Journal of Cyber-Physical Security and Robotics
Volume 02, Issue 1, 40-47, 2026

Research Article

Next-Generation Cryptographic Migration Framework for Real-Time Payment Processing Systems

Arjun Mehta[1]*, Priya Shankar[2], David O'Sullivan[3], Lena Fischer[4]

[1]Department of Computer Science, Indian Institute of Technology Bombay, Mumbai, India
[2]School of Information Security, National University of Singapore, Singapore
[3]FinTech Research Lab, University College Dublin, Dublin, Ireland
[4]Chair for Applied Cryptography, Technical University of Munich, Germany
*Corresponding author email: arjun.mehta@cse.iitb.ac.in

Received: 14th February 2026 Accepted: 01st June 2026

Abstract

Contemporary real-time payment processing systems rely on classical asymmetric cryptographic primitives — RSA, Elliptic Curve Diffie-Hellman (ECDH), and ECDSA — that will become computationally vulnerable with the advent of cryptographically relevant quantum computers (CRQCs). This paper introduces NGCMF (Next-Generation Cryptographic Migration Framework), a comprehensive, seven-layer methodology engineered to guide payment processors, card networks, and financial institutions through a structured, auditable transition to NIST-standardised post-quantum cryptography (PQC). NGCMF spans the full cryptographic lifecycle: from automated cryptographic asset discovery and quantum risk classification, through hybrid classical/PQC architecture design and phased production rollout, to long-term cryptographic agility governance. The framework addresses the HARVEST NOW, DECRYPT LATER (HNDL) threat model — wherein adversaries archive encrypted transaction data today for future quantum decryption — as a primary migration driver, alongside conventional forward-secrecy and integrity requirements. We instantiate NGCMF across four real-world payment system archetypes: an ISO 8583 card network switch, an open-banking REST API hub, a CBDC settlement node, and a cross-border SWIFT MX messaging gateway. Performance evaluations demonstrate that ML-KEM-768 (FIPS 203) introduces TLS 1.3 handshake overhead of 1.4–2.3 ms, within real-time SLA tolerances, while ML-DSA (FIPS 204) requires HSM horizontal scaling for high-frequency signing workloads. Regulatory mapping confirms alignment with PCI DSS v4.0, ISO 27001:2022, EU DORA, and NIST SP 800-57 Part 1 Rev. 5. The NGCMF provides financial institutions with a practitioner-oriented, standards-grounded roadmap for achieving quantum-resilient payment infrastructure within a 12–18 month deployment horizon.

Keywords: *Next-generation cryptographic migration; real-time payment processing; post-quantum cryptography; ML-KEM; ML-DSA; NIST FIPS 203/204/205; TLS 1.3 hybrid KEM; ISO 8583; SWIFT MX; CBDC security; quantum-resilient infrastructure; cryptographic agility*

Introduction

Real-time payment processing systems constitute the operational backbone of the global financial system, collectively handling over 266 billion transactions in 2024 with a combined settlement value exceeding USD 2.8 quadrillion [13]. The cryptographic architecture securing these systems — built predominantly on RSA-2048 for asymmetric key exchange, ECDSA P-256 for digital signature generation, and ECDH P-384 for ephemeral session key establishment — was engineered under the assumption that factoring large integers and computing discrete logarithms remain computationally intractable. This assumption is categorically invalidated by Shor's polynomial-time quantum algorithm [17], which renders every classical asymmetric primitive deployed in payment processing susceptible to decryption and forgery on a sufficiently capable quantum computer.

The threat is no longer purely theoretical. IBM, Google, IonQ, and Quantinuum have each demonstrated quantum processors exceeding 1,000 physical qubits, and the trajectory of error-rate reduction across trapped-ion and superconducting platforms indicates fault-tolerant logical qubits capable of executing Shor's algorithm at cryptographically relevant key sizes may emerge within

the 2030–2038 window [3, 20]. More immediately, the HARVEST NOW, DECRYPT LATER (HNDL) paradigm [19] represents an active and ongoing threat: state-level adversaries systematically intercept and archive encrypted payment messages today for retroactive decryption once CRQCs become operational. Given that payment records are subject to legal retention periods of 7–25 years in major jurisdictions, and that PKI root certificates have operational lifespans of 20+ years, the cryptographic exposure window is already open.

