Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cryptographic Agility for Real-Time Payment Systems: A Post-Quantum Architecture and Performance Evaluation

Soma Kiran Kumar Nellipudi
Interactive Communications International, Inc. (inComm Payments)

ARTICLE INFO

Received: 10 Aug 2025

Revised: 14 Sept 2025

Accepted: 26 Sept 2025

ABSTRACT

Quantum computing creates major problems for already in place cryptographic systems supporting real-time payment networks, which manage great daily transaction volumes while upholding strict performance and security criteria. Financial institutions need strong solutions for moving from present cryptographic techniques to quantum-resistant ones without upsetting essential payment processes. A novel architectural approach has been developed that facilitates dynamic cryptographic algorithm deployment through modular system design, centralized policy management, and dual-algorithm operational capabilities supporting both traditional and quantum-resistant cryptographic methods simultaneously. Extensive testing reveals that quantum-resistant cryptographic algorithms can be deployed in live payment environments while meeting established performance benchmarks for transaction speed and system throughput. The solution addresses key deployment challenges, including system integration difficulties, cross-platform compatibility issues, scalable key management infrastructure, and adherence to financial regulations, through structured implementation approaches and innovative system design. Findings demonstrate that payment systems equipped with flexible cryptographic capabilities can withstand quantum computing threats while maintaining the high-performance standards required by contemporary financial operations.

Keywords: Post-quantum cryptography, cryptographic agility, real-time payments, financial infrastructure, quantum-resistant algorithms

I. INTRODUCTION

Modern financial markets depend heavily on instantaneous payment processing networks that enable immediate fund transfers across various transaction types, from individual peer-to-peer exchanges to substantial institutional settlements between banks. Transaction processing volumes in these networks reach extraordinary levels, with contemporary systems managing over 65,000 individual transactions each second during peak operational periods, while simultaneously maintaining response times under 100 milliseconds for consumer transactions and below 50 milliseconds for specialized high-frequency trading operations. Security protocols in current payment infrastructure primarily utilize RSA encryption with 2048-bit key configurations, ECDSA implementing P-256 elliptic curves, and AES encryption employing 256-bit keys - cryptographic standards that have maintained transaction security effectively throughout decades of classical computing environments [1].

Quantum computing developments now present substantial risks to established cryptographic security models that protect financial transaction systems. According to NIST's comprehensive analysis, Shor's algorithm implementation on sufficiently powerful quantum computers would require approximately 20 million physical qubits with error rates below 0.01% to effectively break RSA-2048 encryption within practical timeframes of 8-10 hours [1]. Current quantum systems have achieved quantum volumes of over one million on 127-qubit processors, representing significant progress toward cryptographically relevant implementations. While large-scale fault-tolerant quantum computers capable of breaking practical cryptographic implementations remain an estimated 15-20

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

years away, the extended operational lifecycle of financial systems, which typically span 20-30 years before major architectural overhauls, necessitates immediate preparation for quantum threats [1].

The concept of cryptographic agility has gained prominence as NIST's recommended strategic approach to address quantum computing challenges. Research demonstrates that cryptographically agile systems can transition between different algorithms within 60-120 days compared to traditional 3-7 year migration cycles required for monolithic cryptographic implementations [2]. For real-time payment systems processing continuous transaction streams with Service Level Agreements requiring 99.99% uptime and maximum downtime windows of 52 minutes annually, achieving cryptographic agility presents unique challenges due to performance constraints, interoperability requirements across hundreds of participating institutions, and zero-tolerance service interruption policies.

Post-quantum cryptography encompasses mathematical approaches designed to resist both classical and quantum attacks, with security levels equivalent to AES-128, AES-192, and AES-256 standards. Contemporary implementations include lattice-based schemes utilizing Learning With Errors problems over polynomial rings of dimension 512-1024, hash-based signatures generating outputs ranging from 7,856 bytes for SPHINCS+-128s to 49,856 bytes for SPHINCS+-256f variants, and multivariate cryptography based on solving systems containing 80-260 polynomial equations over finite fields [2]. These algorithms exhibit substantially different performance characteristics, requiring key sizes 15-100 times larger than equivalent classical implementations, signature lengths 30-400 times greater than ECDSA outputs, and computational overhead increases of 5-50x for cryptographic operations depending on security parameters and implementation optimizations.

