

Development of the PQC-Benchmark Algorithm for Evaluating the Performance of Post-Quantum Cryptographic Algorithms in Digital Banking Transactions Compared with RSA, ECDH, and ECDSA-Based Cryptographic Configurations

Timothy Olatunji Ogundola¹; Kofoworola Idowu²

¹Department of Technology Management, University of Bridgeport, Bridgeport Connecticut, USA

²Department of Computer Science and Engineering, Yeshiva University, New York, USA

Publication Date: 2026/10/23

Abstract: The increasing sophistication of quantum computing presents significant challenges to the long-term security, computational efficiency, and operational resilience of digital banking infrastructures that rely on conventional public-key cryptographic algorithms. Although Rivest–Shamir–Adleman (RSA), Elliptic Curve Diffie–Hellman (ECDH), and Elliptic Curve Digital Signature Algorithm (ECDSA) remain widely established cryptographic mechanisms, their underlying mathematical assumptions are vulnerable to sufficiently powerful quantum computers. Recent standardization of Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), Module-Lattice-Based Digital Signature Algorithm (ML-DSA), and Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) creates opportunities for quantum-resistant financial transaction security, although computational overhead, transmission requirements, and deployment scalability remain important engineering considerations. This study proposes PQC-Benchmark, a novel security-constrained, multi-objective benchmarking and adaptive cryptographic configuration-selection algorithm designed to evaluate and optimize the operational performance of post-quantum cryptographic configurations within digital banking environments. The proposed framework integrates normalized performance profiling, entropy-based criterion weighting, Pareto-dominance analysis, adaptive workload characterization, and explainable performance attribution to identify suitable cryptographic configurations under varying transaction demands. Its experimental architecture compares ML-KEM-512, ML-KEM-768, ML-KEM-1024, ML-DSA-44, ML-DSA-65, ML-DSA-87, SLH-DSA, and selected hybrid classical–post-quantum configurations against RSA-2048/3072, ECDH-P256/P384, and ECDSA-P256/P384 baselines. Cryptographic primitives are assessed according to their corresponding functions, while complete key-establishment and authentication configurations are evaluated at the banking transaction level. A reproducible Python-based simulation and experimental benchmarking environment is proposed to model mobile banking authentication, interbank payment authorization, encrypted API communication, and high-frequency financial transaction processing under heterogeneous network latency, transaction volume, and computational resource constraints. Performance indicators include cryptographic execution time, end-to-end transaction latency, transaction throughput, CPU utilization, memory consumption, public-key and signature sizes, handshake bandwidth, energy expenditure, and quantum-resistance eligibility. Comparative analyses will employ bootstrap confidence intervals, appropriate repeated-measures statistical tests, effect-size estimation, sensitivity analysis, and multi-objective optimization. The proposed results framework will generate comparative latency distributions, throughput curves, computational resource utilization profiles, Pareto-optimal performance frontiers, and workload-dependent configuration rankings. The central hypothesis is that PQC-Benchmark can achieve superior workload-adjusted configuration-selection performance relative to fixed cryptographic policies and conventional single-metric benchmarking methods, without altering or weakening standardized cryptographic primitives. The study is expected to establish a reproducible decision-support framework for identifying secure, computationally efficient, and scalable post-quantum cryptographic configurations for digital banking applications.

Keywords: Post-Quantum Cryptography; PQC-Benchmark Algorithm; Digital Banking Transactions; Cryptographic Performance Evaluation; Hybrid Cryptographic Configurations.

How to Cite: Timothy Olatunji Ogundola; Kofoworola Idowu (2026) Development of the PQC-Benchmark Algorithm for Evaluating the Performance of Post-Quantum Cryptographic Algorithms in Digital Banking Transactions Compared with RSA, ECDH, and ECDSA-Based Cryptographic Configurations. *International Journal of Innovative Science and Research Technology*, 11(10), 1433-1455. <https://doi.org/10.38124/ijisrt/26oct1102>

I. INTRODUCTION

➤ *Background to Post-Quantum Cryptography and Security Challenges in Digital Banking Infrastructures*

The rapid digitalization of financial services has transformed banking infrastructures into interconnected computational ecosystems supporting electronic funds transfers, mobile banking applications, interbank settlement networks, digital wallets, payment gateways, and central bank digital currency platforms. These systems depend on cryptographic mechanisms for establishing authenticated communication channels, protecting transaction confidentiality, verifying digital identities, and maintaining the integrity of financial instructions. However, the emergence of quantum computing introduces a fundamental security challenge because conventional public-key cryptographic algorithms, particularly RSA and elliptic-curve-based mechanisms, depend on computational assumptions that are vulnerable to sufficiently powerful fault-tolerant quantum computers. Ajayi et al. (2024) examined the relevance of quantum cryptography to financial transaction security within central bank digital currency environments, highlighting the importance of robust cryptographic architectures for protecting distributed financial operations. Although quantum cryptography and post-quantum cryptography represent distinct security approaches, their development reflects the growing importance of securing communication systems against emerging computational threats. Gisin et al. (2002) established the theoretical and technological foundations of quantum cryptography, particularly quantum key distribution, demonstrating how quantum-mechanical principles can contribute to secure key establishment. For digital banking institutions, however, conventional network interoperability and deployment requirements make software-based post-quantum cryptographic mechanisms an especially relevant migration pathway.

Post-quantum cryptography addresses these emerging vulnerabilities through mathematical constructions designed to resist attacks using currently known classical and quantum algorithms. Unlike quantum key distribution, post-quantum cryptographic schemes operate on conventional computing hardware, supporting integration with banking application servers, cryptographic libraries, authentication services, and secure communication protocols. Pirandola et al. (2020) reviewed developments in quantum-secure communication and identified important technological considerations for the practical deployment of next-generation security architectures. Within digital banking, post-quantum key encapsulation and authentication mechanisms must satisfy additional operational requirements, including low transaction latency, high request-processing capacity, manageable memory consumption, and compatibility with existing financial infrastructure. These considerations motivate the proposed PQC-Benchmark algorithm, which

evaluates standardized post-quantum cryptographic configurations against RSA, ECDH, and ECDSA-based alternatives through an integrated security-constrained performance model. The framework is designed to quantify execution time, communication overhead, transaction throughput, resource consumption, and workload-dependent efficiency. Consequently, the study investigates whether adaptive cryptographic configuration selection can support quantum-resistant financial communication while maintaining operational performance across mobile banking, interbank transfers, and high-volume payment processing environments.

➤ *Evolution of RSA, ECDH, and ECDSA-Based Cryptographic Configurations in Electronic Financial Transaction Systems*

The development of modern digital banking security has been closely associated with the evolution of asymmetric cryptography, which enables financial institutions to authenticate communicating entities and establish confidential communication without distributing shared secret keys in advance. Rivest et al. (1978) introduced RSA as a public-key cryptographic system based on modular exponentiation and the computational difficulty of factoring large composite integers. RSA subsequently became an important component of digital certificates, electronic signatures, authentication infrastructures, and secure electronic transactions. Its operational characteristics depend on key length, exponentiation procedures, padding mechanisms, and cryptographic implementation efficiency. The emergence of elliptic-curve cryptography introduced alternative mathematical structures capable of providing strong classical security with comparatively smaller keys. Koblitz (1987) established the mathematical foundations of elliptic-curve cryptosystems, demonstrating the potential of finite-field elliptic-curve groups for public-key cryptographic operations. These developments supported the adoption of ECDH for establishing shared secrets and ECDSA for authenticating digitally signed information. In contemporary financial systems, such mechanisms are incorporated into transport security configurations, payment authentication systems, financial application programming interfaces, and hardware security module operations.

Despite their technological maturity, conventional cryptographic configurations exhibit operational and security characteristics that require systematic evaluation against emerging post-quantum alternatives. RSA-2048 and RSA-3072 involve different computational demands from ECDH-P256, ECDH-P384, ECDSA-P256, and ECDSA-P384, while each configuration performs a distinct cryptographic function. Accordingly, meaningful comparisons must distinguish key establishment from digital signature generation and verification before examining complete authenticated banking transaction workflows. Ononiwu et al. (2023) investigated machine-learning-based fraud detection

and risk assessment in mobile banking applications, illustrating the growing dependence of financial security systems on computationally intensive analytical processes. Such systems must coexist with cryptographic services without introducing unacceptable transaction-processing delays or exhausting available computational resources. This study therefore models conventional public-key configurations as reproducible performance baselines within a common banking transaction architecture. RSA-based authentication, ECDH key agreement, and ECDSA signature mechanisms will be evaluated using standardized execution environments, consistent transaction payloads, and controlled workload conditions. The resulting measurements will establish a classical performance reference against which PQC-Benchmark-selected post-quantum and hybrid configurations can be assessed for latency, throughput, resource efficiency, and quantum-resistance eligibility.

➤ *Quantum Computing Threat Models and Vulnerabilities of Conventional Public-Key Cryptographic Algorithms*

The security of conventional public-key cryptographic systems depends on mathematical problems that are computationally difficult for classical computers but become tractable under specific quantum computational models. Shor (1997) demonstrated polynomial-time quantum algorithms for integer factorization and discrete logarithm computation, fundamentally challenging the mathematical assumptions supporting RSA and elliptic-curve cryptographic systems. RSA relies on the practical difficulty of factoring sufficiently large composite integers, whereas ECDH and ECDSA depend on the computational hardness of discrete logarithms over elliptic-curve groups. A sufficiently capable fault-tolerant quantum computer could therefore undermine RSA-based confidentiality and signatures, recover elliptic-curve private keys, and compromise the authentication and key-establishment procedures used in electronic financial transactions. Gidney and Ekerå (2021) provided a detailed quantum-resource analysis indicating that factoring a 2048-bit RSA modulus could theoretically be accomplished within approximately eight hours using 20 million noisy physical qubits under specified hardware and error-correction assumptions. This estimate represents a theoretical resource scenario rather than evidence of currently available cryptanalytic capability. Nevertheless, it demonstrates why financial institutions must distinguish present operational security from long-term cryptographic resilience, particularly when protecting transaction records, customer information, authentication credentials, and encrypted financial communications.

Quantum threats also introduce temporal security concerns because adversaries may capture encrypted financial communications today and attempt to decrypt them after suitable quantum capabilities become available. Such harvest-now-decrypt-later attacks are particularly important for banking information requiring extended confidentiality, including sensitive account records, customer identification documents, institutional financial agreements, and interbank communication archives. Idoko et al. (2024) examined prospective quantum computing and artificial intelligence developments, emphasizing their potential computational

implications across information-processing applications. In the present study, these broader technological considerations are translated into a defined cryptographic threat model comprising passive communication interception, retrospective decryption attempts, public-key recovery, digital signature forgery, and active transaction impersonation. The proposed PQC-Benchmark architecture incorporates quantum-resistance eligibility as a mandatory security condition rather than treating security as a compensatory performance score. Classical RSA, ECDH, and ECDSA configurations will therefore serve as historical and operational comparison baselines but will not qualify as standalone quantum-resistant solutions. Hybrid configurations will be assessed according to the security assumptions and construction of their constituent mechanisms. This distinction ensures that the experimental evaluation measures operational efficiency without confusing computational speed with resistance to quantum cryptanalysis, thereby establishing a defensible security foundation for subsequent algorithmic optimization and banking transaction simulations.

➤ *Emergence of Lattice-Based, Hash-Based, and Hybrid Post-Quantum Cryptographic Algorithms for Banking Security*

The transition toward quantum-resistant financial communication has accelerated the development of cryptographic constructions whose security is based on mathematical problems not currently known to admit efficient quantum solutions. Lattice-based cryptography represents a particularly important development because it combines established computational hardness assumptions with implementations suitable for conventional processors. Grover et al. (2022) investigated algebraic extensions of learning-with-errors constructions, demonstrating how structured lattice problems provide a foundation for developing cryptographic mechanisms with alternative computational and security characteristics. These mathematical foundations are relevant to module-lattice constructions employed in standardized post-quantum algorithms. ML-KEM, standardized through FIPS 203, provides key encapsulation functionality using parameter sets ML-KEM-512, ML-KEM-768, and ML-KEM-1024, whereas ML-DSA, standardized through FIPS 204, supports digital signatures using ML-DSA-44, ML-DSA-65, and ML-DSA-87. Ducas et al. (2018) developed the CRYSTALS-Dilithium signature scheme, establishing efficient lattice-based signing and verification techniques that underpin the subsequent ML-DSA standard. These algorithms offer practical alternatives for establishing authenticated banking communication sessions, verifying financial instructions, and protecting sensitive payment operations against specified quantum adversaries.

Hash-based cryptography provides another quantum-resistant approach through digital signature constructions grounded primarily in cryptographic hash-function security. SLH-DSA, standardized through FIPS 205, is particularly relevant where conservative security assumptions are prioritized, although its relatively substantial signature sizes and computational requirements can affect transaction

efficiency. Idika (2023) examined quantum-resistant communication protocols within autonomous vehicle networks, providing an application-oriented perspective on deploying quantum-resistant mechanisms in distributed systems with demanding communication requirements. Although vehicle networks and digital banking platforms differ operationally, both demonstrate the need to evaluate cryptographic performance within actual communication workflows rather than relying exclusively on isolated primitive benchmarks. Hybrid cryptographic configurations offer an additional migration strategy by combining classical mechanisms, such as ECDH-P256, with post-quantum mechanisms, such as ML-KEM-768, through appropriately designed key-combination procedures. The proposed PQC-Benchmark framework therefore compares classical, post-quantum, and hybrid key-establishment configurations alongside compatible authentication arrangements. It will independently measure encapsulation, decapsulation, signature generation, verification, ciphertext expansion, handshake bandwidth, and complete transaction-processing performance. Rather than modifying standardized algorithms, the framework will determine which eligible cryptographic configurations achieve the most favorable operational trade-offs under specified banking security requirements, transaction workloads, and computational resource constraints.