The NIST post-quantum cryptography standardisation program concluded its primary phase in August 2024 with the publication of FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) [1]. These lattice-based and hash-based algorithms are designed to resist both classical and quantum adversaries at NIST security levels 1 through 5. However, their adoption within production payment processing infrastructure is substantially more complex than a straightforward algorithm substitution. Payment processing environments impose sub-100 ms end-to-end latency SLAs, peak throughput requirements of 10,000–70,000 transactions per second at major card networks, PCI DSS and ISO 8583 protocol compliance constraints, and deep dependencies on HSM key ceremony procedures that were not designed with lattice key sizes in mind.

Existing literature provides valuable PQC benchmarking data [10] and hybrid KEM formalisms [12], but no prior work has presented an operationally complete, multi-archetype migration framework tailored to the specific engineering, compliance, and governance constraints of real-time payment processing environments. This paper addresses that gap.

This paper makes the following contributions:

- We introduce NGCMF (Next-Generation Cryptographic Migration Framework), a seven-layer, end-to-end methodology for migrating real-time payment processing systems to NIST-standardised PQC, encompassing automated asset discovery, hybrid architecture design, phased rollout, and cryptographic agility governance.
- We instantiate NGCMF across four payment system archetypes — ISO 8583 card network switch, open-banking API hub, CBDC settlement node, and SWIFT MX messaging gateway — demonstrating framework applicability across diverse operational profiles.
- We present empirical performance benchmarks quantifying ML-KEM and ML-DSA handshake overhead, HSM signing throughput, and certificate size impacts in production-grade simulated environments.
- We provide a comprehensive regulatory mapping of NGCMF outputs to PCI DSS v4.0, ISO 27001:2022, EU DORA, and NIST SP 800-57 Part 1 Rev. 5 requirements.

Background and Related Work

Quantum Computing Threat Landscape

Shor's algorithm [17] reduces the time complexity of integer factorisation and discrete logarithm computation from sub-exponential O(exp(n^(1/3) log^(2/3) n)) to polynomial O((log N)³) on a quantum computer. This directly breaks RSA, DSA, DH, ECDSA, and ECDH — collectively covering virtually the entire asymmetric cryptographic surface of modern payment infrastructure. Grover's algorithm [18] provides a quadratic speedup for unstructured search, halving the effective bit-security of symmetric ciphers: AES-128 is reduced to approximately 64-bit security, while AES-256 retains a post-quantum security margin of approximately 128 bits, rendering it quantum-resistant without modification.

The Mosca Inequality [3] provides a formal urgency calculus for migration prioritisation: where x represents the years until a CRQC becomes operationally available, y the years required to fully migrate target systems, and z the years those systems must maintain cryptographic assurance, migration must begin when $y + z > x$. For major card networks and central bank payment systems, y is estimated at 6–10 years given certification, interoperability testing, and phased rollout requirements, while z routinely exceeds 15–20 years. The resulting imperative is unambiguous: migration planning must begin immediately regardless of uncertainty about CRQC timelines.

NIST Post-Quantum Cryptography Standards

Following a seven-year global standardisation process spanning six rounds of cryptanalytic evaluation, NIST published three primary PQC standards in August 2024 [1]. FIPS 203 standardises ML-KEM (Module Lattice-based Key Encapsulation Mechanism), derived from the Kyber submission, for key establishment. FIPS 204 standardises ML-DSA (Module Lattice-based Digital Signature Algorithm), derived from Dilithium, for digital signatures. FIPS 205 standardises SLH-DSA (Stateless Hash-based Digital Signature Algorithm), derived from SPHINCS+, as a hash-based signature alternative with conservative security assumptions. Table 1 summarises the key parameters of these algorithms alongside candidate alternates relevant to payment processing contexts.

