International Journal of Advance Industrial Engineering
E-ISSN 2320–5539

Available at http://ijaie.com/

Research Article

Enhancing Payment Gateway Security Through a Post-Quantum Cryptography Migration Framework

Janardan Jacob*

Software Development Engineer, Amazon Inc., USA

Vol. 14, No. 1 (2026)

Abstract

Payment gateways are the critical cryptographic chokepoints of the global digital economy, yet the RSA, ECDSA, and ECDH primitives securing them are susceptible to Shor's algorithm on a cryptographically relevant quantum computer (CRQC). This paper presents the Enhanced Payment Gateway Post-Quantum Migration Framework (EPQMF), a structured seven-phase methodology designed to guide payment service providers and financial institutions through a comprehensive, risk-managed transition to NIST-standardised post-quantum cryptography (PQC). The framework spans the complete migration lifecycle: automated cryptographic asset discovery and quantum risk classification; hybrid classical/PQC architecture design incorporating ML-KEM-768 and ML-DSA-65; phased production rollout using blue-green deployment and dual-certificate strategies; hardware security module (HSM) compatibility planning; and long-term cryptographic agility governance. Empirical performance evaluations demonstrate that ML-KEM-768 introduces TLS 1.3 handshake overhead of 1.4–2.2 ms — within real-time payment SLA tolerances — while ML-DSA-65 signing requires HSM horizontal scaling for high-frequency workloads. The HARVEST NOW, DECRYPT LATER (HNDL) threat model is addressed as the primary migration driver, establishing that migration must commence immediately regardless of CRQC timeline uncertainty. Regulatory alignment with PCI DSS v4.0, ISO/IEC 27001:2022, and the EU Digital Operational Resilience Act (DORA) is embedded across all framework phases. The EPQMF provides practitioners with a standards-grounded, operationally validated migration pathway achievable within a 9-month deployment horizon.

Keywords: *post-quantum cryptography; payment gateway security; ML-KEM; ML-DSA; NIST FIPS 203/204; TLS 1.3; PCI DSS v4.0; quantum-resistant cryptography*

Introduction

Digital payment gateways processed over 266 billion transactions globally in 2024, underpinning commerce valued at more than USD 2.8 quadrillion (Bank for International Settlements, 2024). The cryptographic architecture securing these transactions — built on RSA-2048 for asymmetric key exchange, ECDSA P-256 for digital signatures, and ECDH P-384 for ephemeral session key establishment — has proven resilient against classical computational adversaries for decades. However, the maturation of quantum computing platforms now threatens the mathematical hardness assumptions upon which these primitives depend.

Shor (1997) demonstrated that a quantum computer can factorise large integers and solve discrete logarithm problems in polynomial time, directly invalidating RSA, ECDSA, and ECDH security guarantees. Grover (1996) further showed that symmetric cipher security is halved under quantum search, requiring AES-256 rather than AES-128 for adequate quantum resistance. The combined implication for payment infrastructure is severe: a sufficiently capable cryptographically relevant quantum computer (CRQC) could forge transaction authorisations, decrypt inter-bank settlement messages, and extract private keys from payment terminals and card network signing systems.

The HARVEST NOW, DECRYPT LATER (HNDL) threat model identifies an immediate, ongoing risk independent of CRQC availability: state-level and well-resourced adversaries intercept and archive encrypted payment traffic today for decryption once CRQCs become operational, expected between 2030 and 2038 (Mosca, 2018; World Economic Forum, 2023). Given that payment records carry legal retention periods of 7–25 years and that root CA certificates have 20-year operational lifespans, the exposure window is already open.

*Author for Correspondence: janardanjacsrmu@gmail.com

The National Institute of Standards and Technology (NIST) addressed this threat through a seven-year global standardisation program, culminating in the August 2024 publication of FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) — three post-quantum cryptographic standards resistant to both classical and quantum adversaries (NIST, 2024a, 2024b, 2024c). However, deploying these standards within production payment gateway environments presents profound engineering challenges: sub-100 ms latency SLAs, throughput requirements of thousands of transactions per second, PCI DSS compliance obligations, and HSM key management ecosystems that were not designed with lattice key sizes in mind.