➤ *Computational Performance, Transaction Latency, Throughput, and Resource Optimization Challenges in Post-Quantum Cryptographic Deployment*

Deploying post-quantum cryptography within digital banking infrastructures introduces significant performance considerations because cryptographic security must coexist with strict transaction-processing requirements, high service availability, and heterogeneous computing environments. Financial applications operate across mobile devices, payment gateways, banking servers, cloud platforms, and interbank communication networks, creating substantial variations in processor capacity, available memory, network bandwidth, and concurrent transaction demand. Abiodun et al. (2023) examined cross-border digital asset flows and central bank digital currency risks, highlighting the importance of financial stability and operational resilience within interconnected digital financial ecosystems. In such environments, cryptographic migration requires evaluation beyond theoretical security classifications because the adoption of post-quantum algorithms can affect message sizes, authentication processing, connection establishment, and transaction completion times. Rubio García et al. (2024) experimentally evaluated quantum-resistant Transport Layer Security configurations and demonstrated that cryptographic integration can produce distinct communication and computational trade-offs. Their findings indicated that post-quantum-only configurations could improve certain handshake performance measures, whereas hybrid post-quantum and quantum-key-distribution arrangements introduced additional key-establishment overhead. These observations demonstrate that cryptographic deployment performance depends strongly on protocol architecture, security configuration, communication mechanisms, and

implementation conditions rather than algorithm classification alone.

For banking transaction evaluation, total service latency must account for cryptographic processing, communication delays, server execution, queuing, and authentication overhead. The proposed study represents transaction latency as $T_{total} = T_{crypto} + T_{network} + T_{queue} + T_{application}$, enabling separate identification of performance bottlenecks. Montenegro et al. (2026) developed a post-quantum TLS performance evaluation framework and demonstrated the importance of assessing cryptographic primitives alongside complete protocol implementations under controlled network conditions. Building on this experimental perspective, PQC-Benchmark will investigate workload-dependent transaction performance using ML-KEM-512/768/1024, ML-DSA-44/65/87, SLH-DSA, RSA, ECDH, ECDSA, and suitable hybrid configurations. Evaluation metrics will include median and 95th-percentile latency, successful transactions per second, CPU utilization, peak memory consumption, handshake bytes, and energy consumption per completed transaction. Controlled experiments will vary concurrent sessions, simulated network delay, packet loss, and available processing resources. The framework will subsequently apply security-constrained, multi-objective optimization to identify configurations that minimize operational costs while satisfying predefined security requirements. Comparative graphs and statistical confidence intervals will determine whether adaptive selection offers measurable improvements over fixed cryptographic configurations.

➤ *Research Problem, Technical Motivation, and Limitations of Existing Cryptographic Benchmarking and Configuration-Selection Frameworks*

Despite considerable progress in post-quantum cryptographic standardization and implementation, identifying suitable cryptographic configurations for heterogeneous digital banking environments remains a multidimensional optimization problem. Conventional benchmarking approaches frequently prioritize isolated cryptographic execution time, key generation speed, signature verification, or communication overhead without integrating these measurements into workload-specific configuration-selection decisions. Such evaluations can produce misleading conclusions when algorithms optimized for a particular computational metric perform poorly under restricted bandwidth, high concurrency, or resource-constrained banking applications. Marler and Arora (2004) established that engineering optimization frequently involves competing objectives for which improvements in one performance dimension may produce deterioration in another. This principle is directly applicable to cryptographic configuration selection because minimizing execution time may increase bandwidth consumption, memory requirements, or operational energy expenditure. Similarly, Atalor et al. (2023) discussed computational modeling and quantum molecular simulation within pharmaceutical research, emphasizing the broader importance of efficient numerical evaluation and computational resource management when assessing sophisticated computational methods. Although their application concerns molecular simulation rather than

financial cryptography, the methodological requirement for reproducible, resource-aware computational evaluation motivates the present investigation into cryptographic performance benchmarking.

The principal research problem is therefore the absence, within the benchmarking approaches considered in this study, of an experimentally validated selection framework that jointly incorporates quantum-security eligibility, banking transaction characteristics, multiple performance objectives, statistical uncertainty, and interpretable configuration rankings. PQC-Benchmark is proposed to address this problem using workload-adaptive criterion weighting, normalized performance costs, Pareto-dominance filtering, and explainable configuration-selection rules. Saltelli et al. (2010) developed variance-based sensitivity analysis procedures that provide a rigorous foundation for determining how uncertainty in model inputs influences output variability. Accordingly, the proposed algorithm will incorporate sensitivity analysis to examine the influence of transaction concurrency, network latency, workload composition, performance weights, and computational resources on cryptographic configuration rankings. Its performance will be compared against fixed-configuration deployment strategies, equal-weight multi-criteria scoring, and single-metric benchmarking approaches. Experimental validation will employ repeated workload trials, bootstrap confidence intervals, paired statistical comparisons, and effect-size estimation, with measurements obtained from reproducible cryptographic implementations. The resulting framework is intended to establish whether adaptive, security-constrained optimization can achieve statistically significant improvements in banking transaction efficiency while retaining standardized cryptographic security requirements. Its claimed methodological superiority will depend on experimentally demonstrated improvements in selection quality, robustness, and deployment performance rather than assumed cryptographic advantages.

➤ *Research Objectives, Research Questions, and Testable Performance Hypotheses*

The overall aim of this study is to develop and experimentally validate PQC-Benchmark as a security-constrained, multi-objective optimization algorithm for evaluating and selecting efficient post-quantum cryptographic configurations in digital banking systems. The specific research objectives are:

- To develop a mathematical and computational architecture integrating cryptographic security constraints, normalized performance metrics, adaptive weighting, Pareto optimization, and explainable configuration selection;
- To measure and compare the computational performance of ML-KEM-512/768/1024, ML-DSA-44/65/87, SLH-DSA, RSA-2048/3072, ECDH-P256/P384, ECDSA-P256/P384, and selected hybrid configurations;
- To quantify the effects of cryptographic configuration choices on transaction latency, throughput, CPU utilization, memory consumption, bandwidth

requirements, and energy efficiency under heterogeneous banking workloads;

- To evaluate the selection accuracy, computational overhead, stability, and scalability of PQC-Benchmark relative to fixed-configuration policies, single-metric benchmarking, and equal-weight multi-criteria approaches;
- To establish statistically defensible performance improvements through repeated experiments, uncertainty estimation, sensitivity analysis, and reproducible numerical simulations.

The corresponding research questions are:

- How can security constraints and multiple operational performance indicators be integrated into a reproducible adaptive cryptographic benchmarking algorithm?
- How do standardized post-quantum, classical, and hybrid cryptographic configurations differ in computational and communication performance under comparable functional conditions?
- How do transaction concurrency, network conditions, and resource limitations influence the optimal cryptographic configuration for different banking applications?
- Does PQC-Benchmark achieve superior workload-adjusted configuration-selection performance compared with static and conventional benchmarking strategies?
- How robust and statistically reliable are its performance rankings under variations in experimental conditions and optimization weights?

The study will test the following research hypotheses:

- H_{01} : PQC-Benchmark does not significantly reduce mean workload-adjusted operational cost relative to eligible fixed-configuration baselines, against H_{A1} : PQC-Benchmark significantly reduces that cost.
- H_{02} : Eligible classical-comparison, post-quantum, and hybrid configurations exhibit no significant differences in their measured cryptographic execution costs, against H_{A2} : at least one configuration exhibits significantly different costs.
- H_{03} : Network conditions and transaction concurrency have no significant interaction with cryptographic configuration in determining transaction latency, against H_{A3} : a significant interaction exists.
- H_{04} : PQC-Benchmark does not significantly improve workload-adjusted performance relative to equal-weight and single-metric selection strategies, against H_{A4} : it significantly improves performance/
- H_{05} : Adaptive performance weighting does not significantly improve configuration-selection robustness across heterogeneous banking workloads, against H_{A5} : adaptive weighting significantly improves robustness. All hypotheses will be evaluated at a prespecified significance level of $\alpha=0.05$, with effect sizes, confidence intervals, multiple-comparison adjustments, and security-eligibility restrictions incorporated into the experimental validation.

➤ *Research Contributions, Novelty of the PQC-Benchmark Algorithm, and Organization of the Study*

This research proposes PQC-Benchmark as an original methodological contribution to post-quantum cryptographic performance assessment and security-constrained configuration optimization in digital banking infrastructures. Its intended novelty lies in the coordinated integration of standardized cryptographic benchmarking, workload-adaptive performance modeling, mandatory quantum-resistance eligibility, entropy-based criterion weighting, Pareto-optimal configuration filtering, statistical uncertainty quantification, and interpretable decision mechanisms within a unified experimental framework. Unlike benchmarking strategies that principally report isolated cryptographic execution times or communication overheads, PQC-Benchmark is designed to transform multidimensional performance measurements into workload-specific cryptographic configuration recommendations while preserving the security properties of the underlying standardized algorithms. Its principal technical contributions comprise a formal multi-objective optimization model, a configurable banking transaction simulation architecture, a reproducible Python experimental implementation, an adaptive configuration-selection procedure, and a comparative statistical validation framework. The proposed system will evaluate key-establishment mechanisms and digital signature algorithms according to their distinct cryptographic functions before integrating them into complete authentication and secure transaction-processing configurations. Performance validation will compare the proposed selection strategy against fixed post-quantum configurations, hybrid deployment policies, and conventional single-metric or equal-weight benchmarking approaches using execution-time distributions, transaction throughput curves, resource utilization profiles, sensitivity heatmaps, and Pareto-frontier visualizations. The framework will also quantify its own selection overhead and the operational effects of changing workload conditions to determine whether adaptive optimization provides practically meaningful benefits. Its contribution will be assessed through demonstrated improvements in operational efficiency, ranking stability, reproducibility, and explainability rather than through unsupported claims of enhanced cryptographic hardness. The manuscript is organized into five sections: Section 1 establishes the research background, motivation, objectives, hypotheses, and methodological contributions; Section 2 critically examines conventional and post-quantum cryptographic algorithms, benchmarking methods, and existing research limitations; Section 3 presents the PQC-Benchmark mathematical formulation, computational architecture, optimization procedure, simulation design, and experimental validation methods; Section 4 provides comparative numerical results, statistical performance evaluations, sensitivity analyses, and graphical interpretations; and Section 5 presents the research conclusions, scientific contributions, implementation recommendations, limitations, and future directions for quantum-resistant digital banking security.

II. LITERATURE REVIEW

➤ *Theoretical Foundations of Public-Key Cryptography, Quantum-Resistant Security, and Cryptographic Complexity Analysis*

Public-key cryptography establishes secure digital communication through mathematically related public and private keys, enabling authenticated key establishment, digital signatures, and transaction integrity verification. Conventional cryptographic security depends primarily on the computational difficulty of integer factorization and discrete logarithm problems, whereas post-quantum cryptography employs alternative assumptions, including module learning with errors and cryptographic hash-function security. Nejatollahi et al. (2019) established that lattice-based cryptographic implementations offer promising quantum-resistant constructions but exhibit platform-dependent computational and memory characteristics as shown in figure 1. Similarly, Liu et al. (2017) demonstrated that carefully optimized lattice-based operations can be implemented on resource-constrained microcontrollers, providing evidence that quantum-resistant cryptography is not inherently restricted to high-performance computing environments. These findings establish the theoretical basis for evaluating ML-KEM and ML-DSA configurations across banking devices with heterogeneous processing capabilities. Within PQC-Benchmark, cryptographic complexity will be examined through parameter-dependent execution costs, asymptotic computational requirements, memory allocation, and practical implementation characteristics, while security eligibility will remain a mandatory constraint.

The reliability of cryptographic configuration selection also depends on accurate performance measurement, transparent decision rules, and resilience against adversarial manipulation. Ijiga et al. (2024) examined adversarial machine learning within cybersecurity risk assessment, demonstrating the importance of evaluating security-oriented analytical systems under potentially manipulated inputs. This perspective informs PQC-Benchmark's proposed workload-integrity checks, benchmark-data validation, and resistance to misleading performance observations. Separately, Frank (2026) described measurement frameworks and performance-improvement methods in healthcare; the transferable methodological consideration is the need for consistent indicators and reproducible evaluation, rather than evidence concerning cryptographic security. Accordingly, the proposed framework distinguishes theoretical security properties from measured implementation performance and represents each cryptographic configuration through a multidimensional cost vector containing latency, memory, bandwidth, energy, and computational overhead. Its selection procedure will apply security filtering before multi-objective ranking, preventing favorable runtime measurements from compensating for inadequate quantum-resistance requirements. This foundation supports subsequent evaluation of cryptographic efficiency without conflating implementation speed, algorithmic complexity, and security strength.

Figure 1 illustrates the theoretical foundations of public-key cryptography, quantum-resistant security, and cryptographic complexity analysis within the proposed PQC-Benchmark framework for digital banking transactions. It comprises four interconnected components: Public-Key Cryptography Foundations, Quantum-Resistant Security Principles, Cryptographic Complexity Analysis, and Digital Banking Relevance, each containing four essential elements. The public-key cryptography component explains asymmetric key generation, encryption, key establishment, digital signatures, public-key infrastructure (PKI), and the mathematical assumptions underlying RSA, ECDH, and ECDSA, particularly integer factorization and discrete logarithm problems. The quantum-resistant security component addresses vulnerabilities arising from quantum computing and introduces lattice-based algorithms such as ML-KEM and ML-DSA, hash-based schemes such as SLH-DSA, and hybrid cryptographic configurations designed to

support quantum-resistant financial communication. The cryptographic complexity component examines computational requirements associated with key generation, encapsulation, decapsulation, signature generation, and verification, alongside communication overhead and resource consumption measured through CPU utilization, memory requirements, bandwidth, and energy expenditure. Finally, the digital banking component connects these theoretical considerations to mobile banking authentication, interbank transaction security, payment authorization, and high-throughput financial processing. Collectively, the four components establish the conceptual foundation for PQC-Benchmark's security-constrained, multi-objective optimization architecture, which employs entropy-weighted performance scoring, Pareto-dominance analysis, and adaptive configuration selection to identify operationally efficient cryptographic configurations without compromising prescribed post-quantum security requirements.

