying their security when executed on a sufficiently powerful fault-tolerant quantum computer.

ML-KEM, ML-DSA, and SLH-DSA are standardized to provide security based on different mathematical constructions that are not known to be efficiently broken by Shor's algorithm. However, post-quantum cryptography should not be interpreted as providing absolute or unconditional security. Implementation weaknesses, side-channel attacks, poor key management, and protocol vulnerabilities can still compromise systems.

A hybrid deployment may help organizations transition gradually by combining compatible classical and post-quantum mechanisms. Nevertheless, the security of a hybrid system depends on the protocol construction, correct implementation, and resistance to downgrade attacks. Hybrid deployment therefore requires careful validation rather than an assumption that combining algorithms automatically improves security.

4.5 Overall Evaluation of the Proposed Model

The proposed five-layer framework combines cryptographic discovery, risk assessment, algorithm selection, hybrid deployment, and continuous validation. Its principal advantage is that it treats quantum readiness as an infrastructure-wide migration problem rather than an isolated algorithm replacement.

Proposed component	Expected contribution	Evaluation criterion
Cryptographic discovery	Identifies vulnerable algorithms and dependencies	Inventory completeness
Quantum risk assessment	Prioritizes systems according to exposure and criticality	Risk classification accuracy
PQC algorithm selection	Matches cryptographic functions to standardized algorithms	Security and performance compliance
Hybrid deployment	Supports staged migration where appropriate	Interoperability and protocol security
Crypto-agility	Simplifies future algorithm updates	Replacement time and configuration flexibility
Continuous validation	Detects operational and implementation problems	Failure rates, availability, and test coverage

The framework is expected to support a more controlled transition by identifying high-priority assets, evaluating candidate algorithms, and validating changes before production deployment. Its effectiveness should ultimately be

assessed using measurable outcomes, including inventory coverage, migration completion, connection success rates, latency, resource utilization, and recovery behavior.

4.6 Practical Implications for Critical Infrastructure

The analysis suggests that no single cryptographic configuration will be optimal for every infrastructure environment. High-capacity servers may accommodate different algorithm and protocol choices than low-power sensors or safety-critical controllers. Consequently, algorithm selection should be based on both quantum threat exposure and operational requirements.

Organizations should prioritize systems that protect long-lived sensitive information, support essential services, or have lengthy hardware replacement cycles. They should also establish cryptographic inventories, test standardized PQC implementations, review certificate and key-management systems, and develop phased migration plans.

The "harvest now, decrypt later" threat further strengthens the case for early planning. Information collected today may remain sensitive when future quantum capabilities become available, making the confidentiality lifetime of data an important factor in migration prioritization.

4.7 Summary of Findings

The comparative analysis identifies three principal conclusions.

1. Quantum vulnerability: RSA and ECC require migration planning because Shor's algorithm threatens their underlying mathematical security assumptions.

2. Performance trade-offs: Post-quantum algorithms introduce implementation-specific computational, storage, and communication considerations that must be evaluated under realistic workloads.

3. Structured migration: Cryptographic discovery, risk-based prioritization, crypto-agility, hybrid deployment where appropriate, and continuous validation provide a practical foundation for quantum readiness.

Overall, the proposed model offers a structured approach to preparing critical infrastructure for the potential impact of quantum computing. However, the magnitude of performance overhead and the operational benefits of individual configurations must be established through reproducible experimental measurements. Future evaluation should include real-world or representative testbeds, standardized parameter sets, independent security testing, and comparisons across both server-grade and resource-constrained hardware.

Comparative Analysis

Evaluation Parameter	Classical Cryptography (RSA/ECC)	Post-Quantum Cryptography (ML-KEM, ML-DSA, SLH-DSA)	Hybrid Cryptography
Security against Shor's algorithm	Vulnerable	Designed to resist known quantum attacks	Depends on secure integration of classical and PQC mechanisms
Key establishment	RSA key transport or ECC-based mechanisms	ML-KEM	Combines compatible classical and PQC key-establishment methods
Digital signatures	RSA and ECDSA	ML-DSA and SLH-DSA	May combine classical and PQC signatures
Computational overhead	Implementation-dependent; mature optimization	Varies by algorithm, parameter set, and platform	May require additional computation
Key and signature sizes	Generally smaller for ECC; RSA sizes vary	Varies; some keys and signatures are larger	May increase total message size
Communication latency	Established baseline	Depends on algorithm and protocol integration	May increase handshake or authentication latency
Legacy compatibility	Generally high	Requires compatible software, hardware, and protocols	Requires support for hybrid mechanisms
Resource requirements	Well understood in existing deployments	Must be evaluated for memory, CPU, and energy use	May require additional resources
Migration complexity	Low for existing systems	Requires cryptographic and infrastructure updates	Supports staged migration but adds integration complexity

Long-term quantum readiness	Insufficient for quantum-vulnerable public-key mechanisms	Suitable foundation for quantum-resistant migration	Useful transitional approach when securely implemented
Major limitation	Vulnerability to sufficiently powerful quantum computers	Implementation and compatibility challenges	Protocol complexity and potential downgrade risks
Recommended application	Existing systems during the transition period	Long-term quantum-resistant deployments	Carefully tested transitional deployments

Analysis: The comparison indicates that post-quantum cryptography provides a practical path toward protecting critical infrastructure from future quantum attacks. Classical cryptography offers mature ecosystem support but cannot provide long-term quantum resistance when based on RSA or ECC. PQC algorithms introduce implementation-specific performance and compatibility considerations, while hybrid cryptography can facilitate gradual migration when appropriately designed and validated. Therefore, a risk-based migration strategy combining standardized PQC algorithms, crypto-agility, and performance testing is recommended.