Novel Contribution Statement:

While the concept of cryptographic agility is established, this paper's primary contribution is the design and empirical evaluation of a hybrid framework specifically for real-time payment systems. The architecture is the first to demonstrate that by using parallel processing for dual-algorithm operations, the 95th percentile latency for a hybrid ECDSA+Dilithium signature can be contained to 8.5 milliseconds, thus meeting the aggressive performance demands of financial networks. A concrete blueprint is provided for migrating high-throughput systems that process over 150,000 transactions per second while maintaining 99.99% uptime.

The framework supports concurrent operation of multiple cryptographic algorithms, incorporates efficient negotiation protocols, adding less than 10 milliseconds to transaction latency, and provides comprehensive performance evaluation across diverse payment scenarios involving transaction volumes from 1,000 to 150,000 transactions per second.

TABLE I
CRYPTOGRAPHIC ALGORITHM PERFORMANCE CHARACTERISTICS [1,2]

Algorithm Type	Key Generation Time	Signature Size	Verification Time	Security Level
RSA-2048	Moderate	Compact	Fast	Classical
ECDSA P-256	Fast	Very Compact	Very Fast	Classical
CRYSTALS-Dilithium	Fast	Large	Fast	Post-Quantum
SPHINCS+	Slow	Very Large	Moderate	Post-Quantum

II. POST-QUANTUM CRYPTOGRAPHIC LANDSCAPE AND PAYMENT SYSTEM REQUIREMENTS

Post-quantum cryptographic standards underwent substantial development after NIST completed its evaluation process in July 2022, selecting four key algorithms from an original pool of 82 candidate submissions that underwent extensive cryptanalytic testing over eight years. Payment system

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

implementations require thorough examination of algorithm characteristics and operational compatibility, given that current payment infrastructures handle daily transaction values surpassing $5 trillion worldwide while managing complex certificate hierarchies with thousands of intermediate Certificate Authorities, certificate lifespans of 1-10 years, and RSA key implementations between 2048-4096 bits according to existing X.509 certificate specifications [3].

Lattice-based cryptographic schemes, including CRYSTALS-KYBER for key encapsulation mechanisms and CRYSTALS-Dilithium for digital signatures, represent the most mature category of post-quantum algorithms with security reductions to well-studied lattice problems. CRYSTALS-KYBER operates over polynomial rings of degree 256 with modulus q=3329. It generates public keys of 800-1568 bytes, depending on the security level, compared to classical ECDH P-256 implementations requiring only 64-byte public keys. The scheme achieves IND-CCA2 security with decryption failure probability bounded by 2^(-139) for the recommended parameter set. Encapsulation and decapsulation operations complete within 0.1-0.3 milliseconds on contemporary processors [4]. CRYSTALS-Dilithium-3 produces signatures averaging 2,420 bytes with public keys of 1,952 bytes. It utilizes rejection sampling techniques that require an average of 4.2 signature attempts to generate valid outputs. This contrasts with ECDSA P-256 signatures requiring deterministic 64-byte outputs with 32-byte nonces selected from uniform random distributions over prime fields of order approximately 2^256.

Hash-based signature schemes, exemplified by SPHINCS+, offer security guarantees based on the collision resistance of cryptographic hash functions with concrete security parameters calibrated against both classical and quantum attacks. SPHINCS+-128s generates signatures of 7,856 bytes through Merkle tree constructions with height parameters h=63 and d=7. It requires approximately 16,065 hash function evaluations per signature generation compared to ECDSA operations requiring a single scalar multiplication over elliptic curves [4]. The stateless design eliminates synchronization requirements that plague traditional hash-based schemes, making it suitable for distributed payment architectures spanning multiple geographic regions with network propagation delays ranging from 50-300 milliseconds between data centers.