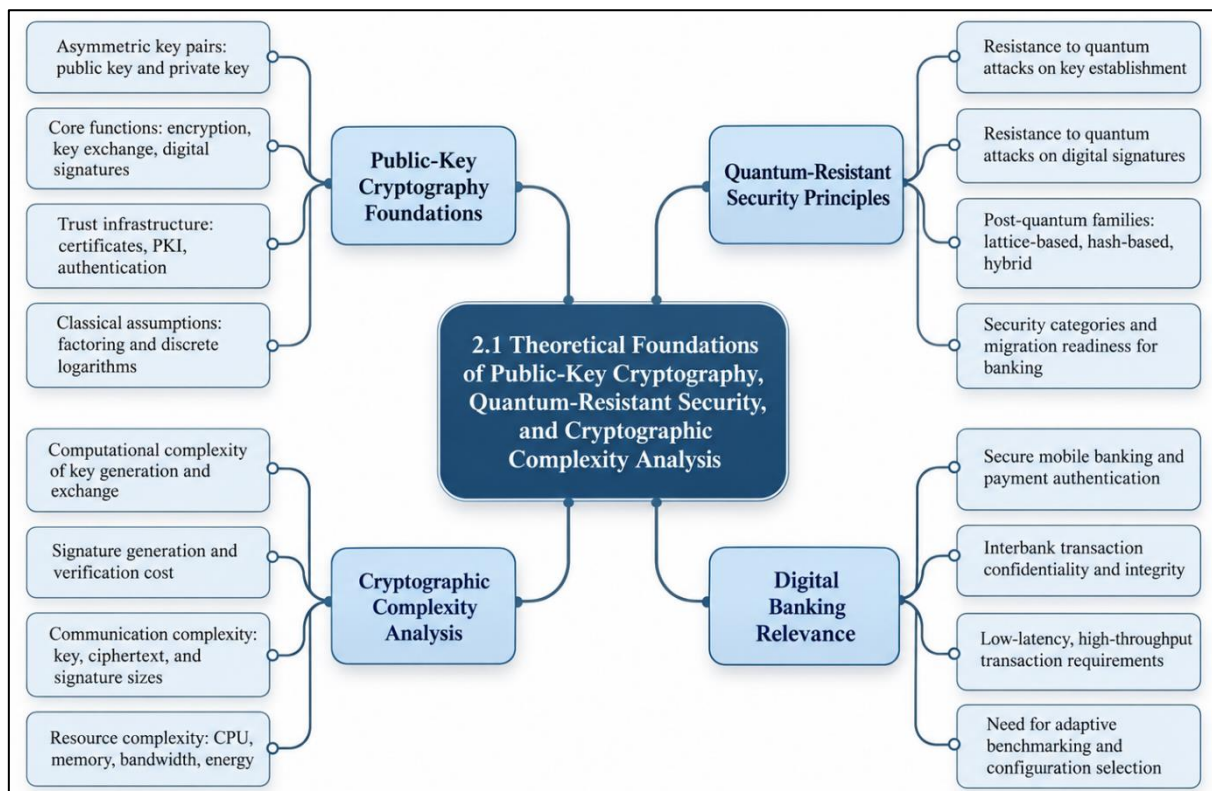


Fig 1 Conceptual Framework Linking Public-Key Cryptography, Quantum-Resistant Security, Computational Complexity, and Adaptive Cryptographic Optimization in Digital Banking Transactions.

➤ Comparative Computational Characteristics of RSA, ECDH, ECDSA, and Conventional Banking Cryptographic Configurations

Conventional financial cryptography relies on distinct asymmetric operations whose computational characteristics influence authentication overhead, session establishment, and transaction processing. Rivest et al. (1978) introduced RSA using modular exponentiation, enabling public-key encryption and digital signatures through integer-factorization-based security assumptions as shown in figure 2. RSA private-key operations typically require substantially different computational effort from public-key verification operations, making performance sensitive to modulus length,

exponent selection, and implementation optimizations. Koblitz (1987) introduced elliptic-curve cryptographic constructions, providing the mathematical foundation for compact public-key mechanisms based on elliptic-curve discrete logarithms. ECDH subsequently became a widely used key-agreement mechanism, whereas ECDSA provides digital signature generation and verification. These mechanisms must be compared according to their intended cryptographic functions rather than as interchangeable algorithms. In PQC-Benchmark, RSA-2048/3072 signing and verification, ECDH-P256/P384 shared-secret establishment, and ECDSA-P256/P384 authentication will therefore be

measured independently before integration into equivalent banking transaction configurations.

Financial transaction security additionally requires protection against threats that cannot be resolved through cryptographic primitive selection alone. Ayoola et al. (2024) investigated spear-phishing risks within financial institutions, emphasizing the importance of security awareness and human-centered protective mechanisms. Idowu et al. (2026) examined real-time DDoS and phishing detection in banking environments, identifying operational conditions under which financial systems require responsive security monitoring. These studies demonstrate why cryptographic performance assessment must account for concurrent security services and potentially hostile transaction environments. The proposed benchmarking architecture will integrate classical cryptographic configurations into simulated mobile banking authentication, payment authorization, and encrypted banking API sessions. Experimental indicators will include signing latency, verification latency, key-establishment time, CPU utilization, memory consumption, and end-to-end transaction completion time. Each configuration will be tested using comparable workloads, controlled hardware resources, consistent transaction payloads, and repeated execution trials. The resulting performance distributions will establish baseline operational characteristics against which security-eligible post-quantum configurations and PQC-Benchmark's adaptive selection decisions can be evaluated.

Figure 2 illustrates the comparative computational characteristics of conventional public-key cryptographic algorithms and their operational applications within digital

banking infrastructures, organized into two primary branches with two subbranches each. The first branch, Classical Public-Key Cryptographic Algorithms, examines RSA and elliptic-curve-based cryptographic configurations. RSA-2048 and RSA-3072 employ integer-factorization-based security assumptions and modular exponentiation for digital signatures and other supported public-key operations, with computational requirements influenced by key length and implementation efficiency. In contrast, ECDH-P256/P384 provides elliptic-curve-based shared-secret establishment, while ECDSA-P256/P384 supports digital signature generation and verification using comparatively compact key structures. The second branch, Comparative Computational Performance and Banking Applications, evaluates these algorithms using cryptographic execution time, transaction latency, throughput, CPU utilization, memory consumption, public-key and signature sizes, and communication overhead. These performance indicators determine their suitability for mobile banking authentication, electronic payment authorization, encrypted banking application programming interfaces, and interbank financial communication. Within the proposed PQC-Benchmark framework, RSA, ECDH, and ECDSA serve as classical reference configurations for evaluating standardized post-quantum mechanisms, including ML-KEM and ML-DSA, alongside hybrid classical–post-quantum architectures. The diagram therefore establishes the functional and computational relationships necessary for security-constrained performance benchmarking, highlighting the importance of comparing equivalent cryptographic operations while distinguishing conventional computational efficiency from resistance to quantum attacks.

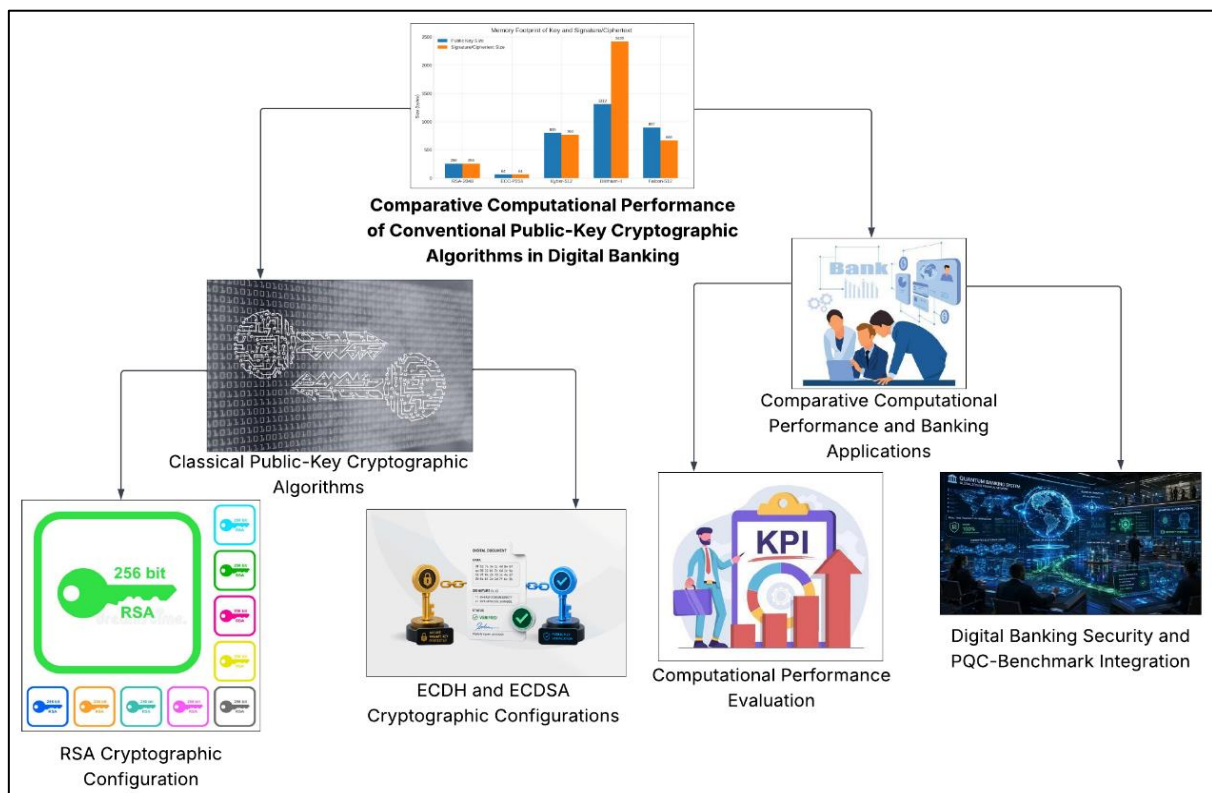


Fig 2 Conceptual Comparison of RSA, ECDH, and ECDSA Computational Characteristics and their Applications in Digital Banking Security.

➤ *Post-Quantum Key-Encapsulation Algorithms: ML-KEM-512, ML-KEM-768, ML-KEM-1024, and Hybrid ECDH–ML-KEM Architectures*

Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) is a standardized post-quantum cryptographic construction designed to establish shared secret material without depending on integer factorization or elliptic-curve discrete logarithms. Its ML-KEM-512, ML-KEM-768, and ML-KEM-1024 parameter sets provide different security categories and computational characteristics, introducing measurable differences in key sizes, ciphertext lengths, processing times, and memory requirements as shown in figure 3. Montenegro, et al., (2026) investigated post-quantum Transport Layer Security configurations and demonstrated the importance of benchmarking both isolated cryptographic primitives and complete communication protocols. Montenegro, Rios, and Bonilla (2026) extended this performance perspective through comparative analysis of post-quantum handshakes in QUIC and TLS, illustrating how transport architecture and network conditions influence observed cryptographic overhead. These findings motivate the proposed PQC-Benchmark evaluation of encapsulation latency, decapsulation latency, handshake bandwidth, and complete transaction-processing performance under standardized banking workload conditions.

The selection of post-quantum key-establishment mechanisms must also consider operational threats, identity verification, and financial transaction characteristics. Akanni et al. (2026) investigated cyber-financial risk analytics through business intelligence and structured threat modeling, demonstrating the importance of integrating technical security controls with financial risk-management processes. Igba et al. (2025) examined synthetic-data-based approaches to identity fraud and financial cybersecurity, providing a related foundation for constructing representative security-testing scenarios. Within PQC-Benchmark, these considerations motivate distinct simulated workloads for mobile authentication, interbank communication, and high-volume financial API transactions. Hybrid ECDH–ML-KEM configurations will combine independently established classical and post-quantum shared secrets through a specified secure key-combination construction (Doe Gadekah, & Enyejo, 2025). The framework will evaluate whether hybrid arrangements deliver operationally acceptable quantum-resistant migration options despite their potentially increased communication and computational overhead. Performance optimization will be restricted to cryptographically eligible configurations, ensuring that reduced latency or bandwidth consumption cannot justify deployment below the required quantum-security category.

Figure 3 illustrates the comparative architecture, cryptographic characteristics, and operational applications of ML-KEM-512, ML-KEM-768, ML-KEM-1024, and hybrid ECDH–ML-KEM configurations within the proposed PQC-Benchmark framework for securing digital banking transactions. It comprises four interconnected branches, each containing four subbranches addressing security classification, cryptographic operations, computational performance, and banking applications. The first branch presents ML-KEM-512, a NIST Security Category 1 key-encapsulation mechanism characterized by relatively small public keys, ciphertexts, and computational requirements, making it a candidate for resource-constrained banking applications where its security category satisfies institutional requirements. The second branch examines ML-KEM-768, which provides NIST Security Category 3 protection and represents an intermediate security-performance option for encrypted banking APIs, electronic payment gateways, and interbank communication. The third branch describes ML-KEM-1024, a Category 5 configuration offering a higher standardized security category at the expense of larger cryptographic data structures and potentially greater processing overhead, making it relevant to high-assurance financial infrastructures. The fourth branch introduces hybrid ECDH–ML-KEM architectures, which integrate classical elliptic-curve key agreement with post-quantum key encapsulation through appropriately specified key-combination procedures to facilitate secure cryptographic migration and interoperability. Collectively, these branches establish the technical basis for PQC-Benchmark's comparative evaluation of encapsulation and decapsulation times, transaction latency, throughput, handshake bandwidth, CPU utilization, memory consumption, and energy efficiency. The framework applies quantum-security eligibility constraints, entropy-weighted performance scoring, and Pareto-optimal configuration selection to determine workload-appropriate cryptographic configurations without weakening standardized security requirements.