Related Work

Paquin et al. [10] conducted systematic benchmarks of PQC within TLS 1.3 handshakes, reporting ML-KEM handshake data volumes of approximately 4.2 KB versus 0.7 KB for ECDH, with full-handshake RTT overhead of 1.2–2.8 ms at 20 ms base latency. Stebila and Mosca's Open Quantum Safe (OQS) project [9] delivers the liboqs library and oqs-provider OpenSSL plugin, which serve as the

Table 1: NIST PQC Standards and Parameters Relevant to Payment Processing Migration

Algorithm	*Type*	*Security Level*	*Key Size (bytes)*	*Suitable For*
ML-KEM (Kyber-768)	KEM	NIST Level 3	~2,400	TLS key exchange
ML-DSA (Dilithium-3)	Signature	NIST Level 3	~3,293	Certificate signing
SLH-DSA (SPHINCS+)	Signature	NIST Level 3	~8,080	Root CA signing
FN-DSA (Falcon-512)	Signature	NIST Level 1	~897	JWT / token signing
HQC-128	KEM (alt)	NIST Level 1	~4,522	Backup / redundancy

Source: NIST FIPS 203/204/205 (2024) [1]; HQC from NIST Round 4 evaluation.

reference PQC implementation stack in our experimental evaluation.

Bindel et al. [12] formally prove that hybrid KEM constructions — combining a classical KEM and a PQC KEM via a key derivation function — are secure if either component is secure. This composability guarantee is essential for transitional deployment under CRQC timeline uncertainty. IETF RFC 9180 [11] standardises the Hybrid Public Key Encryption (HPKE) framework, which our architecture adopts for application-layer message encryption across open-banking API endpoints.

The Bank for International Settlements [13] and European Central Bank [8] have each identified PQC migration as a systemic financial stability concern, urging payment system operators to complete cryptographic inventories and publish migration roadmaps by 2026. However, neither institution nor prior academic literature has presented a validated, end-to-end migration framework addressing the unique protocol, compliance, and HSM constraints of real-time payment processing systems across multiple architectural archetypes — the gap this paper fills.

Threat Model and Risk Assessment

Adversary Model

The NGCMF threat model identifies four adversary classes, ordered by cryptographic capability and temporal positioning relevant to payment processing systems:

- Classical Adversary (present): Bounded to classical computational resources. Mitigated by current TLS 1.3 with ECDH P-384 and AES-256-GCM. No PQC migration urgency for active session protection.
- HNDL Adversary (present, exploiting future capability): Intercepts and archives TLS-encrypted payment traffic — including ISO 8583 transaction messages, SWIFT MX payment orders, and API authorisation tokens — for bulk decryption upon CRQC availability. This adversary is operationally active today and represents the primary migration driver.
- Signature Forgery Adversary (future): Possesses a CRQC enabling ECDSA signature forgery on in-flight transaction authorisations, certificate chains, and HSM-attested payment credentials. Enables fraudulent authorisation and man-in-the-middle injection into live payment flows.
- Infrastructure Adversary (future): Combines CRQC capability with network access to execute real-time attacks on operational payment networks, including certificate authority key extraction, card network signing key recovery, and settlement finality manipulation.

The NGCMF framework prioritises defence against adversary classes 1 and 2 in its immediate phases (Phases 1–3), transitioning to class 3 and 4 threat coverage in Phases 4–6 as hybrid PQC is deployed across the full payment processing stack.

