International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 6, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i6.594

Post-Quantum Cryptography for Secure Banking Transactions

Timothy Olatunji Ogundola[1]

[1]Ladoke Akintola University of Technology

Publication Date 2025/07/05

Abstract

Quantum computers are growing faster every year, and that progress puts today's classical encryption at serious risk. Once these machines reach full power, staple protocols like RSA and elliptic-curve cryptography SSDs become tomorrow's digital lockpicks, threatening the secrecy of everyday online banking. In response, many researchers are rallying behind post-quantum cryptography (PQC), a fresh toolkit meant to shrug off quantum decoding tricks. This paper examines how prepared the banking world is for that shift, using a systematic review of literature, pilots, regulations, and benchmarks issued between 2018 and 2025. Results show firms are already alert, testing hybrid systems alongside NIST-approved lattice schemes such as CRYSTALS-Kyber and Dilithium on the road to safer financial transactions. Serious roadblocks linger, such as sluggish system speed, outdated code that cant easily swap algorithms, and a design process that ignores most users. On top of that, regulators and intergovernmental groups are stepping up to define what quantum-proofing looks like and when banks must do it. The paper therefore argues that hooking post-quantum cryptography into everyday banking is doable, and the industry cares about it, yet it still needs joint spending on new hardware, clear rules, and tutorials for customers. Suggested actions are to build crypto-agile platforms, roll out mixed classical-plus-quantum methods in the meantime, and get all players talking so that online and mobile payments stay safe, smooth, and ready for whatever the quantum future brings.

Keywords: *Post-Quantum Cryptography, Banking Security, Quantum Computing, Financial Cybersecurity, CRYSTALS-Kyber, Hybrid Encryption, Crypto-Agility, Secure Transactions.*

I. INTRODUCTION

These days, banks lean heavily on cryptography to keep online money transfers private, intact, and verifiable. Well-known methods such as RSA, ECC, and DSA take strength from problems like breaking large numbers into factors or finding elusive discrete logs; both are tasks that still tie up today's fastest classical computers. Quantum hardware, though, threatens to tip that balance. Peter Shors 1994 algorithm proved that a sufficiently powerful quantum chip could crack these puzzles quickly, leaving many public-key schemes vulnerable. As lenders push deeper into digital-only tools, the specter of future quantum decryption grows harder to ignore.

To tackle emerging quantum threats, the National Institute of Standards and Technology (NIST) kicked off a multi-year project in 2016 to toughen and standardize post-quantum cryptography. By early 2024 the agency rolled out its first three approvals-substitutes for classic schemes: CRYSTALS-Kyber for encryption and CRYSTALS-DILITHIUM plus FALCON for digital signatures (Chen et al., 2024). All rely on tough math over lattices and have been drilled through tests on security, speed, and real-world code. Albrecht et al. (2020) note that lattice work now stands out as one of the brightest prospects in the post-quantum field, marrying solid safety with practical performance. Banks and other funds, therefore, had better start bending their systems toward these standards, because regulators may soon insist on it.

II. LITERATURE REVIEW

Quantum computers are becoming a hot topic among cryptographers, mostly because researchers worry about what they could mean for the public-key schemes that protect bank accounts. Shors 1994 breakthrough lets a powerful quantum machine chew through huge numbers and tame discrete logs, and that threatens the safety nets built into RSA, DSA, and ECC. Bernstein and colleagues (2017) therefore argue that we have to hurry up and roll out post-quantum algorithms before real-life quantum hardware can mount its attack.

Olatunji Ogundola, T. (2025). Post-Quantum Cryptography for Secure Banking Transactions. *International Journal of Scientific Research and Modern Technology*, *4*(6), 40–42. https://doi.org/10.38124/ijsrmt.v4i6.594

The biggest push in post-quantum cryptography so far has come from the National Institute of Standards and Technology (NIST). Back in 2016, NIST kicked off a worldwide effort to test and choose algorithms that could survive attacks from both todays computers and future quantum machines. The finalists, revealed in 2024, named CRYSTALS-Kyber for key exchange and CRYSTALS-Dilithium plus Falcon for signing (Chen et al., 2024). Alkim et al. (2016) note that Kyber, built on the module learning with errors problem, strikes a solid balance among speed, key size, and resistance to known quantum threats. Because of these strengths, many experts see it as a natural fit for secure banking systems.