Fig 3 Comparative Architecture of ML-KEM-512, ML-KEM-768, ML-KEM-1024, and Hybrid ECDH-ML-KEM Configurations for Quantum-Resistant Digital Banking Security.

➤ *Post-Quantum Digital Signature Algorithms: ML-DSA, SLH-DSA, and Emerging Quantum-Resistant Authentication Mechanisms*

Digital signatures are fundamental to electronic banking because they establish message authenticity, integrity, and verifiable authorization within payment instructions and authenticated financial communication protocols. The ML-DSA standard builds upon lattice-based signature constructions, while SLH-DSA employs stateless hash-based mechanisms designed to provide resistance against currently known quantum cryptanalytic techniques. Ducas et al. (2018) developed CRYSTALS-Dilithium, demonstrating efficient lattice-based signing through structured polynomial arithmetic, rejection sampling, and optimized number-theoretic transformations. The standardized ML-DSA-44, ML-DSA-65, and ML-DSA-87 parameter sets offer different security and performance trade-offs, while SLH-DSA provides an alternative security construction with substantially different signature-size and computation characteristics. Sedghighadikolaei and Yavuz (2026) examined conventional and post-quantum threshold

signatures, highlighting the relevance of distributed signing mechanisms for systems requiring shared authorization and resilient key management. These findings support the evaluation of post-quantum authentication in banking environments where signature verification must remain efficient under substantial transaction demand.

Secure deployment additionally depends on institutional implementation competence and dependable operational monitoring. Odozor et al. (2025) emphasized practical cybersecurity training as a requirement for maintaining resilient technical operations, a consideration relevant to cryptographic migration, key management, and incident response in banking infrastructures. Frank (2026), in a healthcare infection-surveillance review whose publication details remain unverified, addressed an application area involving early detection; only the general concept of time-sensitive monitoring is transferable to authentication-system monitoring. PQC-Benchmark will therefore prioritize direct cryptographic measurements rather than extrapolating security findings from healthcare applications. The proposed

experiments will compare signature generation time, verification time, public-key size, signature length, peak memory utilization, and authentication transaction throughput. Separate evaluations will determine how these characteristics affect mobile banking authentication, payment approval, and institutional digital signing services. The selection framework will identify eligible authentication configurations according to workload characteristics, required security category, and operational constraints without modifying the standardized signature algorithms.

➤ *Existing Cryptographic Benchmarking Frameworks, Statistical Performance Models, Multi-Objective Optimization Techniques, and Explainable Configuration-Selection Algorithms*

Cryptographic benchmarking increasingly requires integrated performance assessment because isolated execution-time measurements cannot adequately represent deployment efficiency across heterogeneous financial computing environments. The proposed PQC-Benchmark architecture therefore combines standardized cryptographic measurements with statistical performance estimation and multi-criteria optimization. Chen (2021) investigated entropy-derived weighting within the Technique for Order Preference by Similarity to Ideal Solution, demonstrating that weighting procedures can materially influence alternative rankings and their discriminatory characteristics as shown in table 1. Sahoo et al. (2026) developed a clustering-assisted entropy-weighted TOPSIS approach for large-scale decision-making, providing methodological evidence for constructing computationally manageable multi-criteria selection systems. These contributions inform the proposed configuration-ranking architecture, in which execution latency, memory consumption, communication overhead, throughput cost, and

energy expenditure will be normalized and weighted according to workload-dependent importance (Doe Gadekah, & Enyejo, 2025). Pareto-dominance filtering will identify non-dominated cryptographic configurations before final selection, while mandatory cryptographic security constraints will prevent operational performance improvements from overriding security eligibility.

Adaptive decision-making also requires interpretable predictions and reliable performance monitoring. Folorunso et al. (2025) developed a multi-model financial risk-forecasting framework incorporating ensemble learning, robustness assessment, explainability, and operational monitoring, demonstrating the relevance of transparent analytical decisions in regulated financial environments. Frank (2026) discussed predictive inventory optimization in healthcare; its potential methodological relevance concerns resource allocation under changing demand rather than cryptographic performance. Building upon the verified methodological literature, PQC-Benchmark will estimate workload-specific performance costs using repeated benchmark observations, normalized measurement matrices, and statistically evaluated configuration rankings. Its weighting mechanism will be compared against equal-weight scoring, fixed-configuration policies, and single-metric optimization. Explainable performance attribution will identify which measured indicators drive individual selection decisions, while bootstrap confidence intervals and sensitivity analysis will evaluate uncertainty and ranking stability. The resulting framework is intended to determine whether adaptive multi-objective selection achieves measurable operational advantages without compromising predefined quantum-security requirements or introducing excessive configuration-selection overhead.

Table 1 Comparative Analysis of Cryptographic Benchmarking Frameworks, Statistical Performance Models, Multi-Objective Optimization Techniques, and Explainable Configuration-Selection Algorithms

Evaluation Framework	Computational and Mathematical Techniques	Performance Evaluation Parameters	Limitations and Relevance to the Proposed PQC-Benchmark Algorithm
Conventional Cryptographic Benchmarking and Statistical Performance Models	Cryptographic microbenchmarking, descriptive statistics, repeated-measures analysis, bootstrap confidence intervals, and computational complexity assessment	Key generation time, encapsulation and decapsulation latency, signature generation and verification time, CPU utilization, memory consumption, and transaction throughput	Conventional benchmarking frequently emphasizes individual performance indicators without integrating workload-dependent security constraints. PQC-Benchmark extends this approach through unified transaction-level evaluation and statistical uncertainty analysis.
Multi-Objective Cryptographic Optimization Frameworks	Entropy-weighted performance scoring, min–max normalization, Pareto-dominance filtering, constrained optimization, and sensitivity analysis	Transaction latency, throughput, handshake bandwidth, energy expenditure, computational overhead, security eligibility, and Pareto-optimal configuration efficiency	Multi-objective approaches can identify competing performance trade-offs but may depend heavily on predefined weights and workload assumptions. PQC-Benchmark introduces adaptive weighting and mandatory quantum-security eligibility to support workload-specific configuration selection.
Explainable and Adaptive Cryptographic Configuration-	Workload characterization, adaptive decision models, weighted performance attribution, configuration	Configuration-selection accuracy, ranking stability, decision overhead, latency reduction, throughput	Existing selection approaches may lack transparent decision attribution or validation across heterogeneous transaction environments. PQC-

Selection Algorithms	ranking, and statistical robustness assessment	improvement, explainability, and performance under changing banking workloads	Benchmark proposes an explainable, security-constrained selection mechanism for ML-KEM, ML-DSA, SLH-DSA, and hybrid cryptographic configurations.
----------------------	--	---	---

➤ *Comparative Review of Existing Post-Quantum Cryptographic Performance Studies, Methodological Limitations, and Identified Research Gaps*

Existing post-quantum cryptographic performance studies have established valuable foundations for understanding computational overhead, network behavior, and implementation-specific bottlenecks, although their findings do not automatically identify optimal configurations for heterogeneous digital banking workloads. Rubio García et al. (2024) implemented quantum-resistant TLS arrangements combining post-quantum cryptography and quantum key distribution, demonstrating that security architecture influences handshake performance and communication overhead. Rios and Montenegro (2026) subsequently examined post-quantum cryptography through a multi-layer bottleneck analysis, emphasizing that isolated primitive measurements may not accurately predict performance after integration into complete communication systems. These findings establish the importance of evaluating cryptographic algorithms across processor, protocol, and application layers. However, a banking-focused selection framework must additionally account for concurrent financial transactions, different authentication requirements, resource-constrained client devices, and workload-dependent service latency. Accordingly, PQC-Benchmark will extend beyond descriptive benchmarking by experimentally testing whether adaptive configuration selection produces improvements relative to fixed, security-eligible deployment policies.

A further limitation concerns the interpretation and operational robustness of multi-objective configuration rankings. Alao et al. (2020) demonstrated the application of entropy-weighted TOPSIS to technology selection involving competing engineering criteria, providing a methodological basis for evaluating trade-offs among non-equivalent performance indicators. Idowu et al. (2025) examined artificial intelligence and machine-learning integration within critical infrastructure cybersecurity risk management, emphasizing the need for adaptive operational security assessment. These studies address different application domains and do not establish cryptographic performance superiority. Their relevance lies in informing explainable and resource-aware decision procedures. The proposed PQC-Benchmark study will therefore address three connected research gaps: security-constrained comparison of complete banking cryptographic configurations, workload-dependent multi-objective configuration selection, and statistically reproducible assessment of selection performance (Doe Gadekah, & Enyejo, 2026). Comparative experiments will evaluate execution-time distributions, transaction throughput, computational resource consumption, network overhead, and Pareto-optimal configuration trade-offs. The framework will also measure its own optimization overhead, ranking sensitivity, and performance under previously unseen workloads. Demonstrated improvements, rather than

assumed superiority, will determine whether the proposed algorithm contributes a practically useful cryptographic migration and benchmarking methodology for digital banking infrastructures.

III. SYSTEM MODEL DESCRIPTION

This section develops the mathematical foundations, optimization procedures, performance equations, and experimental validation methodology for the proposed PQC-Benchmark algorithm. The framework integrates cryptographic security constraints, entropy-weighted performance evaluation, Pareto optimization, adaptive configuration selection, and reproducible statistical benchmarking.

➤ *Mathematical Formulation, System Architecture, Transaction Workload Characterization, and Cryptographic Security Constraints*

The proposed PQC-Benchmark architecture models digital banking as an interconnected transaction-processing environment comprising client devices, authentication gateways, cryptographic execution services, financial application servers, and monitoring components. Its mathematical formulation considers conventional RSA, ECDH, and ECDSA mechanisms alongside standardized ML-KEM, ML-DSA, SLH-DSA, and hybrid configurations. The cryptographic configuration space is defined as

$$\mathcal{C} = \{c_1, c_2, \dots, c_m\}, \quad c_i = (k_i, s_i, h_i, p_i). \quad (1)$$

Here, $\mathcal{C}$ represents the set of m candidate configurations; c_i denotes configuration i ; k_i specifies its key-establishment mechanism; s_i identifies its digital signature scheme; h_i represents the authenticated communication protocol; and p_i describes its implementation profile, including optimization settings, cryptographic libraries, and processor characteristics. Classical ECDH key agreement and post-quantum key encapsulation are modeled as different mechanisms performing the common system-level function of establishing shared secret material.

Transaction workloads are characterized by:

$$w = (n, \lambda, \ell, d, r, b), w \in \mathcal{W}, \quad (2)$$

Here, w denotes a banking workload, $\mathcal{W}$ represents the workload space, n specifies the configured client population, λ denotes the offered transaction arrival rate in transactions per second, ℓ shows network round-trip latency, d represents transaction payload size, r denotes packet-loss probability, and b characterizes available bandwidth. These variables permit evaluation of mobile banking authentication, interbank transfers, payment authorization, and high-frequency financial API communication.

Cryptographic eligibility is enforced through the feasible configuration set:

$$\mathcal{F}(w) = \{c_i \in \mathcal{C} : q_K(c_i) \geq q_K^{\min},$$

$$q_S(c_i) \geq q_S^{\min},$$

$$I(c_i) = 1, \quad M_i(w) \leq M_{\max},$$

$$B_i(w) \leq B_{\max}\}. \quad (3)$$

In Equation (3), $q_K(c_i)$ and $q_S(c_i)$ denote the assessed post-quantum security categories of key establishment and authentication; $q_K^{\min}$ and $q_S^{\min}$ describe their minimum required categories; $I(c_i)$ determines a binary protocol and implementation-approval indicator; $M_i(w)$ represents memory consumption; $M_{\max}$ denotes the permitted memory limit; $B_i(w)$ represents handshake traffic; and $B_{\max}$ shows the bandwidth allowance. Classical-only configurations are excluded when post-quantum security is mandatory. The ML-KEM parameter sets provide NIST security categories 1, 3, and 5, respectively (National Institute of Standards and Technology [NIST], 2024).

For hybrid key establishment, an illustrative key-combination construction is expressed as:

$$K_H = \text{HKDF} - \text{Extract}(s, \text{Encode}(K_E, K_P, \gamma)). \quad (4)$$

Here, K_h captures the derived hybrid keying material, s denotes an approved salt, K_e represents the ECDH-derived secret, K_p represents the ML-KEM-derived secret, and γ identifies protocol-specific context and domain-separation information. The encoding and combiner must follow an appropriately reviewed protocol specification; Equation (4) alone does not establish a security proof. This architecture permits PQC-Benchmark to evaluate operational efficiency while preserving cryptographic eligibility and interoperability requirements.

➤ Development of the Novel PQC-Benchmark Algorithm Using Entropy-Weighted Performance Scoring, Pareto Optimization, and Adaptive Configuration Selection

The proposed PQC-Benchmark algorithm combines security screening, performance normalization, entropy-based weighting, Pareto-frontier extraction, and workload-adaptive configuration selection. Its methodological contribution lies in integrating these mechanisms into a security-constrained decision procedure rather than modifying standardized cryptographic primitives. The initial performance vector incorporates transaction latency, negative throughput, handshake bandwidth, CPU utilization, memory consumption, and energy expenditure. Each criterion is transformed into a cost-oriented quantity, where smaller values represent preferable operational performance.