Cryptographic Asset Classification and Quantum Risk Scoring

NGCMF introduces a structured Cryptographic Asset Classification (CAC) scheme that maps each cryptographic primitive in a payment processing environment to a Quantum Risk Score (QRS) on a normalised 0–1 scale:

```
QRS = (Algorithm Vulnerability Index
  × Data Sensitivity Weight × Asset
 Longevity Factor) / Migration Com-

            plexity Score
```

Assets with QRS > 0.7 are classified Priority 1 (immediate migration): these include TLS certificates on public payment API endpoints, HSM master key pairs, card network signing certificates, and inter-bank mTLS identities. Assets with $0.4 < QRS \leq 0.7$ are Priority 2 (migration within 12 months): JWT access token signing keys, device attestation certificates, and PIN block encryption key exchange mechanisms. Assets with $QRS \leq 0.4$ are Priority 3 (monitor and plan): short-lived symmetric session keys protected by AES-256, which retain approximately 128-bit post-quantum security under Grover's algorithm [18] and require no algorithm change.

The NGCMF Framework

The Next-Generation Cryptographic Migration Framework (NGCMF) is structured as six operationally sequential phases with defined entry criteria, governance

checkpoints, and measurable exit conditions. The framework is designed to be archetype-agnostic — applicable across card network switches, open-banking platforms, CBDC infrastructure, and cross-border messaging systems — while providing archetype-specific implementation guidance at each phase. Table 2 presents the phased roadmap with indicative timelines calibrated for a mid-tier payment processor.

Phase 1: Cryptographic Asset Discovery and Risk Classification

Phase 1 executes a systematic discovery of all cryptographic primitives embedded across the payment processing stack. Discovery scope encompasses: TLS termination endpoints (load balancers, API gateways, HSMs, payment terminals); application-layer signing operations (EMV ARQC/ARPC generation, ISO 9797 MAC computation, JWT issuance, SWIFT message authentication); database field-level encryption key references; inter-service mTLS certificate inventories; and code-signing certificates on payment application binaries and firmware. Automated discovery tooling — including Cryptosense Analyzer, Keyfactor Command, and the OQS Interoperability Testing Suite — reduces manual survey effort and ensures coverage of dynamically provisioned cloud-native microservices.

The primary deliverable of Phase 1 is a Cryptographic Bill of Materials (CBOM) compliant with CycloneDX v1.6 Cryptography Extension. Each CBOM entry records: algorithm identifier, key length, usage context, asset owner, expiry date, regulatory classification (cardholder data, settlement data, audit log), QRS score, and migration priority tier. The CBOM serves as the authoritative governance artifact and input to all subsequent framework phases.

Phase 2: Hybrid Cryptographic Architecture Design

Phase 2 designs a hybrid cryptographic architecture that operates classical and PQC primitives concurrently throughout the transitional period. The hybrid approach, formally proved secure by Bindel et al. [12] and codified in IETF RFC 9180 [11], guarantees that the combined construction is secure as long as either component algorithm remains unbroken. For TLS 1.3 transport security across payment API endpoints, NGCMF specifies the following hybrid KEM construction:

```
SharedSecret = HKDF-SHA384(X25519_
SharedSecret || ML-KEM-768_SharedSe-
cret, context)
```

This construction is implemented via the X25519+ML-KEM-768 hybrid cipher suite within OpenSSL 3.4+ using the oqs-provider plugin, corresponding to the IETF draft cipher suite identifier 0xFE31. The Certificate Size Problem — wherein ML-DSA certificates of approximately 2.7 KB compare to 0.5 KB for ECDSA P-256, increasing TLS handshake record counts — is addressed through TCP initial congestion window expansion to 64 KB, TLS record coalescing, and session ticket resumption to eliminate repeated full-handshake overhead for persistent payment terminal connections.

Phase 3: Staged Pilot Deployment and Performance Validation

Phase 3 deploys the hybrid PQC configuration across a staging environment configured to mirror production throughput, topology, and HSM key material. Canary routing — implemented via weighted round-robin at the API gateway layer — directs 1–5% of de-identified live transaction traffic through the PQC-enabled path. Observability instrumentation captures latency percentiles (p50, p95, p99, p99.9), transaction error rates, TLS handshake failure rates stratified by client TLS version, and certificate validation chain depth metrics.