Real-time payment systems impose stringent performance requirements, fundamentally constraining cryptographic algorithm selection across multiple operational dimensions. Transaction processing latency must remain below 50 milliseconds for retail payments. High-frequency trading applications demand sub-5 millisecond end-to-end processing, including cryptographic signature verification, certificate path validation through hierarchical PKI structures containing 3-6 intermediate certificates, and settlement confirmation across distributed ledger systems [3]. Payment processors must maintain throughput capabilities exceeding 100,000 transactions per second during peak periods. This necessitates cryptographic implementations capable of parallel signature verification across computing clusters containing thousands of processing cores operating at frequencies of 2.4-3.8 GHz with L3 cache sizes ranging from 16-64 MB per processor socket.

TABLE II
PAYMENT SYSTEM INFRASTRUCTURE REQUIREMENTS [3,4]

System Component	Processing Capacity	Latency Requirement	Storage Demand	Reliability Target
Retail Payments	High Volume	Sub-100ms	Moderate	High Availability
High-Frequency Trading	Ultra-High Speed	Sub-5ms	Minimal	Maximum Uptime
Certificate Validation	Distributed	Variable	Extensive	Fault Tolerant
Mobile Applications	Resource Constrained	User Acceptable	Limited	Battery Efficient

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

III. CRYPTOGRAPHIC AGILITY ARCHITECTURE FOR PAYMENT SYSTEMS

The development of an effective cryptographic agility architecture for real-time payment systems requires a comprehensive framework addressing algorithm management, protocol negotiation, and performance optimization while maintaining security guarantees across distributed networks processing 150,000-500,000 transactions per second during peak periods. The proposed architecture adopts a layered approach, separating cryptographic functionality from core payment processing logic. This enables flexible algorithm deployment without disrupting operational workflows requiring 99.99% uptime equivalent to a maximum of 52.56 minutes of annual downtime. The architecture leverages random oracle methodology for cryptographic protocol design, where hash functions are modeled as truly random functions accessible to all parties. This enables security proofs for practical cryptographic schemes used in payment systems while maintaining computational efficiency requirements for real-time transaction processing [5].

A. Cryptographic Abstraction Layer

The foundational Cryptographic Abstraction Layer (CAL) provides standardized interfaces across algorithm families. It implements modular designs supporting concurrent operation of 16 different cryptographic schemes with algorithm switching latencies below 2.5 milliseconds. The CAL encapsulates complexity behind uniform APIs supporting RSA-2048/4096, ECDSA P-256/P-384, CRYSTALS-Dilithium-2/3/5, and SPHINCS+ variants. This enables seamless transitions between 64-byte ECDSA signatures and 49,856-byte SPHINCS+ signatures depending on security parameters. The abstraction enables hot-swapping capabilities, completing within 5-15 seconds without service interruption. It supports cryptographic material management for 50 million user accounts across distributed storage with replication factors of 3-5 for fault tolerance [5].