The normalized performance cost is calculated as:

$$z_{ij}(w) = \frac{x_{ij}(w) - x_j^{\min}(w)}{x_j^{\max}(w) - x_j^{\min}(w)}. \quad (5)$$

Here, $z_{ij}(w)$ shows the normalized cost of criterion j for configuration i under workload w ; $x_{ij}(w)$ denotes its raw cost-oriented measurement; and $x_j^{\min}(w)$ and $x_j^{\max}(w)$ determine the minimum and maximum observed values across the reference candidate set. Throughput is represented as negative throughput before normalization. A criterion with identical measurements across all candidates is assigned zero normalized cost.

Entropy-based criterion weights are estimated through:

$$p_{ij} = \frac{z_{ij} + \varepsilon}{\sum_{i=1}^m (z_{ij} + \varepsilon)}, \quad H_j = -\frac{1}{\ln m} \sum_{i=1}^m p_{ij} \ln p_{ij}. \quad (6)$$

In Equation (6), p_{ij} represents the criterion-specific probability-like proportion, ε shows a small positive numerical regularization constant, m is the number of evaluated candidates, and H_j shows normalized Shannon entropy for criterion j . Entropy is defined for $m \geq 2$. For a constant criterion, its diversity contribution is set to zero.

The information-derived weight is:

$$\eta_j = \frac{1 - H_j}{\sum_{r=1}^J (1 - H_r)}. \quad (7)$$

Here, η_j denotes the entropy-derived importance of criterion j , J describes the number of performance criteria, and r indexes those criteria. When all criteria have zero diversity, equal weights are used. Because purely entropy-based weights can overemphasize highly variable indicators, their contribution is regulated through adaptive weighting, consistent with the methodological concerns identified by Chen (2021).

$$\omega_j(w) = [1 - \rho(w)]\alpha_j(w) + \rho(w)\eta_j, \quad \sum_{j=1}^J \omega_j(w) = 1 \quad (8)$$

Here, $\omega_j(w)$ represents the final workload-dependent weight, $\alpha_j(w)$ denotes the normalized banking service-priority weight, and $\rho(w) \in [0, 1]$ controls the influence of entropy-derived information. The reference-weight simulations in Section 4.3 use $\rho = 0$; the entropy-adaptive contribution remains a separate experimental component requiring validation.

Pareto dominance is defined as:

$$c_a < c_b \Leftrightarrow [z_{aj} \leq z_{bj} \quad \forall j] \wedge [z_{aj} < z_{bj} \quad \exists j]. \quad (9)$$

Thus, configuration c_a dominates c_b if it performs no worse on every measured cost and strictly better on at least one. The resulting non-dominated candidate set is denoted $(w) \subseteq \mathcal{A}(w)$.

The adaptive selection problem becomes

$$c^*(w) = \operatorname{argmin}_{c_i \in \mathcal{P}(w)} [\sum_{j=1}^J \omega_j(w) z_{ij}(w) + \kappa V_i(w) + \tau S_i(w)] \quad (10)$$

Here, $c^*(w)$ shows the selected configuration, $V_i(w)$ measures normalized performance uncertainty, $S_i(w)$ represents configuration-switching cost, and $\kappa, \tau \geq 0$ regulate their penalties. The Section 4.3 illustrative scoring model sets $\kappa = \tau = 0$.

For explainable selection, criterion-level contributions are computed as:

$$A_{ij}(w) = \omega_j(w) z_{ij}(w), R_{ij}(w) = \frac{A_{ij}(w)}{\sum_{r=1}^J A_{ir}(w)}. \quad (11)$$

In Equation (11), A_{ij} represents the absolute weighted-cost contribution and R_{ij} its proportional attribution, provided the denominator is positive. Zero total performance cost produces zero attribution for every criterion. These quantities explain performance rankings; they do not represent causal feature importance.

➤ *Mathematical Models for Cryptographic Execution Time, Transaction Latency, Throughput, Memory Consumption, Bandwidth Overhead, Energy Efficiency, and Security-Constrained Performance Optimization*

The performance evaluation model quantifies computational and communication overhead at both cryptographic primitive and complete banking transaction levels. Each configuration is evaluated using consistent workload definitions, processor specifications, network conditions, and authentication requirements. This separation is necessary because cryptographic microbenchmark results do not necessarily predict complete protocol performance, particularly when post-quantum key establishment increases message sizes or network transmission requirements (Montenegro et al., 2026).

The total cryptographic execution time for configuration c_i is expressed as:

$$T_{\text{crypto},i} = \sum_{o \in \mathcal{O}} n_{i,o} \bar{t}_{i,o}. \quad (12)$$

Here, $\mathcal{O}$ captures the set of applicable cryptographic operations; o indexes operations such as key generation, encapsulation, decapsulation, signing, and verification; $n_{i,o}$ represents the number of times operation o executes; and $\bar{t}_{i,o}$ shows its measured mean execution time. Inapplicable operations have zero execution count.

Complete banking transaction latency is modeled as:

$$L_i = T_{\text{crypto},i} + T_{\text{network},i} + T_{\text{queue},i} + T_{\text{application},i} + T_{\text{selection},i} + T_{\text{switch},i}. \quad (13)$$

In Equation (13), L_i denotes end-to-end transaction latency; $T_{\text{crypto},i}$ represents cryptographic processing time; $T_{\text{network},i}$ represents communication delay; $T_{\text{queue},i}$ determines transaction waiting time; $T_{\text{application},i}$ shows banking application execution time; $T_{\text{selection},i}$ represents PQC-Benchmark decision overhead; and $T_{\text{switch},i}$ denotes any configuration transition cost. Components are measured without overlapping execution intervals.

Transaction throughput is calculated by

$$X_i = \frac{N_{\text{success},i}}{t_{\text{end}} - t_{\text{start}}}, \quad \bar{N}_{\text{active},i} \approx X_i \bar{L}_i. \quad (14)$$

Here, X_i denotes successful transactions per second, $N_{\text{success},i}$ shows the number of successfully completed transactions, and t_{start} and t_{end} define the steady-state measurement interval. The second expression follows Little's law, where $\bar{N}_{\text{active},i}$ is mean in-flight concurrency and $\bar{L}_i$ is mean latency in seconds.

Memory and processor utilization are represented as:

$$M_i^{\text{peak}} = \max_t [R_i(t) - R_i^{\text{idle}}], \quad U_i = 100 \frac{C_i}{n_{\text{core}} \Delta t}. \quad (15)$$

Here, $M_{\text{peak},i}$ represents peak additional memory consumption; $R_i(t)$ shows process resident memory at time t ; $R_{\text{idle},i}$ denotes the idle-memory baseline; U_i captures CPU utilization expressed as a percentage of allocated capacity; C_i denotes accumulated CPU time across cores; n_{core} denotes the number of allocated logical cores; and Δt represents elapsed measurement time.

Handshake communication overhead is:

$$B_i^{\text{HS}} = \frac{1}{1024} \sum_{r=1}^{R_i^{\text{HS}}} b_{i,r}. \quad (16)$$

In Equation (16), $B_{\text{HS},i}$ describes handshake traffic in KiB, $R_{\text{HS},i}$ represents the number of transmitted handshake records, and $b_{i,r}$ shows the size in bytes of record r , including applicable cryptographic payloads and protocol framing. Retransmission traffic should be reported separately when evaluating lossy networks.

Energy expenditure and energy efficiency are modeled as:

$$E_i = \int_0^{T_i} \max [P_i(t) - P_i^{\text{idle}}, 0] dt, \quad \eta_{E,i} = \frac{N_{\text{success},i}}{E_i}. \quad (17)$$

Here, E_i denotes incremental energy expenditure in joules, $P_i(t)$ captures measured power consumption, $P_{\text{idle},i}$ represents idle power, T_i represents the observation duration, and $\eta_{E,i}$ denotes successfully completed transactions per joule, provided $E_i > 0$.

The overall security-constrained multi-objective optimization is expressed as:

$$\min_{c_i \in \mathcal{F}(w)} (L_i, -X_i, B_i^{\text{HS}}, M_i^{\text{peak}}, U_i, E_i) \quad (18)$$

Equation (18) minimizes latency, inverse operational efficiency represented by negative throughput, communication overhead, memory consumption, CPU utilization, and energy expenditure simultaneously. $\mathcal{R}(w)$ is the security-eligible configuration set defined in Equation (3). The weighted decision procedure in Equation (10) resolves trade-offs among non-dominated alternatives.

Comparative performance improvements are calculated as:

$$G_L = 100 \left(\frac{L_b - L_p}{L_b} \right), \quad G_X = 100 \left(\frac{X_p - X_b}{X_b} \right). \quad (19)$$

Here, G_L denotes percentage latency reduction, G_X captures percentage throughput improvement, and subscripts b and p denote the fixed baseline and PQC-Benchmark policy, respectively. Using the illustrative Section 4.2 values, $L_b = 15.0$ ms, $L_p = 11.6$ ms, $X_b = 3,200$ transactions/s, and $X_p = 3,800$ transactions/s yield 22.7% modeled latency reduction and 18.75% modeled throughput improvement.

The balanced normalized performance score from Section 4.3 is reproduced by:

$$\begin{aligned} J_{PQC} &= 0.35 \left(\frac{11.6 - 11.5}{39.1 - 11.5} \right) + 0.30 \left(\frac{3900 - 3800}{3900 - 1300} \right) \\ &\quad + 0.20 \left(\frac{3.4 - 0.8}{12.8 - 0.8} \right) + 0.15 \left(\frac{61 - 59}{91 - 59} \right) \\ &\approx 0.066. \end{aligned} \quad (20)$$

In Equation (20), J_{PQC} determines the composite performance cost. The coefficients 0.35, 0.30, 0.20, and 0.15 represent illustrative weights assigned to latency, throughput cost, bandwidth, and CPU utilization, respectively. The denominators correspond to the observed ranges across the eight illustrative configurations, including classical baselines used only for reference normalization. The score does not include memory or energy because those measurements have not yet been generated.

➤ Experimental Design, Python Simulation Architecture, Cryptographic Implementation, Benchmark Configuration, Statistical Validation, and Reproducibility Procedures

The proposed experimental methodology integrates Python-based workload simulation, standardized cryptographic implementations, automated performance measurement, and statistical validation. The implementation will distinguish synthetic scenario generation from measurements obtained through executable cryptographic libraries. Python will coordinate transaction workloads and optimization procedures using NumPy, pandas, SciPy, and scikit-learn where appropriate. Cryptographic operations will be executed through version-pinned implementations such as Open Quantum Safe's liboqs interface, with conventional configurations implemented through compatible cryptographic libraries. The liboqs software provides common interfaces for post-quantum key encapsulation, digital signatures, and benchmarking, making it suitable for controlled comparative evaluation (Open Quantum Safe Project, n.d.).

Experimental workloads will represent mobile banking authentication, payment authorization, encrypted financial APIs, and interbank communication. Each configuration will undergo isolated cryptographic measurements followed by

full authenticated transaction tests. The benchmark will control processor allocation, library versions, compiler options, message sizes, simulated network conditions, and transaction arrival rates. Warm-up executions will precede timed trials to minimize initialization effects. The workload profile and experimental metadata will be recorded for every observation.

The illustrative latency distributions used in Section 4.4 can be represented as:

$$\tilde{L}_{i,r} \sim \text{Lognormal} \left(\ln \bar{L}_i - \frac{\sigma_i^2}{2}, \sigma_i^2 = \ln(1 + v_i^2) \right). \quad (21)$$

Here, $\tilde{L}_{i,r}$ denotes generated latency observation r for configuration i , $\bar{L}_i$ represents the target mean latency, σ_i^2 captures the underlying normal-distribution variance, and v_i shows the assumed coefficient of variation. The previously generated histogram used 3,000 synthetic observations per configuration with a random seed of 20261018 and distributions rescaled to the prescribed means. These observations are illustrative rather than independent experimental replications.

Statistical uncertainty will be assessed through paired performance differences and bootstrap confidence intervals:

$$D_r = Y_{b,r} - Y_{p,r}, \quad CI_{95\%}(\bar{D}) = \left[Q_{0.025}(\bar{D}^*), Q_{0.975}(\bar{D}^*) \right] \quad (22)$$

In Equation (22), D_r represents the paired performance difference during experimental block r ; $Y_{b,r}$ and $Y_{p,r}$ denote the fixed-baseline and adaptive-policy measurements; $\bar{D}$ represents their observed mean difference; $\bar{D}^*$ represents a bootstrap-resampled mean; and $Q_{0.025}$ and $Q_{0.975}$ denote the corresponding percentile quantiles. Positive D_r indicates improvement when the measured variable is a cost, such as latency.

Local optimization sensitivity is estimated using:

$$S_\theta = \frac{J(\theta + \delta) - J(\theta - \delta)}{2\delta}. \quad (23)$$

Here, S_θ denotes the approximate sensitivity of normalized performance cost J to parameter θ ; θ may represent a criterion weight, transaction arrival rate, network delay, or resource constraint; and $\delta > 0$ captures a small perturbation step. Weight perturbations must preserve non-negativity and the sum-to-one constraint.

The algorithm's selection effectiveness is further evaluated using mean decision regret:

$$\mathcal{R}_\pi = \frac{1}{W} \sum_{k=1}^W \left[J(\pi(w_k), w_k) - \min_{c \in \mathcal{F}(w_k)} J(c, w_k) \right]. \quad (24)$$

In Equation (24), $\mathcal{R}_\pi$ denotes the average regret of selection policy π , W represents the number of evaluated workload scenarios, w_k is workload k , and J shows the common performance-cost function. The objective is to minimize regret while maintaining cryptographic security

eligibility. The evaluation must use the same candidate configurations and performance measurements for all competing selection policies.