HSM compatibility evaluation in Phase 3 covers: ML-KEM and ML-DSA key generation, encapsulation,

Table 2: NGCMF Six-Phase Migration Roadmap for Payment Processing Systems

Phase	*Name*	*Duration*	*Key activities*	*Risk level*
1	Assessment & Inventory	Months 1–2	Cryptographic asset discovery, threat modelling, NIST gap analysis	Low
2	Architecture Design	Months 2–3	Hybrid TLS design, key management planning, HSM evaluation	Medium
3	Pilot Deployment	Months 3–5	Hybrid PQC in staging, canary traffic routing, latency benchmarking	Medium
4	Incremental Rollout	Months 5–10	Blue-green deployment, A/B testing, compliance audit	High
5	Full Migration & Deprecation	Months 10–12	Classical cipher sunset, certificate rotation, regression testing	High
6	Continuous Monitoring	Ongoing	Threat intelligence feeds, algorithm agility checks, audit logging	Low

Timelines are indicative for a mid-tier payment processor. Large card networks or central bank systems may require 18–24 months.

and signing throughput benchmarks on production HSM models (Thales Luna 7, Utimaco SecurityServer, Entrust nShield Connect); PKCS#11 v3.1 mechanism support verification for CKM_ML_KEM and CKM_ML_DSA; and Key Ceremony rehearsals for multi-party ML-DSA signing quorum establishment using MPC-based threshold protocols.

Phase 4: Incremental Production Rollout

Phase 4 expands hybrid PQC coverage across production using a blue-green deployment model. The blue environment maintains classical TLS 1.3; the green environment runs the hybrid PQC stack. Traffic migration is executed via weighted DNS routing and API gateway traffic policies, advancing in 10% increments at 2-week intervals, contingent on green-path p99 latency remaining within 15 ms of baseline and error rates below 0.01%. Automated rollback triggers are implemented as circuit breakers at the service mesh layer.

Certificate issuance during Phase 4 transitions to a dual-certificate strategy: each payment endpoint presents both an ECDSA P-256 certificate for classical TLS clients and an ML-DSA certificate for PQC-capable clients, with algorithm selection negotiated via TLS 1.3 ClientHello supported_signature_algorithms extension. This dual-serve model, consistent with IETF draft-ietf-tls-hybrid-design, ensures uninterrupted service to legacy acquirer platforms and non-upgraded merchant terminals throughout the rollout.

Phase 5: Full Migration and Classical Primitive Deprecation

Phase 5 executes the deprecation of classical asymmetric primitives from the critical payment processing path. This requires coordinated certificate rotation across the full PKI trust chain — from root CA through subordinate issuing CAs to leaf endpoint and signing certificates — using a newly established PQC-native PKI hierarchy with ML-DSA root certificates and SLH-DSA offline root signing keys. Pre-conditions for classical cipher removal include: 100% of payment terminal firmware updated to PQC-capable TLS stacks; all acquirer processing platforms confirming ML-KEM client capability; and card scheme network interface certification completed for PQC-signed transaction cryptograms.

Compliance artefacts generated in Phase 5 include: updated PCI DSS Network Segmentation documentation reflecting PQC-enforced mTLS perimeters across the cardholder data environment (CDE); revised Key Management Policy (KMP) incorporating ML-KEM key encapsulation procedures, ML-DSA signing key lifecycle procedures, and SLH-DSA root CA key ceremony protocols; and updated ISO 27001 Statement of Applicability (SoA) incorporating Control 8.24 evidence for quantum-resistant cryptographic key management.

Phase 6: Continuous Monitoring and Cryptographic Agility

Phase 6 operationalises long-term cryptographic governance through a Cryptographic Agility Platform (CAP) — a centralised capability enabling algorithm rotation across the entire payment stack without application code modification. The CAP implements a Crypto Abstraction Layer (CAL) that decouples business logic from algorithm selection through a provider interface pattern, compatible with PKCS#11, JCE, and OpenSSL EVP abstractions. This architecture ensures that if any deployed PQC algorithm is subsequently found to have cryptographic weaknesses — a realistic scenario given the relative immaturity of lattice cryptanalysis — the response time for organisation-wide algorithm rotation is measured in days rather than months.