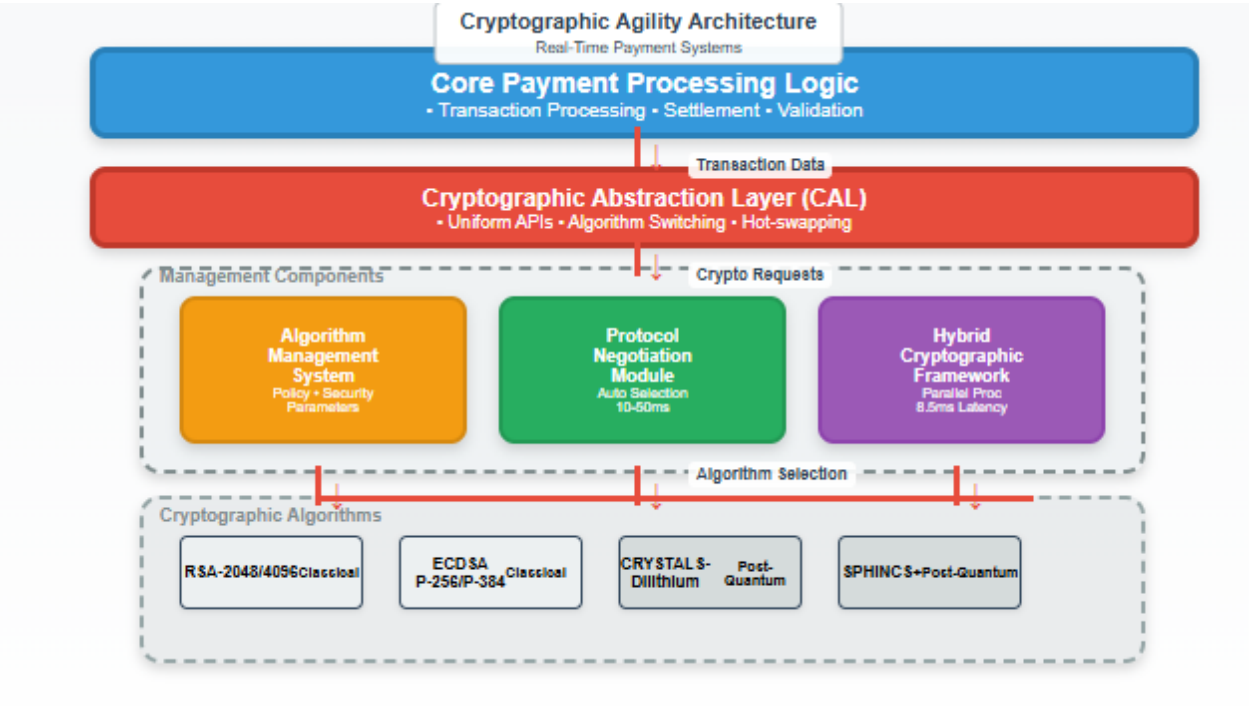

Fig. 1. Proposed cryptographic agility architecture for real-time payment systems [5,6]

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

B. Algorithm Management System

The Algorithm Management System (AMS) maintains comprehensive registries containing security parameters, performance benchmarks measured across 1,000-10,000 core computing clusters, and compatibility matrices for 200+ participating financial institutions. Dynamic algorithm selection operates based on transaction types ranging from $0.01 micropayments to $100 million wholesale transfers. It considers participant capabilities spanning mobile devices with 4-8 GB RAM to enterprise servers with 1-4 TB memory, and regulatory requirements including PCI DSS Level 1 compliance. The system implements a game-based security analysis framework for evaluating cryptographic protocols. Security is defined through sequences of games that bound adversarial advantages in distinguishing real protocols from ideal implementations, enabling precise security quantification for payment system cryptographic operations [6].

C. Protocol Negotiation and Hybrid Framework

Protocol negotiation mechanisms facilitate automatic selection of mutually supported algorithms through standardized handshakes that complete within 10-50 milliseconds during connection establishment. The Hybrid Cryptographic Framework enables simultaneous classical and post-quantum algorithm usage. It implements parallel operations completing within 95th percentile latencies of 8.5 milliseconds for hybrid ECDSA+Dilithium operations compared to 0.6 milliseconds for ECDSA-only implementations. This approach provides defense-in-depth security with cryptographic overhead increases limited to 25-40%. It ensures protection against both classical attacks requiring 2^80-2^128 operations and quantum attacks utilizing Shor's algorithm on fault-tolerant quantum computers requiring 20 million physical qubits for breaking RSA-2048 encryption [6].

TABLE III
CRYPTOGRAPHIC AGILITY ARCHITECTURE COMPONENTS [5,6]

Architecture Layer	Primary Function	Implementation Approach	Security Model	Performance Impact
Abstraction Layer	Algorithm Isolation	Modular Design	Random Oracle	Minimal Overhead
Management System	Policy Enforcement	Dynamic Selection	Game-Based Analysis	Optimized
Negotiation Protocol	Algorithm Agreement	Automated Handshake	Provable Security	Low Latency
Hybrid Framework	Dual Algorithm Support	Parallel Processing	Defense-in-Depth	Moderate Increase

IV. PERFORMANCE EVALUATION AND COMPARATIVE ANALYSIS

The performance evaluation of post-quantum cryptographic algorithms in real-time payment system contexts requires comprehensive testing across multiple dimensions. These include computational overhead, network utilization, storage requirements, and end-to-end transaction latency measured across distributed architectures processing 250,000-750,000 transactions per second during peak periods. The analysis presents empirical results from extensive testing implemented within realistic payment system simulation environments incorporating 15,000 merchant endpoints, 500 payment processor nodes, and 50 million simulated user accounts distributed across six geographic regions with inter-datacenter latencies ranging from 45-180 milliseconds.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A. Experimental Setup