This paper addresses the gap between PQC standardisation and practical payment gateway migration. We introduce the Enhanced Payment Gateway Post-Quantum Migration Framework (EPQMF), providing financial institutions and payment service providers with a structured, evidence-based migration pathway aligned to NIST, PCI DSS v4.0, and ISO/IEC 27001:2022 requirements.

Literature Review

Quantum Computing and Cryptographic Vulnerability

The theoretical foundation for quantum-era cryptographic risk was established by Shor (1997), whose algorithm reduces RSA and elliptic-curve-based cryptosystem security from exponential to polynomial time complexity on a quantum computer. Bernstein and Lange (2017) provided a comprehensive survey of post-quantum cryptographic proposals, categorising candidate approaches by mathematical hardness family and assessing their resistance to both classical and quantum attacks. Mosca (2018) formalised the migration urgency calculus — the Mosca Inequality — demonstrating that organisations whose systems must remain secure for z years and require y years to migrate must begin migration when y + z exceeds the estimated years until a CRQC becomes available.

Chen et al. (2016) established the NIST evaluation framework for PQC candidates, identifying four primary mathematical families: lattice-based, code-based, multivariate, and hash-based constructions. The subsequent Alagic et al. (2020) second-round status report narrowed the candidate set and established the performance and security benchmarks that ultimately led to the 2024 final standards. Jao and De Feo (2011) proposed isogeny-based cryptography as an additional candidate; however, the SIKE isogeny scheme was broken in 2022, illustrating the importance of ongoing cryptanalytic vigilance for deployed PQC systems.

Post-Quantum Standards and Implementation

The three NIST-finalised standards (NIST, 2024a, 2024b, 2024c) provide standardised interfaces for key encapsulation and digital signature operations. Paquin et al. (2020) conducted systematic benchmarks of PQC algorithms within TLS 1.3 handshakes, reporting ML-KEM handshake data volumes of approximately 4.2 KB versus 0.7 KB for ECDH, with RTT overhead of 1.2–2.8 ms — findings that directly inform our performance evaluation methodology.

Stebila and Mosca (2017) developed the Open Quantum Safe (OQS) project and liboqs library, providing the reference PQC implementation stack that enables experimental and production PQC deployments in OpenSSL. Bindel et al. (2019) formally proved that hybrid KEM constructions — combining classical and PQC KEMs via a key derivation function — are secure if either component is secure, establishing the theoretical basis for the transitional hybrid approach adopted in the EPQMF. IETF RFC 9180 (2022) standardised the Hybrid Public Key Encryption (HPKE) framework, providing the composable API-layer message encryption mechanism used in the framework's open-banking integration layer.

Financial Sector Quantum Risk and Regulatory Context

The Bank for International Settlements (2024) identified PQC migration as a systemic financial stability concern, recommending that payment system operators complete cryptographic inventories by 2025 and publish quantum risk mitigation roadmaps by 2026. The European Central Bank (2023) noted that the unique characteristics of financial infrastructure — long operational lifespans, regulatory retention requirements, and multi-party trust chains — amplify the HNDL threat beyond other sectors. Payment Card Industry Security Standards Council (2022) v4.0 requirements mandate NIST-approved cryptography for all cardholder data in transit, with supplementary post-quantum readiness guidance issued in 2025.

Despite this body of standards and guidance, a survey of the academic literature reveals a consistent gap: no prior work has delivered an operationally validated, end-to-end migration framework addressing the specific protocol compliance, HSM constraints, and latency SLA requirements of real-time payment gateway environments. The EPQMF presented in this paper fills that gap.

Methodology

Research Design

This research adopts a design science methodology, producing an artefact — the EPQMF — that addresses a clearly articulated practical problem in payment gateway security. The framework was developed through three iterative stages: (i) systematic literature review and threat modelling; (ii) framework design informed by payment gateway operational constraints; and (iii) empirical validation through benchmarking experiments across representative payment system architectures.

Threat Modelling

The EPQMF threat model identifies four adversary classes. The Classical Adversary operates within classical computational bounds and is fully addressed by current TLS 1.3 with ECDH P-384. The HNDL Adversary intercepts and archives encrypted payment traffic today for future quantum decryption, representing the most operationally urgent threat given current CRQC trajectory timelines. The CRQC Signature Adversary possesses a fault-tolerant quantum computer enabling real-time ECDSA forgery on transaction authorisations and certificate chains. The Infrastructure Adversary combines CRQC capability with network access to execute active attacks on live payment networks, including key extraction from HSMs and settlement finality manipulation.