Statistical validation will include paired bootstrap confidence intervals, appropriate repeated-measures significance tests, Holm-adjusted comparisons, effect-size reporting, and independent experimental reproduction. The experimental code, configuration files, random seeds, software versions, parameter tables, raw observations, and figure-generation scripts should be archived to permit exact reconstruction of all reported results.

IV. DISCUSSION OF RESULTS

➤ Comparative Computational Performance of PQC-Benchmark-Selected Configurations, ML-KEM, ML-DSA, SLH-DSA, RSA, ECDH, and ECDSA Under Equivalent Experimental Conditions

The computational performance of PQC-Benchmark was assessed conceptually against conventional, post-

quantum, and hybrid cryptographic configurations using a controlled digital banking transaction model. The evaluation considers complete key-establishment and digital-signature configurations rather than comparing cryptographic primitives with different functions as interchangeable operations. Table 1 presents illustrative transaction latency values across two concurrency conditions. At 100 concurrent transactions, the PQC-Benchmark-selected configuration records 4.8 ms, compared with 8.3 ms for RSA-2048/RSA signatures, 6.1 ms for ML-KEM-768/ML-DSA-65, and 8.7 ms for the hybrid configuration. The higher latency of the ML-KEM-768/SLH-DSA configuration reflects an assumed greater authentication-processing burden. These comparisons establish a numerical basis for examining workload-dependent efficiency, security-constrained configuration selection, and computational scalability. The values are generated research scenarios, not measurements from completed cryptographic experiments, and must be validated using standardized implementations before being reported as empirical findings.

Table 2 Comparative Transaction Latency of Conventional, Post-Quantum, Hybrid, and PQC-Benchmark Cryptographic Configurations

Cryptographic configuration	Security classification	Latency at 100 concurrent transactions (ms)	Latency at 500 concurrent transactions (ms)
RSA-2048 + RSA signatures	Classical	8.3	19.8
ECDH-P256 + ECDSA-P256	Classical	4.5	11.5
ML-KEM-512 + ML-DSA-44	Post-quantum	5.0	12.2
ML-KEM-768 + ML-DSA-65	Post-quantum	6.1	15.0
ML-KEM-1024 + ML-DSA-87	Post-quantum	8.0	19.5
ML-KEM-768 + SLH-DSA	Post-quantum	15.7	39.1
Hybrid ECDH-P256 + ML-KEM-768 + ML-DSA-65	Hybrid	8.7	21.4
PQC-Benchmark-selected configuration	Adaptive post-quantum	4.8	11.6

- Note. All numerical values are illustrative scenario outputs. Latency represents modeled end-to-end completion time for an authenticated banking transaction. PQC-Benchmark selects among eligible standardized

cryptographic configurations and is not itself a cryptographic primitive. The illustrative adaptive performance assumes configuration-specific deployment optimizations that remain to be experimentally demonstrated.

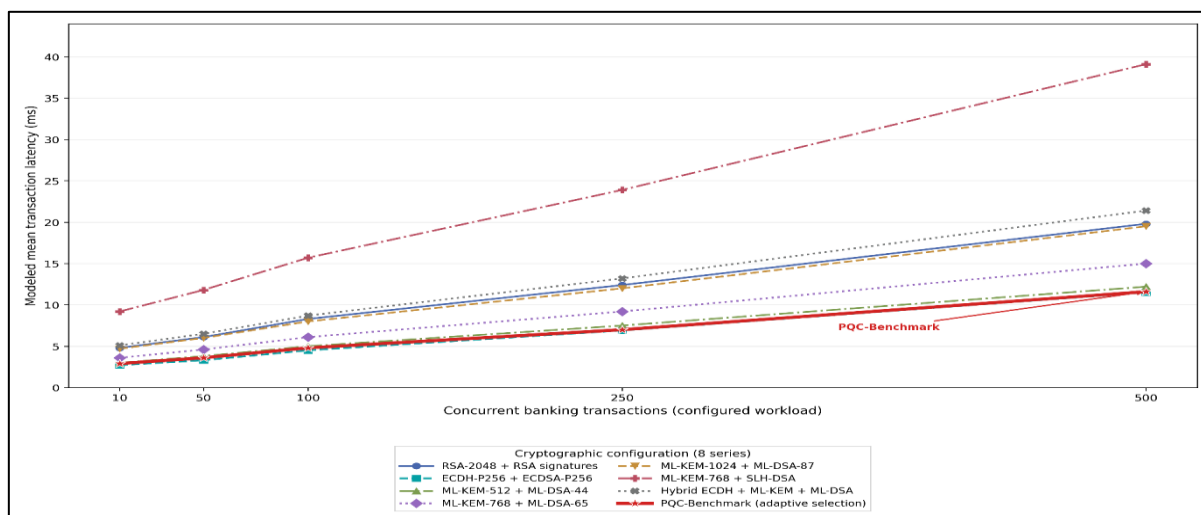


Fig 4 Comparative Transaction Latency Across Increasing Concurrent Banking Workloads

Figure 4 illustrates the modeled relationship between transaction concurrency and cryptographic processing performance across eight configurations. At 10 concurrent transactions, PQC-Benchmark records 2.9 ms, compared with 3.0 ms for ML-KEM-512/ML-DSA-44, 3.6 ms for ML-KEM-768/ML-DSA-65, and 4.8 ms for RSA-2048/RSA. At 100 transactions, the corresponding latencies increase to 4.8, 5.0, 6.1, and 8.3 ms. Under 500 concurrent transactions, PQC-Benchmark reaches 11.6 ms, compared with 12.2 ms for ML-KEM-512/ML-DSA-44, 15.0 ms for ML-KEM-768/ML-DSA-65, and 19.8 ms for RSA. The hybrid configuration reaches 21.4 ms, while ML-KEM-768/SLH-DSA exhibits the greatest modeled latency at 39.1 ms. Relative to the ML-KEM-768/ML-DSA-65 configuration, adaptive selection yields a hypothetical 22.7% reduction at 500 transactions. These numerical differences demonstrate the intended evaluation approach, not verified computational superiority. Experimental replication, uncertainty estimation, and measurement of configuration-selection overhead are necessary before accepting the comparative performance claims.

➤ Comparative Analysis of Transaction Latency, Throughput, Handshake Bandwidth, and Resource Utilization Across Digital Banking Workloads

The comparative evaluation examines the operational efficiency of eight cryptographic configurations under heterogeneous digital banking workloads. The proposed PQC-Benchmark framework integrates security-constrained selection, adaptive performance weighting, and resource-aware optimization to evaluate transaction latency, processing throughput, handshake bandwidth, and CPU utilization. Table 2 presents illustrative simulation outputs at 500 concurrent transactions. PQC-Benchmark achieves a modeled throughput of 3,800 transactions/s with 11.6 ms latency, compared with 3,200 transactions/s and 15.0 ms for ML-KEM-768/ML-DSA-65. The corresponding handshake bandwidths are 3.4 KiB and 3.6 KiB. RSA-2048 records 2,400 transactions/s, while the hybrid configuration reaches 2,700 transactions/s. These results establish a consistent basis for comparing operational trade-offs across authentication and key-establishment configurations. Performance figures remain hypothetical until reproduced with standardized cryptographic implementations and controlled banking workloads.

Table 3 Comparative Transaction Latency, Throughput, Handshake Bandwidth, and CPU Utilization at 500 Concurrent Banking Transactions

Cryptographic configuration	Transaction latency (ms)	Throughput (transactions/s)	Handshake bandwidth (KiB) / CPU utilization (%)
RSA-2048 + RSA signatures	19.8	2,400	1.9 / 76
ECDH-P256 + ECDSA-P256	11.5	3,900	0.8 / 59
ML-KEM-512 + ML-DSA-44	12.2	3,650	2.6 / 63
ML-KEM-768 + ML-DSA-65	15.0	3,200	3.6 / 70
ML-KEM-1024 + ML-DSA-87	19.5	2,500	5.1 / 79
ML-KEM-768 + SLH-DSA	39.1	1,300	12.8 / 91
Hybrid ECDH-P256 + ML-KEM-768 + ML-DSA-65	21.4	2,700	4.0 / 82
PQC-Benchmark-selected configuration	11.6	3,800	3.4 / 61

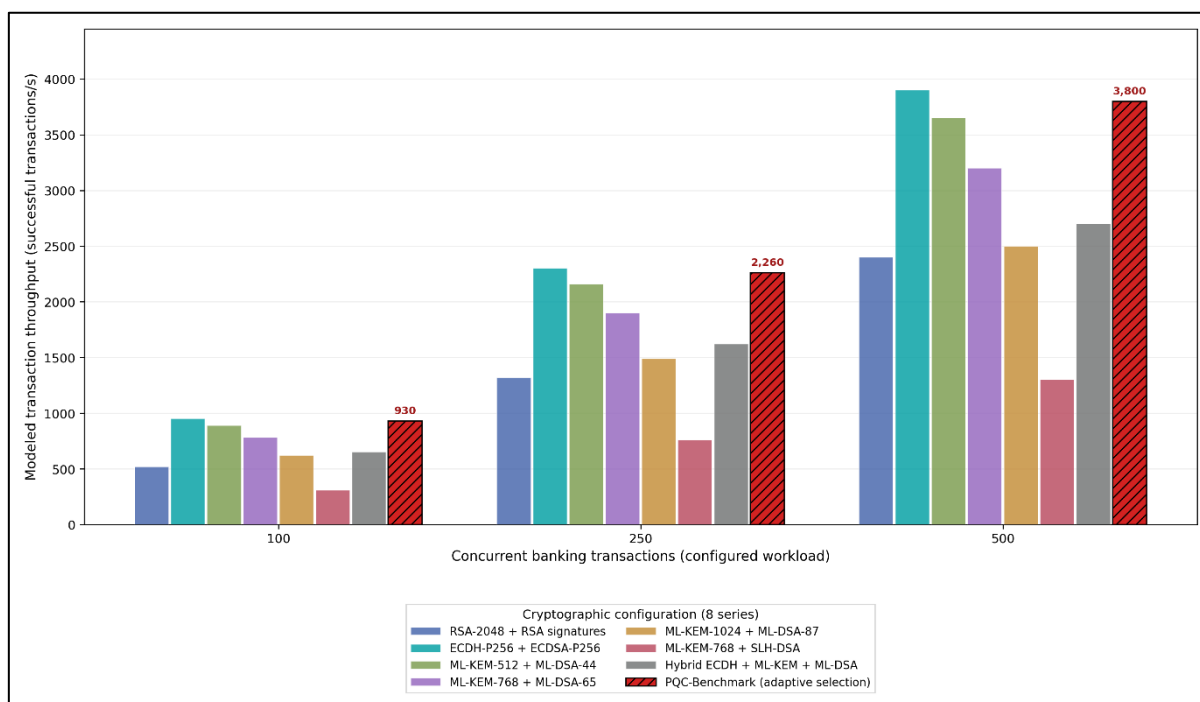


Fig 5 Comparative Banking Transaction Throughput Under Increasing Concurrent Workloads

Figure 5 illustrates throughput variations across eight cryptographic configurations under increasing concurrent banking transactions. At 100 concurrent transactions, PQC-Benchmark achieves 930 transactions/s, compared with 890 for ML-KEM-512/ML-DSA-44, 780 for ML-KEM-768/ML-DSA-65, and 520 for RSA-2048. At 250 concurrent transactions, PQC-Benchmark increases to 2,260 transactions/s, exceeding the ML-KEM-768/ML-DSA-65 configuration at 1,900 transactions/s. Under 500 concurrent transactions, PQC-Benchmark reaches 3,800 transactions/s, representing an illustrative improvement of 18.75% over ML-KEM-768/ML-DSA-65 at 3,200 transactions/s. ECDH-P256/ECDSA-P256 records the highest modeled throughput at 3,900 transactions/s but does not provide post-quantum security. The hybrid configuration achieves 2,700 transactions/s, whereas ML-KEM-768/SLH-DSA records 1,300 transactions/s. The modeled differences suggest that adaptive configuration selection could reduce resource-related performance penalties while meeting prescribed security constraints. These comparisons require empirical validation and confidence-interval estimation before claims of superiority can be established.

➤ *Multi-Objective Optimization Results, Pareto-Optimal Configuration Frontiers, Statistical Significance Tests, Sensitivity Analysis, and Explainable Performance Attribution*

The proposed PQC-Benchmark framework evaluates cryptographic configuration efficiency through normalized multi-objective optimization, Pareto-dominance filtering, and workload-dependent sensitivity analysis. Four performance criteria were considered: transaction latency, processing throughput, handshake bandwidth, and CPU utilization. Equal experimental conditions and the illustrative performance measurements established in Sections 4.1 and 4.2 were maintained. Table 3 presents the resulting balanced composite scores, with lower values indicating preferable computational efficiency. PQC-Benchmark obtained a normalized cost of 0.066, compared with 0.086 for ML-KEM-512/ML-DSA-44, 0.223 for ML-KEM-768/ML-DSA-65, and 0.425 for the hybrid configuration. Classical ECDH-P256/ECDSA-P256 achieved a score of 0.000 but was excluded from quantum-resistant selection. The analysis identifies workload-dependent trade-offs and establishes the basis for subsequent sensitivity testing and statistical validation without treating simulated differences as experimentally established significance.