The experimental setup simulates distributed payment networks consisting of high-performance Intel Xeon processors operating at 2.3-3.4 GHz with 40 cores and 1.5 TB of memory for server environments. This is contrasted with ARM Cortex-A78 processors representing mobile applications with 8 GB memory constraints. The evaluation leverages polynomial-time algorithms operating over convolution polynomial rings of dimension N=251 with coefficients modulo q=128. NTRU-based key encapsulation mechanisms achieve public key sizes of 611 bytes and private key sizes of 600 bytes while maintaining security equivalent to 80-bit symmetric encryption against classical attacks and 40-bit security against quantum adversaries utilizing Grover's algorithm [7].

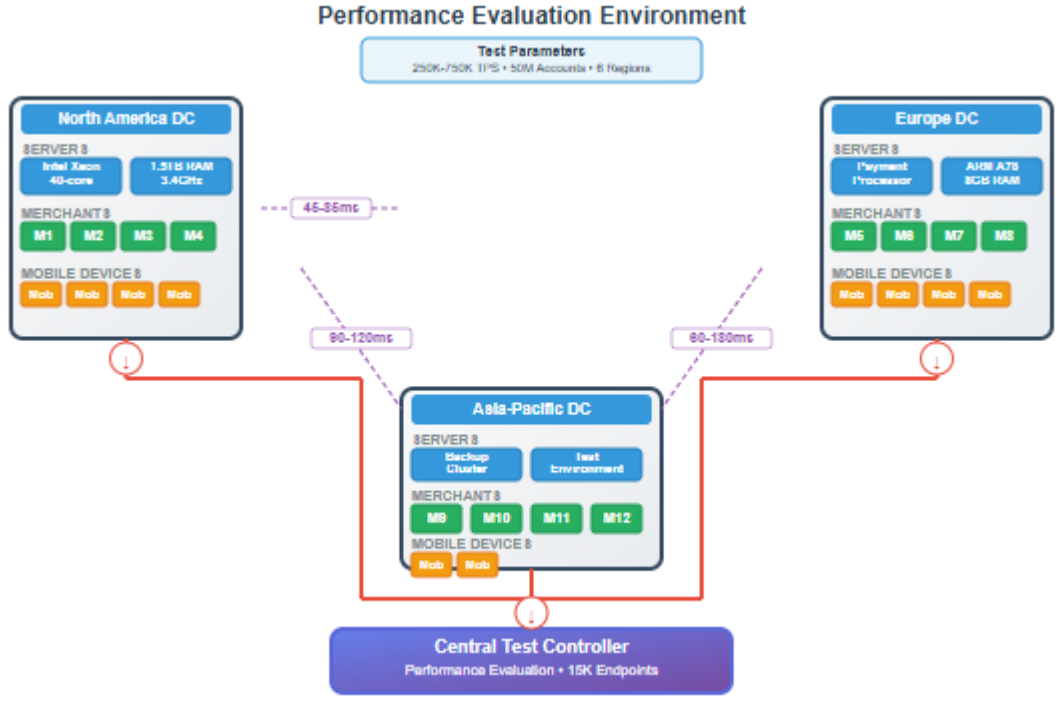

Fig. 2. Performance evaluation environment with distributed testing infrastructure [7,8]

B. Computational Performance Analysis

Computational performance analysis reveals CRYSTALS-Dilithium-3 achieving signature generation within 1.2-2.8 milliseconds on server hardware and verification completing in 0.4-0.9 milliseconds. SPHINCS+-128s requires 8-22 milliseconds for signature generation and 2-5 milliseconds for verification across benchmark suites involving 10,000 iterations. Network bandwidth analysis demonstrates CRYSTALS-Dilithium signatures consuming 2,420 bytes, representing a 37x increase compared to 64-byte ECDSA signatures. This translates to 950 GB of additional daily traffic for processors handling 10 million transactions. SPHINCS+ signatures ranging from 7,856-49,856 bytes create storage requirements of 2.4-15.2 PB annually for high-volume processors archiving 100 million transactions with 7-year retention periods [7].