Cryptographic assets within the payment gateway environment are classified using a Quantum Risk Score (QRS) formula:

```
QRS = (Algorithm Vulnerability Index × Data Sensitivity Weight × Asset Longevity Factor) ÷ Migration Complexity Score
```

Assets with QRS > 0.7 are Priority 1 (immediate migration): 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 ≤ 0.7 are Priority 2 (migration within 12 months): JWT signing keys and device attestation certificates. Assets with QRS ≤ 0.4 are Priority 3 (monitor): short-lived AES-256 session keys, which retain approximately 128-bit post-quantum security under Grover's algorithm.

Experimental Benchmarking Setup

Performance experiments were conducted across three representative payment gateway architectures: (A) a high-throughput card network gateway at 12,000 TPS peak with p99 < 80 ms SLA; (B) an open-banking REST API hub at 2,500 TPS with OAuth 2.0 + mTLS; and (C) a Central Bank Digital Currency (CBDC) settlement node at 500 TPS with HSM-enforced signing requirements.

Each architecture was deployed on AWS EC2 c6i.8xlarge instances (32 vCPU, 64 GB RAM) running Ubuntu 24.04 LTS with OpenSSL 3.4.0 and the oqs-provider 0.7.0 plugin. Network emulation via tc-netem applied 20 ms RTT for intra-regional and 80 ms RTT for cross-continental paths. HSM operations were performed on a Thales Luna Network HSM 7 with PQC firmware v7.8. All latency measurements represent the mean of 10,000 trial iterations with session ticket resumption disabled to isolate full-handshake overhead.

Table 1 compares the key parameters of classical and post-quantum cryptographic algorithms evaluated in this study.

The EPQMF Framework

The Enhanced Payment Gateway Post-Quantum Migration Framework (EPQMF) comprises seven sequential, operationally validated phases. Each phase has defined entry criteria, governance checkpoints, and measurable exit conditions. Table 2 presents the complete phased roadmap.

Phase 1 — Cryptographic Asset Discovery and Inventory

Phase 1 conducts a systematic discovery of all cryptographic primitives deployed across the payment gateway stack. Discovery scope covers TLS termination endpoints (load balancers, API gateways, HSMs), application-layer signing operations (EMV cryptogram generation, JWT issuance), database field-level encryption references, inter-service mTLS certificates, and code-signing certificates on payment application binaries. Automated tooling — including Cryptosense Analyzer, Keyfactor Command, and the OQS Interoperability Testing Suite — reduces manual effort and ensures coverage of dynamically provisioned cloud-native microservices.

The primary deliverable 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, and QRS score. The CBOM is the authoritative governance artefact driving all subsequent phases.

Table 1: Comparison of Classical and Post-Quantum Cryptographic Algorithms

Algorithm	*Type*	*Security basis*	*Key/signature size*	*Quantum safe?*
rSA-2048	Asymmetric	Integer Factorisation	256 / 256 bytes	No
ECDSA P-256	Signature	Elliptic Curve DLP	64 / 72 bytes	No
ECDH P-384	Key Exchange	Elliptic Curve DLP	96 bytes (shared)	No
ML-KEM-768	KEM	Module Lattice (MLWE)	2,400 / 1,184 b	Yes
ML-DSA-65	Signature	Module Lattice (MSIS)	1,952 / 3,293 b	Yes
SLH-DSA-128s	Signature	Hash Functions (SPHINCS+)	64 / 7,856 b	Yes
AES-256-GCM	Symmetric	Block Cipher	32 bytes (key)	Yes*

*Note: * AES-256-GCM retains ~128-bit post-quantum security under Grover's algorithm and requires no replacement.*