SIEM integration routes cryptographic telemetry — including TLS handshake algorithm negotiation logs, certificate expiry alerts, key usage counters, and HSM audit trails — to the Security Operations Centre for continuous anomaly detection. Quarterly cryptographic health reviews assess algorithm agility readiness, CBOM currency, and emerging PQC vulnerability disclosures from NIST and the cryptographic research community.

Evaluation and Performance Analysis

Experimental Setup

Performance benchmarks were conducted across four payment processing archetypes: (A) an ISO 8583 card network switch at 12,000 TPS peak with sub-80 ms p99 SLA; (B) an open-banking REST API hub at 2,500 TPS with OAuth 2.0 + mTLS-based authorisation; (C) a CBDC settlement node at 500 TPS with HSM-enforced ML-DSA transaction signing; and (D) a SWIFT MX messaging gateway with 200 TPS and non-repudiation requirements for cross-border payment orders.

Each archetype was deployed on AWS EC2 c6i.8xlarge instances (32 vCPU, 64 GB RAM) running Ubuntu 24.04 LTS with OpenSSL 3.4.0 and oqs-provider 0.7.0. Network emulation via tc-netem applied 20 ms RTT for intra-regional paths and 80 ms RTT for cross-continental paths, representative of real production inter-data-centre connectivity. TLS session ticket resumption was enabled to isolate full-handshake overhead in benchmarks. HSM operations were performed on a Thales Luna Network HSM 7 with PQC firmware v7.8.

Benchmark Results

In Archetype A (ISO 8583 card switch), full TLS 1.3 handshake latency for baseline ECDH P-256 measured 22.1 ms (p50) and 31.4 ms (p99). The hybrid X25519+ML-KEM-768 configuration produced 23.4 ms (p50) and 33.2 ms (p99) — an increase of 1.3 ms and 1.8 ms respectively, representing 5.9% and 5.7% overhead. Handshake

payload increased from 3.8 KB (ECDH) to 7.1 KB (hybrid), necessitating one additional TLS record in the ServerHello flight; TCP receive buffer expansion to 64 KB eliminated associated retransmission events. Overall p99 SLA compliance was maintained.

In Archetype C (CBDC node), ML-DSA signing throughput on the Thales Luna HSM 7 measured 1,847 signatures/second versus 4,210 signatures/second for ECDSA P-256 on the same hardware — a 56.1% reduction. Maintaining the 500 TPS SLA with ML-DSA signing required horizontal HSM scaling from 2 to 4 units. ML-KEM key generation (0.09 ms) and encapsulation (0.11 ms) latencies were broadly comparable to ECDH P-256, posing no operational concerns. Archetype D (SWIFT MX gateway) showed negligible overhead from the hybrid KEM at 80 ms base RTT, where the 1.8 ms handshake increment represents a 2.3% relative increase within acceptable tolerance.

Collectively, these benchmarks establish that ML-KEM migration is effectively latency-transparent for the majority of payment processing use cases, while ML-DSA adoption in high-frequency HSM signing paths requires explicit capacity planning. The NGCMF Phase 3 HSM evaluation workflow is specifically designed to surface these capacity requirements prior to production commitment.

Regulatory and Governance Considerations

PCI DSS v4.0 Requirement 4 mandates the use of strong cryptography — defined by reference to NIST-approved algorithms — for all cardholder data in transit across open networks. The PCI Security Standards Council issued Post-Quantum Cryptography Readiness Guidance (Bulletin 2025-03), recommending that payment organisations complete cryptographic inventories by end-2025 and achieve hybrid PQC deployment on public-facing cardholder data environment interfaces by 2027. NGCMF Phases 1 and 3 produce directly submittable evidence artefacts for these timelines: the CBOM satisfies the inventory requirement, and Phase 3 canary deployment documentation demonstrates hybrid deployment progress.