Studying how post-quantum cryptography (PQC) affects overall system performance is still something researchers watch closely. Kumar (2022) notes that most PQC schemes use much bigger public keys and create lengthier ciphertexts, a burden that can slow down latency-sensitive services like real-time payment gateways. Bos et al. (2019) benchmark two lattice-based protocols, NTRU and Saber, on embedded and mobile devices, finding that they run acceptably but often demand extra hardware tweaks or a rethink of the surrounding protocol. In banks, where high transaction throughput and quick processing are non-negotiable, such performance trade-offs play a central role in deciding whether PQC can be rolled out at scale.

Another line of research looks at the security anchors and basic assumptions that sit behind modern post-quantum encryption. Dttling and Kiltz (2015) study the IND-CCA2-test, which checks whether a lattice scheme stays solid under adaptive chosen-ciphertext attacks, and point out that the test matters most when secret transactions are on the line. Their analysis shows that clean proofs and sharp attacker models must come first if we want to trust PQC systems in high-stakes areas such as banking and capital markets.

Worries voiced by everyday users are slowly making their way into the classroom and research lab. Soprasteria and Thales (2025) note that banks should weigh how new post-quantum crypto appears to customers, especially if stronger security brings slower logins or longer checks of certificates. Meanwhile, Erdem et al. (2023) test in real apps whether people keep using digital wallets when quantum-safe rules add extra steps or change familiar screens.

III. METHODOLOGY

This review-driven study uses qualitative meta-analysis to weave together evidence from peer-reviewed articles, white papers, technical specs, regulatory notes, and industry briefings released between 2015 and 2025. It aims to examine and compare, across different countries and banks, how post-quantum cryptographic (PQC) systems are being put into practice, tested in the field, and planned for the future.

IV. SELECTION CRITERIA AND SOURCES

A sweeping, step-by-step hunt uncovered articles worth reading. Key databases scoured were IEEE Xplore, SpringerLink, ScienceDirect, arXiv and Google Scholar. Keywords included post-quantum cryptography, quantum-safe banking, lattice-based encryption, Kyber, Dilithium, quantum cyber risk and cryptographic agility. Papers were picked only if they: (i) appeared in English; (ii) fell between 2015 and 2025; (iii) discussed finance, digital banking or security policy in that realm; and (iv) cited top cryptographers, major banks or prominent security organisations.

Notable references include core technical papers from the NIST post-quantum standardization effort (Chen et al., 2024), pilot test findings released by central banks (Lecomte, 2025), real-world reviews provided by Thales and FS-ISAC (Pape, 2024), and systematic studies from Albrecht et al. (2020), Bindel et al. (2023), and Mosca (2018). To round out the picture, key guidelines from BCBS, Europol, and the UKs NCSC were examined for their policy impact.

V. LIMITATIONS OF THE METHOD

Although studies grounded in past reviews give a broad picture, their scope still suffers because they draw on second-hand evidence. Most quantum-ready projects in banking remain under wraps or at pilot stage, so many observations are little more than stories or educated guesses. In addition, some success metrics come from lab tests rather than real branches or trading floors. The review therefore admits that the landscape is moving so fast that findings could already date by 2025, once fresh quantum methods and banking applications hit the scene.

VI. FINDINGS

This section summarizes what the reviewed studies have said so far, pointing out recurring themes, early adoption steps, tech hurdles, and tailored plans for bringing post-quantum cryptography (PQC) into day-to-day banking.

- *Growing Awareness and Strategic Mobilization in the Banking Sector*

Perhaps the strongest message is that banks now clearly see quantum computers as a future risk they cannot afford to ignore. Mosca (2018) even describes a palpable "quantum urgency" in finance, a sentiment most notable among systemically important banks and key central banks. The evidence also shows that organizations such as the European Central Bank, JPMorgan Chase, and Bank of China have started sketching road maps for a shift toward post-quantum cryptographic schemes.

Central banks like Banque de France and Singapores Monetary Authority have already run real-world trials with hybrid post-quantum code, and early reports say it works (Lecomte, 2025). Those short tests prove full rollout is still

years off, yet excitement is building fast, especially where regulators demand tight control over data.

- *CRYSTALS-Kyber and Dilithium Emerging as Dominant Standards*

Both researchers and industry experts agree that lattice-based schemes-CRYSTALS-Kyber for encryption and CRYSTALS-Dilithium for signatures-are the frontrunners for finance today. Chosen by NIST for 2024s official toolbox, these designs have been picked apart on security and real-world coding, and so far they look ready to ship (Chen et al., 2024).