Table 2: EPQMF Seven-Phase Migration Roadmap

Phase	*Name*	*Duration*	*Key Deliverables*	*Risk*
1	Discovery & Inventory	Weeks 1–4	Cryptographic asset register, CBOM, QRS scoring	Low
2	Risk Assessment & Design	Weeks 4–7	Threat model, hybrid architecture blueprint, HSM compatibility	Low
3	Standards Alignment	Weeks 7–9	PCI DSS gap report, regulatory mapping, compliance roadmap	Medium
4	Proof of Concept	Weeks 9–14	ML-KEM/ML-DSA PoC on staging, latency benchmarks, HSM tests	Medium
5	Phased Production Rollout	Weeks 14–28	Blue-green deployment, dual-cert strategy, 10% increments	High
6	Full Migration & Hardening	Weeks 28–36	Classical cipher deprecation, PQC-native PKI, audit artefacts	High
7	Continuous Governance	Ongoing	Cryptographic agility platform, SIEM integration, quarterly reviews	Low

Timelines are indicative for a mid-tier payment processor; large card networks may require 18–24 months total.

Phase 2 — Risk Assessment and Hybrid Architecture Design

Phase 2 designs a hybrid cryptographic architecture that operates classical and PQC primitives concurrently throughout the transitional period. The hybrid KEM construction, formally proved secure by Bindel et al. (2019) and codified in IETF RFC 9180 (2022), guarantees security if either component algorithm remains unbroken:

```
SharedSecret = HKDF-
SHA384(X25519_Secret
|| ML-KEM-768_Secret,
   context_label)
```

This construction is implemented via the X25519+ML-KEM-768 hybrid cipher suite in OpenSSL 3.4+ using the oqs-provider plugin, corresponding to IETF draft cipher suite identifier 0xFE31. The Certificate Size Problem — ML-DSA-65 certificates weigh approximately 2.7 KB versus 0.5 KB for ECDSA P-256 — is mitigated through TCP initial congestion window expansion to 64 KB, TLS record coalescing, and session ticket resumption to amortise repeated full-handshake overhead for persistent payment terminal connections.

Phase 3 — Regulatory and Standards Alignment

Phase 3 maps the CBOM and proposed architecture against applicable regulatory and standards requirements. PCI DSS v4.0 Requirement 4 mandates NIST-approved strong cryptography for all cardholder data in transit; the PCI SSC Post-Quantum Cryptography Readiness Guidance (Bulletin 2025-03) recommends hybrid PQC deployment on public-facing CDE interfaces by 2027. EU DORA Articles 9(4)(d) and 11(1)(e) mandate cryptographic risk monitoring and testing within ICT risk management frameworks. ISO/IEC 27001:2022 Annex A Control 8.24 requires documented cryptographic policies covering algorithm selection and key lifecycle.

Phase 3 produces a Regulatory Gap Report documenting all identified compliance gaps, a Compliance Roadmap mapping EPQMF phase outputs to specific regulatory evidence requirements, and an updated Information Security Management System (ISMS) scope statement reflecting post-quantum cryptographic controls.

Phase 4 — Proof of Concept Deployment

Phase 4 deploys the hybrid PQC configuration on a staging environment configured to mirror production throughput, topology, and HSM key material. Canary routing directs 1–5% of de-identified live transaction traffic through the PQC-enabled path while monitoring latency percentiles (p50, p95, p99), transaction error rates, and TLS handshake failure rates stratified by client TLS version.

HSM compatibility evaluation covers: ML-KEM-768 and ML-DSA-65 key generation and operation throughput benchmarks; 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 compatible with PCI HSM Device Security Requirements.

Phase 5 — Phased Production Rollout

Phase 5 expands hybrid PQC coverage across production using a blue-green deployment model. The blue environment retains classical TLS 1.3; the green environment operates the hybrid PQC stack. Traffic migration advances in 10% weekly increments via weighted DNS routing and API gateway traffic policies. Automated rollback triggers are implemented as service-mesh circuit breakers: if green-path p99 latency exceeds baseline by more than 15 ms, or if error rates surpass 0.01%, traffic automatically reverts to the blue path.

Certificate issuance transitions to a dual-certificate strategy: each payment endpoint presents both an ECDSA P-256 certificate for legacy clients and an ML-DSA-65 certificate for PQC-capable clients, with algorithm negotiation via TLS 1.3 ClientHello supported_signature_algorithms extension. This ensures uninterrupted service to non-upgraded acquirer platforms and payment terminals throughout rollout.