Note: This table presents a qualitative comparison, not measured experimental results. Actual performance depends on the implementation, hardware platform, algorithm parameters, and communication protocol.

CONCLUSION

The advancement of quantum computing presents a significant challenge to conventional cryptographic systems used to protect critical infrastructure. Shor's algorithm has the potential to compromise widely deployed public-key cryptographic algorithms, including RSA and Elliptic Curve Cryptography (ECC), when executed on a sufficiently powerful fault-tolerant quantum computer. This threat highlights the need for proactive security measures to protect essential services such as power grids, financial networks, healthcare systems, telecommunications, and industrial control systems.

This paper examined the role of Post-Quantum Cryptography (PQC) in preparing critical infrastructure for the quantum computing era. The proposed framework integrates cryptographic asset discovery, quantum risk assessment, standardized algorithm selection, hybrid deployment, crypto-agility, and continuous security monitoring. Standardized algorithms such as ML-KEM, ML-DSA, and SLH-DSA provide a foundation for developing quantum-resistant key-establishment and digital-signature mechanisms. Their adoption can help reduce dependence on public-key cryptographic systems vulnerable to quantum attacks.

The comparative analysis also highlights important implementation challenges, including computational overhead, increased cryptographic data sizes, compatibility with legacy infrastructure, deployment costs, and uncertainty associated with future cryptanalysis. These limitations demonstrate that migrating to PQC requires more than replacing existing algorithms; it demands careful planning, performance evaluation, interoperability testing, and ongoing security validation. Furthermore, the threat of "harvest now, decrypt later" attacks emphasizes the importance of protecting sensitive information whose confidentiality must be maintained over long periods.

In conclusion, a phased, risk-based migration to standardized post-quantum cryptographic mechanisms, supported by crypto-agility and rigorous testing, offers a practical strategy for strengthening the long-term security and resilience of critical infrastructure. Future work should focus on implementing the proposed framework in representative industrial environments, conducting reproducible performance benchmarks across diverse hardware platforms, and evaluating the reliability of hybrid cryptographic deployments. Such efforts can help organizations prepare for evolving quantum threats while maintaining operational continuity, data confidentiality, and trust in essential digital systems.

REFERENCES

1. Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), Post-quantum cryptography (pp. 1–14). Springer. https://doi.org/10.1007/978-3-540-88702-7_1
2. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638
3. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (pp. 212–219). Association for Computing Machinery. https://doi.org/10.1145/237814.237866
4. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723
5. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

6. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172
7. Jordan, S. P., & Liu, Y.-K. (2018). Quantum cryptanalysis: Shor, Grover, and beyond. IEEE Security & Privacy, 16(5), 14–21. https://doi.org/10.1109/MSP.2018.3761719
8. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process (NIST Interagency/Internal Report 8413). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8413
9. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 353–367). IEEE. https://doi.org/10.1109/EuroSP.2018.00032
10. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(1), 238–268. https://doi.org/10.13154/tches.v2018.i1.238-268
11. National Institute of Standards and Technology. (2016). Report on post-quantum cryptography (NIST Interagency/Internal Report 8105). U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8105
12. National Institute of Standards and Technology. (2024a). Module-lattice-based key-encapsulation mechanism standard (FIPS PUB 203). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203
13. National Institute of Standards and Technology. (2024b). Module-lattice-based digital signature standard (FIPS PUB 204). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204
14. National Institute of Standards and Technology. (2024c). Stateless hash-based digital signature standard (FIPS PUB 205). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.205
15. National Institute of Standards and Technology. (2025). Status report on the fourth round of the NIST post-quantum cryptography standardization process (NIST Interagency/Internal Report 8545). U.S. Department of Commerce.
16. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography (NIST Interagency/Internal Report 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105
17. Liu, Y.-K., & Moody, D. (2024). Post-quantum cryptography and the quantum future of cybersecurity. Physical Review Applied, 21(4), 040501. https://doi.org/10.1103/PhysRevApplied.21.040501
18. Biasse, J.-F., Bonnetain, X., Bouvier, C., & others. (2023). Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography. IET Information Security, 17(2), 171–209. https://doi.org/10.1049/ise2.12081
19. Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process (NIST Interagency/Internal Report 8309). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8309
20. National Institute of Standards and Technology. (2024). Transition to post-quantum cryptography standards (NIST Interagency/Internal Report 8547, Initial Public Draft). U.S. Department of Commerce.