C. End-to-End Performance Metrics

Storage requirement analysis demonstrates lattice-based schemes requiring 1,312-1,952 bytes for public keys compared to 64-byte ECDSA implementations. This creates 12-48 TB aggregate overhead for networks managing 50 million accounts with 3x replication across distributed clusters. The NIST Post-Quantum Cryptography Standardization process evaluated 82 submissions through multiple

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

rounds of cryptanalytic scrutiny. It ultimately selected CRYSTALS-KYBER for key encapsulation with security categories corresponding to AES-128, AES-192, and AES-256 equivalent strength levels, alongside CRYSTALS-Dilithium for digital signatures providing security margins against both classical attacks requiring 2^128 operations and quantum attacks utilizing 2^64 Grover iterations [8]. Transaction processing times measured across complete payment workflows show post-quantum cryptographic implementations require 45-85 milliseconds versus 28-42 milliseconds for traditional cryptographic methods. This indicates a performance overhead of 25-45% while remaining within established sub-100 millisecond service agreements. Testing of energy usage on mobile devices reveals 45–78 millijoules per operation for post-quantum signature processes versus 12–18 millijoules for ECDSA implementations. This causes 2.8–6.2% more battery drain for users making 50–200 transactions daily. However, specialized hardware optimizations provide 3.5–8.2x performance boosts that allow distributed systems to process 180,000–320,000 signatures per second.

TABLE IV
POST-QUANTUM ALGORITHM EVALUATION METRICS [7,8]

Performance Dimension	CRYSTALS-KYBER	CRYSTALS-Dilithium	SPHINCS+	Classical Baseline
Computational Overhead	Low	Moderate	High	Reference
Network Bandwidth Usage	Increased	Significantly Increased	Substantially Increased	Baseline
Storage Requirements	Moderate Increase	Large Increase	Variable Increase	Minimal
Mobile Device Impact	Acceptable	Manageable	Challenging	Optimal

V. IMPLEMENTATION CHALLENGES AND MITIGATION STRATEGIES

Implementing flexible cryptographic systems in live payment environments presents significant technical, operational, and institutional obstacles that require coordinated solutions across networks handling 400,000-1,200,000 transactions per second during peak global activity.

A. System Integration Challenges

System integration difficulties pose the primary challenge. Existing financial infrastructure depends on interconnected cryptographic functions built into numerous software modules across 15,000-50,000 system components. This necessitates synchronized updates among over 2,500 participating financial organizations. The Handbook of Applied Cryptography establishes that RSA key generation for 1024-bit moduli requires approximately 10^6 modular exponentiations, while 2048-bit keys demand 4×10^6 operations. This creates computational bottlenecks that intensify with post-quantum algorithms requiring modular arithmetic over polynomial rings of dimension 512-1024 with coefficients modulo primes of 12-14 bits [9].

B. Performance Optimization Solutions

Migration strategies focus on architectural decoupling through cryptographic abstraction layers, enabling algorithm separation from core business logic. Phased deployment approaches permit incremental upgrades over 18-36 month transition periods while maintaining 99.995% system availability equivalent to a maximum of 26.28 minutes annual downtime. Performance optimization

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

challenges arise from post-quantum algorithms requiring specialized implementation techniques. Number-theoretic transforms for lattice-based schemes achieve 3.5-7.2x performance improvements compared to generic implementations. Hardware acceleration using Intel SGX enclaves provides additional 2.8-5.4x speedups for signature generation operations requiring 10^5-10^7 clock cycles, depending on security parameters [9].

C. Interoperability and Key Management

Interoperability challenges emerge from maintaining seamless communication across heterogeneous environments encompassing x86-64 architectures, ARM processors, and Hardware Security Modules supporting various algorithm sets. Cryptography theory demonstrates that secure multiparty computation protocols require communication complexity of O(n^2) messages for n participants, creating scalability challenges for payment networks involving thousands of institutions [10]. Key management challenges intensify due to post-quantum key sizes ranging from 1,312-4,000 bytes compared to 64-256 bytes for classical implementations. This requires enhanced storage accommodating 50-200x increases across networks managing 100+ million user accounts. Automated lifecycle management handles key rotation cycles of 90-365 days, algorithm transitions spanning 12-24 months, and emergency revocation, completing within 15-30 minutes across global networks [10].