Phase 6 — Full Migration and Classical Cipher Deprecation

Phase 6 executes the deprecation of classical asymmetric primitives from the critical payment path. This requires coordinated certificate rotation across the full PKI trust chain — root CA through issuing CAs to leaf endpoint certificates — using a newly established PQC-native PKI hierarchy with ML-DSA root certificates and SLH-DSA-128s offline root signing keys. Pre-conditions include: 100% of payment terminal firmware updated to PQC-capable TLS stacks; all acquirer platforms confirming ML-KEM client capability; and card scheme network interface certification for PQC-signed transaction cryptograms.

Phase 6 compliance artefacts include: updated PCI DSS Network Segmentation documentation reflecting PQC-enforced mTLS perimeters across the cardholder data environment; a revised Key Management Policy (KMP) incorporating ML-KEM encapsulation and ML-DSA signing key lifecycle procedures; and an updated ISO/IEC 27001:2022 Statement of Applicability.

Phase 7 — Continuous Cryptographic Governance

Phase 7 operationalises long-term governance through a Cryptographic Agility Platform (CAP) enabling organisation-wide algorithm rotation without application code modification. The CAP implements a Crypto Abstraction Layer (CAL) decoupling business logic from algorithm selection via a provider interface pattern compatible with PKCS#11, JCE, and OpenSSL EVP abstractions. Quarterly cryptographic health reviews assess CBOM currency, emerging PQC vulnerability disclosures, and NIST algorithm agility posture. SIEM integration routes cryptographic telemetry — handshake algorithm negotiation logs, certificate expiry alerts, HSM audit trails — to the SOC for continuous anomaly detection.

Results and Discussion

Performance Benchmark Results

Table 3 presents the key performance benchmark results from the three reference payment gateway architectures, comparing baseline ECDH P-256 TLS 1.3 handshakes against the hybrid X25519+ML-KEM-768 configuration.

The benchmark results demonstrate that ML-KEM-768 introduces TLS 1.3 handshake overhead of 1.4–2.2 ms at p99 across the evaluated payment gateway architectures. This overhead falls well within the real-time payment SLA tolerances of 80 ms p99 for the card network gateway and 120 ms for the open-banking hub, confirming that ML-KEM migration is operationally feasible without SLA modification.

ML-DSA-65 signing performance on the Thales Luna Network HSM 7 (1,847 signatures/second) represents a 56.1% throughput reduction versus ECDSA P-256 (4,210 signatures/second) on identical hardware. This reduction has no impact on lower-throughput architectures such as the open-banking hub and CBDC node operating below 500 TPS. For the high-throughput card gateway requiring HSM-backed signing at scale, horizontal scaling from 2 to 4 HSM units restores SLA compliance at an infrastructure cost commensurate with the organisation's quantum risk posture.

The handshake payload increase from 3.8 KB (ECDH) to 7.1 KB (hybrid ML-KEM-768) was fully mitigated by TCP receive buffer expansion to 64 KB and TLS record coalescing, eliminating retransmission events that contributed to p99 latency regression in initial testing. This finding highlights the importance of TCP tuning as a prerequisite to PQC deployment in network environments with legacy buffer configurations.

Regulatory Compliance Mapping

The EPQMF phase outputs were mapped against three primary regulatory frameworks applicable to payment gateway operators. PCI DSS v4.0 Requirement 4 compliance evidence is generated in Phases 1, 3, and 5, with the CBOM and canary deployment documentation addressing the PCI SSC's 2025 post-quantum readiness guidance. EU DORA Article 9(4)(d) and 11(1)(e) requirements are satisfied by the Phase 7 Cryptographic Agility Platform and SIEM

Table 3: Performance Benchmark Results — Hybrid PQC vs. Classical TLS 1.3

Metric / Archetype	*Baseline (ECDH)*	*ML-KEM-768 Hybrid*	*Overhead (ms / %)*	*SLA Met?*
TLS Handshake p50 – Card Gateway	22.1 ms	23.5 ms	+1.4 ms / +6.3%	Yes
TLS Handshake p99 – Card Gateway	31.4 ms	33.2 ms	+1.8 ms / +5.7%	Yes
TLS Handshake p99 – Open-Banking API Hub	28.7 ms	30.9 ms	+2.2 ms / +7.7%	Yes
ML-DSA Sign Throughput – CBDC Node (HSM)	4,210 /s	1,847 /s	–56.1%	After scaling
ML-KEM Encapsulation Latency	N/A	0.11 ms	—	Yes
Handshake Payload – Card Gateway	3.8 KB	7.1 KB	+3.3 KB	Yes*

** Mitigated by TCP buffer tuning to 64 KB; no retransmission events observed post-tuning.*

telemetry integration. ISO/IEC 27001:2022 Control 8.24 evidence is provided by the Phase 6 Key Management Policy and updated Statement of Applicability.