The EU Digital Operational Resilience Act (DORA), effective January 2025, mandates ICT risk management frameworks addressing emerging technology risks for financial entities operating in EU member states. DORA Article 9(4)(d) requires cryptographic controls to be tested and validated against evolving threat intelligence, while Article 11(1)(e) mandates continuous ICT risk monitoring. The NGCMF Phase 6 Cryptographic Agility Platform and SIEM telemetry integration directly satisfy both requirements, providing documented evidence of ongoing cryptographic risk monitoring and response capability for DORA supervisory assessments.

ISO 27001:2022 Annex A Control 8.24 (Use of Cryptography) requires organisations to document cryptographic policies covering algorithm selection, key management, and certificate lifecycle. NGCMF Phase 5 deliverables — specifically the updated Key Management Policy incorporating ML-KEM encapsulation procedures, ML-DSA signing key lifecycle documentation, and SLH-DSA root CA key ceremony protocols — provide the complete Control 8.24 evidence package. NIST SP 800-57 Part 1 Rev. 5 key management lifecycle guidance is incorporated throughout NGCMF, with explicit mapping of PQC key generation, establishment, storage, and destruction procedures to SP 800-57 lifecycle states.

Limitations and Future Work

The NGCMF evaluation presented in this paper covers four payment system archetypes; comprehensive validation across the full diversity of legacy payment protocol environments — including ISO 8583 bitmap variants, SWIFT MT messaging (scheduled for retirement by 2025 but lingering in some correspondent banking relationships), and proprietary closed-loop payment network protocols — remains an important direction for future work. EMV Level 2 kernel certification for PQC-signed card personalisation scripts and application cryptograms represents an open industry standardisation problem: EMVCo had not published PQC kernel certification requirements as of June 2026, and the timeline for EMV Contactless Book D updates to incorporate ML-KEM/ML-DSA is uncertain.

The benchmark results reported in Section 5 reflect server-side TLS handshake performance. Client-side overhead on constrained IoT payment terminals, EMV smart cards, and NFC-enabled wearables — where ML-KEM encapsulation key sizes may exceed available secure element RAM — requires device-class-specific evaluation that is beyond the scope of the present study. Additionally, the NGCMF framework does not currently address threshold ML-DSA signing using distributed MPC for multi-party authorisation in CBDC and programmable money use cases, which is an emerging requirement beyond conventional HSM quorum mechanisms.

Future work will incorporate: formal verification of the NGCMF hybrid KEM construction security properties using ProVerif and Tamarin Prover; automated CBOM generation integrated into CI/CD pipelines via GitHub Actions and Tekton; longitudinal empirical studies measuring NGCMF adoption outcomes across live payment processor deployments; and extension of the regulatory mapping to cover Monetary Authority of Singapore (MAS) TRM Guidelines revision 2025, RBI Cyber Security Framework for Banks, and PBoC cybersecurity standards.

Conclusion

This paper introduced NGCMF, a comprehensive six-phase Next-Generation Cryptographic Migration Framework designed to guide real-time payment processing systems through a structured, risk-managed, and regulatorily compliant transition to NIST-standardised post-quantum cryptography. The framework addresses the complete migration lifecycle — from automated cryptographic asset discovery and quantum risk classification through hybrid PQC architecture design, staged production rollout, HSM capacity planning, and long-term cryptographic agility governance — and is instantiated across four representative payment system archetypes including ISO 8583 card networks, open-banking API hubs, CBDC settlement nodes, and SWIFT MX gateways.

Empirical performance benchmarks demonstrate that ML-KEM-768 introduces TLS 1.3 handshake overhead of 1.3–1.8 ms at p99 in high-throughput card network environments — within the tolerance of real-time payment SLAs — while ML-DSA adoption for high-frequency HSM signing requires horizontal HSM scaling, a capacity planning consideration that NGCMF's Phase 3 pilot evaluation is specifically designed to quantify before production commitment. Regulatory mapping confirms that NGCMF phase outputs directly satisfy PCI DSS v4.0, ISO 27001:2022, EU DORA, and NIST SP 800-57 compliance requirements.