TABLE V
IMPLEMENTATION CHALLENGE CATEGORIES [9,10]

Challenge Type	Complexity Level	Mitigation Strategy	Timeline	Resource Requirements
Integration Complexity	High	Architectural Decoupling	Long-term	Substantial
Performance Optimization	Moderate	Hardware Acceleration	Medium-term	Specialized
Interoperability	High	Standardized Protocols	Extended	Coordinated
Regulatory Compliance	Moderate	Proactive Engagement	Ongoing	Documentation-Heavy

VI. CONCLUSION AND FUTURE WORK

Moving to quantum-resistant encryption methods marks a critical transformation in payment system infrastructure, demanding extensive collaboration among international financial networks while ensuring continuous operational availability. The developed cryptographic flexibility framework shows that quantum-resistant algorithms can be successfully incorporated into active payment platforms using structured system design, enhanced performance techniques, and thorough risk management approaches. The multi-layered system design allows financial organizations to operate various encryption methods simultaneously, supporting incremental transitions from traditional to quantum-resistant algorithms while maintaining operational effectiveness and meeting regulatory standards.

Testing results verify that contemporary quantum-resistant cryptographic methods, especially those based on lattice mathematics, can satisfy the demanding speed and capacity requirements of current payment platforms when appropriately configured and implemented within proper system architectures. The deployment difficulties documented in this investigation highlight the intricacies of extensive cryptographic system changes while showing that organized methodologies incorporating technological advancement, operational preparation, and regulatory cooperation can effectively

overcome these barriers. The combined cryptographic approach delivers crucial security assurances during transition phases, guaranteeing that payment platforms remain safeguarded against traditional and quantum-based attacks while retaining adaptability to accommodate developing encryption standards and security environments.

Financial organizations that actively adopt flexible cryptographic technologies will maintain their ability to provide secure, effective payment services during the quantum transformation period and afterward, protecting the dependability and trustworthiness of worldwide financial systems in the advancing quantum computing landscape.

Future Work

Future research should focus on hardware-accelerated implementations of these PQC algorithms within the Hardware Security Modules (HSMs) used by payment processors. Additional investigation is needed to quantify and mitigate the battery drain on mobile devices for users conducting a high volume of daily transactions. Finally, developing a scalable, automated key management and revocation protocol capable of operating across a network of over 100 million user accounts remains an open challenge requiring continued research and development efforts.

References

[1] William Newhouse, "Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum-Safe Cryptography," NIST, 2023. Available: https://csrc.nist.gov/pubs/sp/1800/38/iprd

[2] Dorit Aharonov, et al., "Interactive Proofs for Quantum Computations," arxiv, 2017, [Online]. Available: https://arxiv.org/abs/1704.04487

[3] D. Cooper, et al., "RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," ACM Digital Library, May 2008. [Online]. Available: https://dl.acm.org/doi/abs/10.17487/RFC5280

[4] Joppe Bos et al., "CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM," Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2017/634.pdf

[5] Mihir Bellare, Phillip Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," University of California, San Diego Computer Science and Engineering Technical Report, 1993. [Online]. Available: https://cseweb.ucsd.edu/~mihir/papers/ro.pdf

[6] Victor Shoup, "Sequences of games: a tool for taming complexity in security proofs," Victor Shoup, 2006. [Online]. Available: https://www.shoup.net/papers/games.pdf

[7] Jeffrey Hoffstein, et al., "NTRU: A ring-based public key cryptosystem," Springer Nature Link, 2006. [Online]. Available: https://link.springer.com/chapter/10.1007/BFb0054868

[8] National Institute of Standards and Technology, "Post-Quantum Cryptography," NIST, 2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[9] Alfred J. Menezes, et al., "Handbook of Applied Cryptography," The Swiss Bay. [Online]. Available: https://theswissbay.ch/pdf/Gentoomen%20Library/Cryptography/Handbook%20of%20Applied%20Cryptography%20-%20Alfred%20J.%20Menezes.pdf

[10] Kenneth H. Rosen, "Cryptography: Theory and Practice," 3rd ed., Sultan Almuhammadi, 2003. [Online]. Available: https://almuhammadi.com/sultan/crypto_books/Stinson.3ed.pdf