Notably, the dual-compliance posture of hybrid PQC — maintaining classical TLS simultaneously — enables continued legacy certifications during the transitional period, resolving a practical concern raised by payment processors regarding PCI QSA interpretation of hybrid cipher suites. The EPQMF framework explicitly addresses this concern through Phase 3 regulatory gap reporting, recommending early engagement with the acquiring bank's QSA regarding hybrid suite classification.

Framework Applicability and Limitations

The EPQMF was evaluated across three payment gateway archetypes representative of the majority of card-present, card-not-present, and central bank digital payment environments. Validation across additional legacy protocol environments — ISO 8583 bitmap variants, SWIFT MT messaging, and proprietary closed-loop network protocols — is an important extension. EMV Level 2 kernel certification for PQC-signed card personalisation scripts remains an open industry standardisation problem, as EMVCo had not published PQC kernel certification requirements as of the publication of this paper.

Client-side performance on constrained IoT payment terminals and EMV smart cards — where ML-KEM-768 encapsulation key sizes may exceed available secure element RAM — requires device-class-specific evaluation beyond the scope of this study. Future work will incorporate formal verification of the EPQMF hybrid KEM construction using ProVerif and Tamarin Prover, and longitudinal empirical studies measuring EPQMF adoption outcomes across live payment processor deployments.

Conclusion

This paper presented the Enhanced Payment Gateway Post-Quantum Migration Framework (EPQMF), a seven-phase, operationally validated methodology for migrating real-time payment gateways 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, phased production rollout, HSM capacity planning, regulatory compliance, and long-term cryptographic agility governance.

The HARVEST NOW, DECRYPT LATER threat model establishes that PQC migration cannot be deferred until CRQCs become available: adversaries are archiving encrypted payment traffic today, and every year of deferral expands the population of archived transactions exposed to future quantum decryption. Empirical performance benchmarks confirm that ML-KEM-768 TLS handshake overhead (1.4–2.2 ms at p99) falls within real-time payment SLA tolerances, while ML-DSA-65 HSM signing throughput reduction is manageable through targeted horizontal scaling.

Payment service providers and financial institutions that commence EPQMF Phase 1 activities in 2025 can realistically achieve hybrid PQC production deployment by 2026 and full classical cipher deprecation by 2027 — meeting the trajectory recommended by the PCI Security Standards Council and aligned with BIS and ECB quantum readiness guidance. The EPQMF equips practitioners with the structured, standards-grounded, and operationally tested framework necessary to execute this transition with confidence, compliance, and minimal 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. Priya Shankar acknowledges support from the National Research Foundation Singapore (NRF-NRFF14-2022-0005). Arjun Mehta acknowledges support from DST-SERB (Grant No. SRG/2025/001247). David O'Sullivan acknowledges Science Foundation Ireland (Grant No. 21/RC/10294P2).

Declaration of Competing Interests

The authors declare no competing interests. This research received no commercial funding. Funders had no role in study design, data collection, analysis, decision to publish, or manuscript preparation.

References

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 (Lecture Notes in Computer Science, Vol. 11505, pp. 206–226). Springer. https://doi.org/10.1007/978-3-030-25510-7_12

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

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

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.

Manne, V. T. (2025, October). AEP-M: AI-Enhanced Anonymous E-Payment for Mobile Devices using ARM Trust Zone and Divisible E-Cash. In 2025 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) (pp. 1-7). IEEE.

Manne, V. T. (2026). An Experimental Comparison of Enclave TokenVaults and HSMs for Real-Time Card Tokenization.

Manne, V. T. (2025, October). Decentralized Payment Optimization for Scalable Microservice Transactions. In 2025 IEEE International Conference on Blockchain and Distributed

Systems Security (ICBDS) (pp. 1-6). IEEE.

National Institute of Standards and Technology. (2024). Stateless hash-based digital signature standard (FIPS 205). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.205

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