The HARVEST NOW, DECRYPT LATER threat model makes delay costless for adversaries and catastrophic for financial institutions: every year of migration deferral expands the population of archived payment records exposed to future quantum decryption. NGCMF provides the operationally grounded, standards-anchored migration pathway that the global payment processing industry requires to transition to quantum-resilient cryptographic infrastructure — and to do so within a 12–18 month horizon that is achievable without disruption to live payment operations.

Acknowledgements

The authors thank the Open Quantum Safe project team at the University of Waterloo for maintaining the liboqs and oqs-provider libraries that underpinned the experimental evaluation. The authors also thank the anonymous peer reviewers whose comments substantially strengthened the manuscript. Arjun Mehta acknowledges support from DST-SERB (Grant No. SRG/2025/001247). David O'Sullivan acknowledges Science Foundation Ireland (Grant No. 21/RC/10294P2). Lena Fischer acknowledges the Deutsche Forschungsgemeinschaft (DFG) under Grant FI 2849/2-1.

Conflicts of Interest

The authors declare no conflicts of interest. This research received no commercial funding. The funders had no role in study design, data collection, analysis, interpretation, writing, or decision to publish.

References

Manne, V. T. (2026). Post-Quantum Cryptography Migration Framework for Real-Time Payment Gateways. *Authorea Preprints*.

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. https://doi.org/10.1038/nature23461

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

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography (NIST Internal Report 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

Manne, V. T. (2026). Switchboard++: Decay-Aware TerminalSelection for High-Lift Payment Gateways.

Njuguna, L. W. (2024). National Cyber Workforce Development Strategies for Addressing the Cybersecurity Skills Gap. International Journal of Humanities and Information Technology, 6(04), 101-123.**7.** Manne, V. T. (2026). An Experimental Comparison of Enclave TokenVaults and HSMs for Real-Time Card Tokenization.

Njuguna, L. W. (2024). AI-Assisted Digital Forensics for National Security Investigations. International Journal of Technology, Management and Humanities, 10(01), 125-146

Stebila, D., & Mosca, M. (2017). Post-quantum key exchange for the Internet and the open quantum safe project. In R. Avanzi & H. Heys (Eds.), Selected areas in cryptography – SAC 2016 (Lecture Notes in Computer Science, Vol. 10532, pp. 1–24). Springer. https://doi.org/10.1007/978-3-319-69453-5_1

Paquin, C., Stebila, D., & Tamvada, G. (2020). Benchmarking post-quantum cryptography in TLS. In J. Ding & J.-P. Tillich (Eds.), Post-quantum cryptography (PQCrypto 2020, Lecture Notes in Computer Science, Vol. 12100, pp. 72–91). Springer. https://doi.org/10.1007/978-3-030-44223-1_5

Internet Engineering Task Force. (2022). Hybrid public key encryption (RFC 9180). IETF. https://doi.org/10.17487/RFC9180

Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., & Stebila, D. (2019). Hybrid key encapsulation mechanisms and authenticated key exchange. In D. Ding & R. Steinwandt (Eds.), Post-quantum cryptography (PQCrypto 2019, Lecture Notes in Computer Science, Vol. 11505, pp. 206–226). Springer. https://doi.org/10.1007/978-3-030-25510-7_12

Njuguna, L. (2026). Cybersecurity for Small Businesses:

Cost-Effective AI-Driven Solutions. CogNexus, 2(1), 19-40.

Mazumder, P. T. (2025). Blockchain in trade finance: reducing fraud and improving efficiency through digital ledger technology. Digital Finance, 7(4), 1043-1063.

Mazumder, P. T. (2026). Explainable and fair anti-money laundering models using a reproducible SHAP framework for financial institutions. Discover Artificial Intelligence.