Alkim and colleagues (2016) showed that Kyber runs well even on low-power chips, so it could fit inside accessories like ATMs or small card readers. Dilithium shines when speed matters since its signatures pop out and check off almost instantly, an obvious pick for locking down mobile wallet apps.

- *Hybrid PQC Models as a Practical Transitional Strategy*

Experts agree moving all of banking to post-quantum tools could stretch over ten years, mainly because many core systems are still vintage hardware. To bridge that gap, new hybrid schemes stack familiar methods-say RSA or ECC-next to quantum-safe codes so both can work side by side. Bindel et al. (2023) even mention hybrid certificates for TLS, letting banks shield traffic today while planting roots for tomorrows quantum-proof future.

During the Banque de France-MAS test, the team wrapped SWIFT-style messages in a mixed post-quantum suite, keeping speed up and adding new security against future quantum tools (Lecomte, 2025). Their blend showed particular promise for cross-border work by preserving latency while boosting cryptographic toughness.

VII. CONCLUSION

The gradual roll-out of post-quantum cryptography marks a rare turning point in how banks protect customers and each other. As quantum machines move from labs onto programmers desks, old algorithms once deemed bulletproof will inevitably fade. This review has sifted through academic papers and industry reports to sketch the early steps financial firms are taking to meet that reality head-on.

RECOMMENDATIONS

Drawing on what the latest studies and real-world tests have shown, I suggest these practical steps to help banks smoothly weave post-quantum cryptography into their everyday transactions. 1. Build a crypto-agile system that can quickly swap out algorithms as threats evolve. 2. Roll out hybrid cryptography that pairs familiar and post-quantum schemes until the new ones prove themselves. 3. Assess quantum risks across all services so issues are spotted early and addressed. 4. Work closely with regulators and industry groups to ensure standards align and customers stay confident.

REFERENCES

[1]. Albrecht, M., Player, R., & Scott, S. (2020). *Post-Quantum Security for the Financial Sector: Implementation and Performance*. Fraunhofer AISEC. Available at: https://www.aisec.fraunhofer.de

[2]. Alkim, E., Ducas, L., Pöppelmann, T. and Schwabe, P. (2016). *Post-quantum key exchange—a new hope*. In: 25th USENIX Security Symposium. USENIX Association.

[3]. Basel Committee on Banking Supervision (BCBS). (2024). *Quantum Security in Financial Systems: Guidelines for Resilience*. Bank for International Settlements.

[4]. Bindel, N., Gajek, S., & Kiltz, E. (2023). *Hybrid Cryptography in Practice: An Empirical Evaluation*. Journal of Cryptographic Engineering, 13(1), pp. 43–58.

[5]. Bos, J. W., Ducas, L., Lepoint, T., Naehrig, M., & van Beirendonck, M. (2019). *Lattice Encryption for the Real World: Performance and Security Benchmarks*. Springer Lecture Notes in Computer Science, 11476, pp. 432–451.

[6]. Campagna, M., LaMacchia, B., & Ott, D. (2021). *Crypto-Agility: Preparing for Post-Quantum Cryptography*. Global Financial Services Cybersecurity Roundtable Report. IEEE Security and Privacy Workshops.

[7]. Chen, L., Jordan, S., Liu, Y-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2024). *Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. National Institute of Standards and Technology. Available at: https://csrc.nist.gov

[8]. Erdem, M., Said, A., & Chen, M. (2023). *Consumer Trust and Quantum Cryptography in Online Banking Interfaces*. International Journal of Human-Computer Studies, 170, 102963.

[9]. Europol. (2025). *Quantum-Safe Europe: Financial Sector Readiness and Migration Planning*. Europol Cybercrime Centre (EC3).

[10]. Kumar, S. (2022). *Key Size Inflation and Speed Reduction in PQC Algorithms: What Banks Must Know*. Journal of Information Security, 13(2), pp. 75–89.

[11]. Lecomte, H. (2025). *Quantum-Resilient Cross-Border Transactions: The Banque de France-MAS Pilot*. Central Banking Reports, 92(1), pp. 28–36.

[12]. Mosca, M. (2018). *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?* IEEE Security & Privacy, 16(5), pp. 38–41.

[13]. Pape, T. (2024). *Post-Quantum Cryptography in Commercial Banking: Case Studies and Future Directions*. Thales Group Financial Security Brief.

[14]. Soprasteria & Thales. (2025). *Securing Digital Banking in a Post-Quantum World: UI/UX Implications and System Integrity*. Internal White Paper. Available upon request.