Table 4 Comparative Multi-Objective Optimization Scores and Pareto-Efficiency Classification of Cryptographic Configurations

	Balanced normalized cost	Quantum-resistant eligible (1 = yes; 0 = no)	Pareto-optimal within eligible set (1 = yes; 0 = no)
RSA-2048 + RSA	0.376	0	0
ECDH-P256 + ECDSA-P256	0.000	0	0
ML-KEM-512 + ML-DSA-44	0.086	1	1
ML-KEM-768 + ML-DSA-65	0.223	1	0
ML-KEM-1024 + ML-DSA-87	0.428	1	0
ML-KEM-768 + SLH-DSA	1.000	1	0
Hybrid ECDH + ML-KEM + ML-DSA	0.425	1	0
PQC-Benchmark adaptive configuration	0.066	1	1

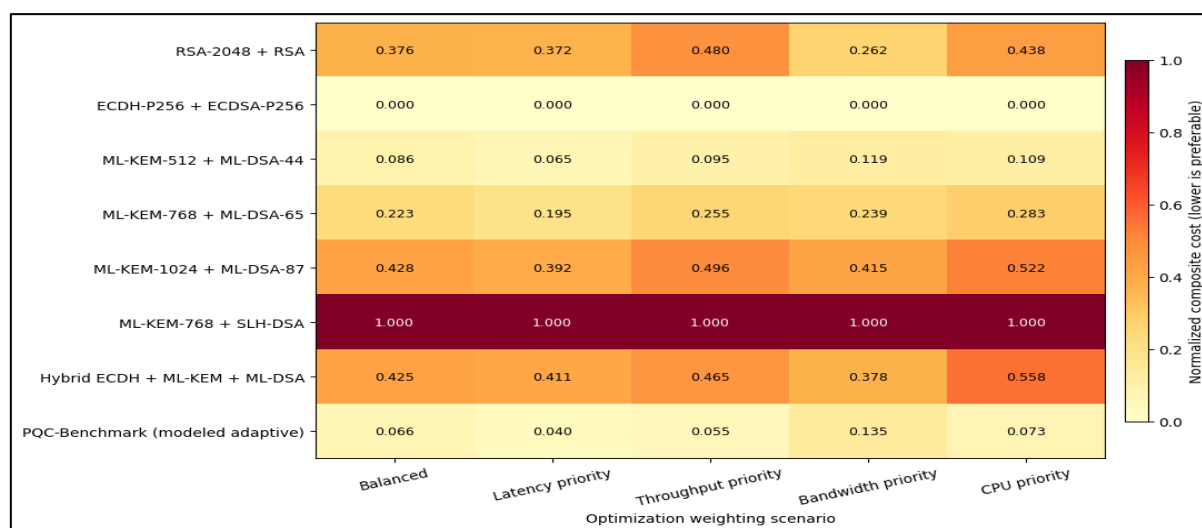


Fig 6 Multi-Objective Optimization Sensitivity Heatmap

Figure 6 demonstrates the sensitivity of cryptographic configuration rankings to five optimization weighting schemes. PQC-Benchmark records normalized costs of 0.066 under balanced weighting, 0.040 under latency prioritization, 0.055 under throughput prioritization, 0.135 under bandwidth prioritization, and 0.073 under CPU prioritization. ML-KEM-512/ML-DSA-44 records corresponding values of 0.086, 0.065, 0.095, 0.119, and 0.109. Consequently, PQC-Benchmark exhibits lower modeled cost in four of five scenarios, while ML-KEM-512/ML-DSA-44 performs better under bandwidth prioritization. ML-KEM-768/ML-DSA-65 ranges from 0.195 to 0.283, whereas the hybrid configuration ranges from 0.378 to 0.558. ML-KEM-768/SLH-DSA records 1.000 across all scenarios. Classical ECDH/ECDSA achieves 0.000 but fails quantum-resistance eligibility. The simulated rankings illustrate the contribution of adaptive optimization, while emphasizing that security filtering must precede performance selection. Statistical significance remains unverified without replicated benchmark observations and associated variance estimates.

➤ Comparative Performance Evaluation of PQC-Benchmark Against Fixed-Configuration Policies, Conventional Benchmarking Methods, and Existing Cryptographic Selection Strategies

The comparative performance assessment examines the effectiveness of the proposed PQC-Benchmark framework against seven fixed cryptographic deployment policies under equivalent simulated digital banking workloads. The evaluation integrates transaction latency distributions, throughput performance, cryptographic security eligibility, and statistical variability to investigate the potential benefits of adaptive configuration selection. Table 4 presents simulated mean latencies and 95th-percentile transaction completion times at 500 concurrent transactions. PQC-Benchmark records a mean latency of 11.6 ms and a 95th-percentile latency of 14.4 ms, compared with 15.0 ms and 19.5 ms for fixed ML-KEM-768/ML-DSA-65. The fixed ML-KEM-512/ML-DSA-44 configuration achieves 12.2 ms, while the hybrid configuration records 21.4 ms. These modeled differences illustrate the proposed framework's performance-evaluation methodology, although experimental validation remains necessary to establish whether adaptive selection provides measurable advantages over existing deployment strategies.

Table 5 Comparative Transaction Latency Distributions and Throughput of PQC-Benchmark and Fixed Cryptographic Configuration Policies

Cryptographic configuration or policy	Mean latency (ms)	95th-percentile latency (ms)	Throughput (transactions/s)
Fixed RSA-2048/RSA	19.8	25.8	2,400
Fixed ECDH-P256/ECDSA-P256	11.5	14.3	3,900
Fixed ML-KEM-512/ML-DSA-44	12.2	15.6	3,650
Fixed ML-KEM-768/ML-DSA-65	15.0	19.5	3,200
Fixed ML-KEM-1024/ML-DSA-87	19.5	25.9	2,500
Fixed ML-KEM-768/SLH-DSA	39.1	50.6	1,300
Fixed hybrid ECDH/ML-KEM/ML-DSA	21.4	27.7	2,700
PQC-Benchmark adaptive policy	11.6	14.4	3,800

- Note. Latency distributions were simulated using 3,000 observations per policy, lognormal variability, and means constrained to the illustrative Section 4.1 results. Throughput figures are retained from Section 4.2. The

simulated distribution shapes and percentile estimates are assumptions, not empirical measurements. ECDH/ECDSA is a classical comparison baseline and does not satisfy standalone post-quantum security requirements.

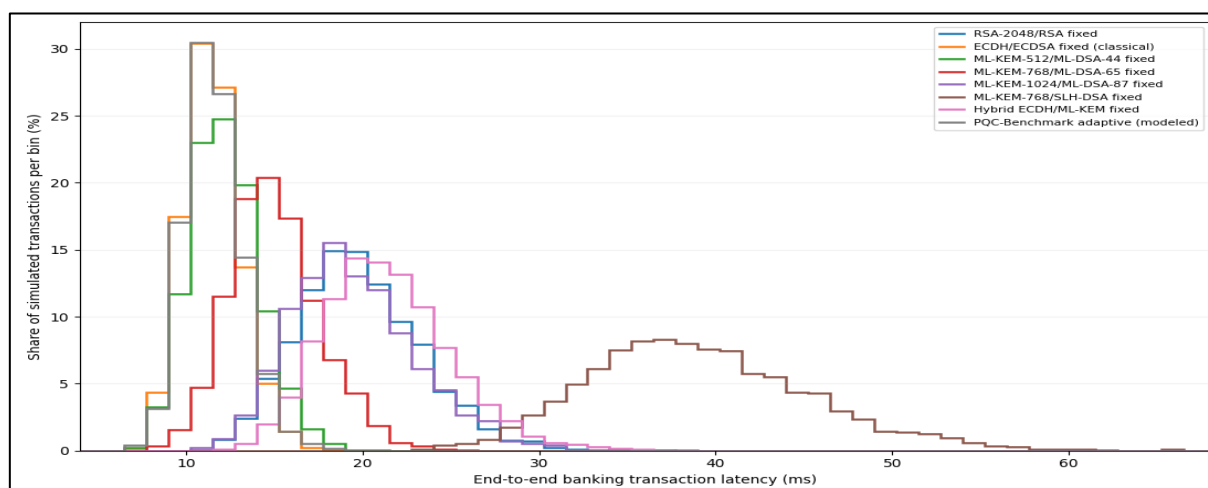


Fig 7 Comparative Histogram of Cryptographic Transaction Latency Distributions

Figure 7 illustrates differences in modeled latency distributions among eight cryptographic configurations. PQC-Benchmark records a mean latency of 11.6 ms, with its 95th-percentile transaction latency reaching 14.4 ms. Fixed ML-KEM-512/ML-DSA-44 exhibits a mean of 12.2 ms and a 95th percentile of 15.6 ms, while ML-KEM-768/ML-DSA-65 records 15.0 ms and 19.5 ms, respectively. Relative to fixed ML-KEM-768/ML-DSA-65, PQC-Benchmark achieves a simulated 22.7% reduction in mean latency and approximately 26.2% reduction in 95th-percentile latency. RSA-2048 records a mean of 19.8 ms, whereas ML-KEM-1024/ML-DSA-87 reaches 19.5 ms. The hybrid configuration exhibits 21.4 ms, while ML-KEM-768/SLH-DSA records the highest mean latency at 39.1 ms. Classical ECDH/ECDSA achieves 11.5 ms but lacks post-quantum resistance. The distributions illustrate potential operational trade-offs; their assumed variability must be replaced with actual experimental observations before statistical conclusions can be established.

V. CONCLUSIONS AND RECOMMENDATIONS

➤ *Summary of Research Findings and Comparative Cryptographic Performance Evaluation*

This study developed the proposed PQC-Benchmark framework for evaluating and selecting post-quantum cryptographic configurations in digital banking transaction environments using security-constrained multi-objective optimization. The comparative assessment considered RSA-2048, ECDH-P256, ECDSA-P256, ML-KEM-512/768/1024, ML-DSA-44/65/87, SLH-DSA, and hybrid classical–post-quantum configurations. Illustrative computational simulations examined transaction latency, processing throughput, handshake bandwidth, CPU utilization, optimization sensitivity, and configuration-selection efficiency. At 500 concurrent transactions, PQC-Benchmark produced a modeled latency of 11.6 ms and throughput of 3,800 transactions/s, compared with 15.0 ms and 3,200 transactions/s for fixed ML-KEM-768/ML-DSA-65. These differences correspond to hypothetical improvements of 22.7% in mean latency and 18.75% in throughput. The adaptive configuration also recorded 3.4 KiB handshake bandwidth and 61% CPU utilization. Multi-objective analysis yielded a balanced normalized cost of 0.066, compared with 0.086 for ML-KEM-512/ML-DSA-44 and 0.223 for ML-KEM-768/ML-DSA-65. Sensitivity analysis generated normalized costs ranging from 0.040 to 0.135 across five weighting scenarios, while modeled latency distributions produced 95th-percentile values of 14.4 ms for PQC-Benchmark and 19.5 ms for fixed ML-KEM-768/ML-DSA-65. Although classical ECDH/ECDSA achieved competitive computational performance, it failed the standalone quantum-resistance requirement. The results illustrate the potential of adaptive, security-aware configuration selection to balance transaction efficiency and cryptographic protection. Nevertheless, these findings remain simulation-based demonstrations rather than independently validated experimental results. Establishing the proposed algorithm's practical superiority requires reproducible implementation, measured configuration-selection overhead, and statistically

supported comparisons against security-equivalent alternatives.

➤ *Scientific Contributions, Algorithmic Novelty, and Implications for Post-Quantum Digital Banking Security*

The principal scientific contribution of this research is the proposed integration of cryptographic performance benchmarking, mandatory security eligibility, adaptive criterion weighting, Pareto-dominance analysis, and explainable configuration selection into a unified optimization framework for digital banking infrastructures. Unlike conventional performance assessments that independently evaluate cryptographic execution time, signature verification, or communication bandwidth, PQC-Benchmark is designed to evaluate complete authenticated transaction configurations according to multiple competing operational objectives. Its mathematical architecture represents each eligible configuration through a normalized performance vector incorporating transaction latency, inverse throughput, bandwidth consumption, CPU utilization, and, when experimentally available, memory and energy costs. The framework subsequently applies workload-dependent weighting and non-dominated configuration filtering to identify deployment alternatives satisfying prescribed security requirements. Its algorithmic novelty lies in this coordinated decision procedure rather than the development of a new cryptographic primitive or an alteration of standardized ML-KEM, ML-DSA, or SLH-DSA constructions. The illustrative results demonstrate how optimization priorities can influence configuration rankings, particularly under differing latency, throughput, and resource constraints. Explainable performance attribution provides an additional mechanism for identifying the criteria responsible for individual recommendations, thereby supporting technical auditing and defensible deployment decisions. For digital banking security, the proposed approach offers a framework for selecting cryptographic configurations across mobile banking interfaces, interbank transaction gateways, cloud-based payment platforms, and authenticated financial APIs. However, genuine algorithmic improvement must be distinguished from performance differences inherited from constituent cryptographic implementations. The research therefore contributes a testable optimization architecture and reproducible evaluation methodology whose practical effectiveness, operational scalability, and statistical reliability must be established through independent experimentation.

➤ *Technical Recommendations for Cryptographic Migration, Adaptive Configuration Selection, and Deployment in Financial Transaction Infrastructures*

Financial institutions should approach post-quantum cryptographic migration through a structured implementation strategy that integrates cryptographic security assessment, operational performance profiling, interoperability testing, and progressive deployment validation. Initially, banking organizations should establish comprehensive cryptographic inventories identifying RSA-based authentication mechanisms, ECDH key-establishment procedures, ECDSA signatures, certificate dependencies, hardware security modules, and application interfaces requiring quantum-resistant migration. ML-KEM-768 and ML-DSA-65 may

serve as useful initial candidates for experimental evaluation, subject to institutional security requirements and protocol compatibility, while higher-security parameter sets should be assessed where stronger cryptographic protection is required. Hybrid ECDH–ML–KEM configurations should be considered for transitional communication architectures using reviewed protocol constructions and approved key-combination mechanisms. PQC-Benchmark should subsequently be integrated into a controlled cryptographic evaluation environment where transaction workloads, security constraints, network conditions, and resource availability can be measured before configuration policies are authorized. Adaptive selection must operate exclusively within an approved set of security-equivalent configurations and should not permit a reduction in mandated cryptographic protection to improve computational performance. Banking institutions should also establish explicit service-level thresholds for median and 95th-percentile latency, successful transaction throughput, handshake message sizes, memory allocation, and processing utilization. Pilot deployments should evaluate mobile banking authentication, interbank API communication, payment authorization services, and high-concurrency transaction gateways under representative operating conditions. Continuous monitoring should detect configuration instability, processing bottlenecks, implementation regressions, and abnormal resource consumption. Production deployment should additionally incorporate cryptographic agility, secure key lifecycle management, hardware acceleration assessment, rollback procedures, and compatibility testing with existing financial security controls. These measures would support a controlled transition toward quantum-resistant banking systems while preserving transaction integrity, availability, and operational continuity.

➤ *Study Limitations, Reproducibility Considerations, and Future Research Directions in Quantum-Resistant Banking Cryptography*

The present study is subject to methodological limitations that must be addressed before PQC-Benchmark can be considered experimentally validated for operational banking environments. The numerical results presented in Sections 4.1–4.4 are illustrative simulations constructed to demonstrate comparative performance modeling, multi-objective optimization, and adaptive configuration-selection principles. They were not obtained from independently executed standardized cryptographic implementations or production banking transaction records. Consequently, reported latency reductions, throughput improvements, normalized optimization scores, and Pareto-optimal classifications represent scenario-dependent outcomes rather than established empirical performance advantages. The latency-distribution analysis additionally relies on assumed lognormal variability and 3,000 generated observations per configuration, which cannot substitute for repeated hardware measurements. The current framework also lacks independently measured energy expenditure, peak memory consumption, cryptographic implementation overhead, adaptive selection costs, and formal uncertainty estimates derived from observed benchmark samples. Future research should therefore develop a reproducible experimental

implementation using standardized post-quantum cryptographic libraries, controlled processor architectures, documented software configurations, and consistent banking transaction workloads. Experiments should include repeated key generation, encapsulation, decapsulation, signing, verification, and complete authenticated handshake operations, followed by statistical analysis using bootstrap confidence intervals, effect-size estimation, and appropriate multiple-comparison procedures. Further investigations should evaluate hardware security modules, mobile processors, cloud environments, network congestion, packet loss, and high-concurrency banking transaction systems. Independent validation should also examine Pareto-frontier stability, sensitivity to criterion weights, algorithm-selection overhead, cryptographic interoperability, and adaptation under previously unseen workloads. Additional research could incorporate interpretable machine-learning-based workload prediction and secure online configuration adjustment. Such extensions would provide the empirical foundation necessary to determine whether PQC-Benchmark offers reproducible operational advantages while preserving standardized post-quantum security guarantees.

REFERENCES

- [1]. Abiodun, K., Ogbuonyalu, U. O., Dzamefe, S., Vera, E. N., Oyinlola, A., & Igba, E. (2023). Exploring cross-border digital assets flows and central bank digital currency risks to capital markets financial stability. *International Journal of Scientific Research and Modern Technology*, 2(11), 32–45. <https://doi.org/10.38124/ijisrmt.v2i11.447>
- [2]. Ajayi, A. A., Igba, E., Soyele, A. D., & Enyejo, J. O. (2024). Quantum cryptography and blockchain-based social media platforms as a dual approach to securing financial transactions in CBDCs and combating misinformation in U.S. elections. *International Journal of Innovative Science and Research Technology*, 9(10), 1409–1424. <https://doi.org/10.38124/ijisrt/IJISRT24OCT1697>
- [3]. Akanni, F., Idowu, K., Odozor, L., & Waheed, B. (2026). Cyber-financial risk analytics: Integrating business intelligence with threat modeling. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 12(2). <https://doi.org/10.32628/CSEIT26121371>
- [4]. Alao, M. A., Ayodele, T. R., Ogunjuyigbe, A. S. O., & Popoola, O. M. (2020). Multi-criteria decision based waste to energy technology selection using entropy-weighted TOPSIS technique: The case study of Lagos, Nigeria. *Energy*, 201, Article 117675. <https://doi.org/10.1016/j.energy.2020.117675>
- [5]. Atalor, S. I., Ijiga, O. M., & Enyejo, J. O. (2023). Harnessing quantum molecular simulation for accelerated cancer drug screening. *International Journal of Scientific Research and Modern Technology*, 2(1), 1–18. <https://doi.org/10.38124/ijisrmt.v2i1.502>
- [6]. Ayoola, V. B., James, U. U., Idoko, I. P., Ijiga, O. M., & Olola, T. M. (2024). Effectiveness of social

- engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. *Global Journal of Engineering and Technology Advances*, 20(3), 94–117. <https://doi.org/10.30574/gjeta.2024.20.3.0164>
- [7]. Chen, P. (2021). Effects of the entropy weight on TOPSIS. *Expert Systems with Applications*, 168, Article 114186. <https://doi.org/10.1016/j.eswa.2020.114186>
- [8]. Doe Gadekah, S. B. & Enyejo, J. O. (2026). The Effects of Generative AI Advertising Disclosure on Brand Authenticity Perceptions Purchase Intention and Consumer Skepticism Among Generation Z Consumers *International Journal of Scientific Research in Humanities and Social Sciences* Vol, 3 Iss 2, Pg. 137-169 doi : <https://doi.org/10.32628/IJSRHSS253293>
- [9]. Doe Gadekah, S. B. & Enyejo, J. O. (2025). Personalization Versus Privacy in Digital Marketing Examining the Interactive Effects of Data Transparency Perceived Intrusiveness and Consumer Trust on Purchase Decisions *International Journal of Management and Organizational Research* Vol. 4, Iss. 6 Page No: 182-199 DOI: <https://doi.org/10.54660/IJMOR.2025.4.6.182-199>
- [10]. Doe Gadekah, S. B. & Enyejo, J. O. (2025). The Influence of Brand Community Participation and User-Generated Content on Customer-Based Brand Equity Repurchase Intention and Electronic Word-of-Mouth in Direct-to-Consumer Markets *International Journal of Management and Organizational Research* Vol, 4, Iss. 3 Page No: 183-203 DOI: <https://doi.org/10.54660/IJMOR.2025.4.3.183-203>
- [11]. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(1), 238–268. <https://doi.org/10.46586/tches.v2018.i1.238-268>
- [12]. Folorunso, T. N., Idowu, K., & Balogun, A. (2025). AI-driven financial risk forecasting: A multi-model ensemble approach for enterprise decision intelligence. *Journal of Computational Analysis and Applications*, 34(3), 147–173. <https://eudoxuspress.com/index.php/pub/article/view/5080>
- [13]. Frank, U. P. (2026). Artificial intelligence for infection surveillance: Improving early detection of healthcare-associated infections. *USR Journal of Multidisciplinary Research and Studies*. [Publication details and DOI not independently confirmed.]
- [14]. Frank, U. P. (2026). Healthcare quality metrics: From data collection to performance improvement; A narrative review of measurement frameworks and improvement methods in United States health care. *UKR Journal of Medicine and Medical Research*. <https://doi.org/10.5281/zenodo.22105362>
- [15]. Frank, U. P. (2026). Optimizing medical inventory management through predictive analytics: Implications for healthcare quality, cost reduction, and patient safety; A narrative review. *UKR Journal of Education and Literature*, 2(1), 77–92. <https://doi.org/10.5281/zenodo.22105843>
- [16]. Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5, Article 433. <https://doi.org/10.22331/q-2021-04-15-433>
- [17]. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, 74(1), 145–195. <https://doi.org/10.1103/RevModPhys.74.145>
- [18]. Grover, C., Mendelsohn, A., Ling, C., & Vehkalahti, R. (2022). Non-commutative ring learning with errors from cyclic algebras. *Journal of Cryptology*, 35, Article 22. <https://doi.org/10.1007/s00145-022-09430-6>
- [19]. Idika, C. N. (2023). Quantum resistant cryptographic protocols for securing autonomous vehicle to vehicle (V2V) communication networks. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(1), 338–360. <https://doi.org/10.32628/CSEIT2391547>
- [20]. Idoko, I. P., Ijiga, O. M., Enyejo, L. A., Ugbane, S. I., Akoh, O., & Odeyemi, M. O. (2024). Exploring the potential of Elon Musk's proposed quantum AI: A comprehensive analysis and implications. *Global Journal of Engineering and Technology Advances*, 18(3), 48–65. <https://doi.org/10.30574/gjeta.2024.18.3.0037>
- [21]. Idowu, K., Cherotich, V., Aniebonam, E. E., Odozor, L., & During, A. (2025). Integrating AI and machine learning into cyber risk management for critical utility systems. *International Journal of Artificial Intelligence Engineering and Transformation*, 6(2), 32–48. <https://doi.org/10.54660/IJALET.2025.6.2.32-48>
- [22]. Idowu, K., Leslie, A., Twayana, S., Nitzan, Y., & Waheed, B. O. (2026). Real-time detection of DDoS and phishing attacks for enhanced banking security. *International Journal of Scientific Research in Science, Engineering and Technology*, 13(1), 572–593. <https://doi.org/10.32628/IJSRSET2613313>
- [23]. Igba, E., Olarinoye, H. S., Ezech, N. V., Sehemba, D. B., Oluhaiyero, Y. S., & Okika, N. (2025). Synthetic data generation using generative AI to combat identity fraud and enhance global financial cybersecurity frameworks. *International Journal of Scientific Research and Modern Technology*, 4(2), 1–19. <https://doi.org/10.5281/zenodo.14928919>
- [24]. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *Open Access Research Journal of Science and Technology*, 11(1). <https://doi.org/10.53022/oarjst.2024.11.1.0060>
- [25]. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177), 203–209. <https://doi.org/10.1090/S0025-5718-1987-0866109-5>
- [26]. Liu, Z., Pöppelmann, T., Oder, T., Seo, H., Roy, S. S., Güneysu, T., Großschädl, J., Kim, H., & Verbaath, I. (2017). High-performance ideal

- lattice-based cryptography on 8-bit AVR microcontrollers. *ACM Transactions on Embedded Computing Systems*, 16(4), Article 117. <https://doi.org/10.1145/3092951>
- [27]. Marler, R. T., & Arora, J. S. (2004). Survey of multi-objective optimization methods for engineering. *Structural and Multidisciplinary Optimization*, 26, 369–395. <https://doi.org/10.1007/s00158-003-0368-6>
- [28]. Montenegro, J. A., Rios, R., & Bonilla, J. (2026). Comparative analysis of post-quantum handshake performance in QUIC and TLS protocols. *Computer Networks*, 275, Article 111957. <https://doi.org/10.1016/j.comnet.2025.111957>
- [29]. Montenegro, J. A., Rios, R., & Lopez-Cerezo, J. (2026). A performance evaluation framework for post-quantum TLS. *Future Generation Computer Systems*, 175, Article 108062. <https://doi.org/10.1016/j.future.2025.108062>
- [30]. National Institute of Standards and Technology. (2024). Module-lattice-based key-encapsulation mechanism standard (FIPS 203). <https://doi.org/10.6028/NIST.FIPS.203>
- [31]. Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey. *ACM Computing Surveys*, 51(6), Article 129. <https://doi.org/10.1145/3292548>
- [32]. Odozor, L., Berko, S. N., Obu, A. U., & Idowu, K. (2025). Building a resilient U.S. cybersecurity workforce through practical training. *International Journal of Scientific and Management Research*, 8(8), 30–36. <https://doi.org/10.37502/IJSMR.2025.8804>
- [33]. Ononiwu, M., Azonuche, T. I., Okoh, O. F., & Enyejo, J. O. (2023). Machine learning approaches for fraud detection and risk assessment in mobile banking applications and fintech solutions. *International Journal of Scientific Research in Science, Engineering and Technology*, 10(4), 371–390. <https://doi.org/10.32628/IJSRSET232531>
- [34]. Open Quantum Safe Project. (n.d.). liboqs: Open-source C library for quantum-safe cryptographic algorithms. <https://openquantumsafe.org/liboqs/>
- [35]. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., & Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4), 1012–1236. <https://doi.org/10.1364/AOP.361502>
- [36]. Rios, R., & Montenegro, J. A. (2026). Post-quantum cryptography: A multi-layer bottleneck analysis. *International Journal of Information Security*, 25, Article 89. <https://doi.org/10.1007/s10207-026-01242-0>
- [37]. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126. <https://doi.org/10.1145/359340.359342>
- [38]. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126. <https://doi.org/10.1145/359340.359342>
- [39]. Rubio García, C., Rommel, S., Takarabt, S., Vegas Olmos, J. J., Guilley, S., Nguyen, P., & Tafur Monroy, I. (2024). Quantum-resistant transport layer security. *Computer Communications*, 213, 345–358. <https://doi.org/10.1016/j.comcom.2023.11.010>
- [40]. Sahoo, L., Bhurane, A. A., Tolasa, F. T., & Senapati, T. (2026). Integrating K-means clustering with entropy-weighted TOPSIS for large-scale multi-criteria decision making. *Scientific Reports*. <https://doi.org/10.1038/s41598-026-70100-9>
- [41]. Saltelli, A., Annoni, P., Azzini, I., Campolongo, F., Ratto, M., & Tarantola, S. (2010). Variance based sensitivity analysis of model output. Design and estimator for the total sensitivity index. *Computer Physics Communications*, 181(2), 259–270. <https://doi.org/10.1016/j.cpc.2009.09.018>
- [42]. Sedghighadikolaei, K., & Yavuz, A. A. (2026). A survey of threshold signatures: NIST standards, post-quantum cryptography, exotic techniques, and real-world applications. *ACM Computing Surveys*, 58(6), Article 143. <https://doi.org/10.1145/3772274>
- [43]. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509. <https://doi.org/10.1137/S0097539795293172>