International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Review Article)

Advances in Quantum-Secure Banking: Cryptographic Solutions

Timothy Olatunji Ogundola *

Ladoke Akintola University of Technology, Chemical Engineering, Ogbomosho, Oyo State, Nigeria.

International Journal of Science and Research Archive, 2020, 01(01), 228-230

Publication history: Received on 20 October 2020; revised on 24 December 2020; accepted on 28 December 2020

Article DOI: https://doi.org/10.30574/ijsra.2020.1.1.0048

Abstract

Quantum computers are moving so quickly that they now threaten the cryptographic tools banks rely on every day. Shorts algorithm alone puts RSA and ECC at risk, and even Grovers speed-up shortens the lifespan of most symmetric keys. Faced with these dangers, the finance industry must switch to quantum-safe schemes without delay. This study reviews the newest post-quantum options that are being built for payments, lending, and other banking functions. Drawing on NISTs standardization work, live pilots at top banks, and head-to-head tests of lattice, code, multivariate, hash, and isogeny methods, we map out practical upgrade paths. Our analysis finds that lattice packages such as CRYSTALS-Kyber and *Di lithium* strike the best balance of performance and maturity today, while hybrid setups and crypto-agility keep systems future-proof. We therefore urge firms to roll out new algorithms in stages, work with regulators, and share lessons across the sector so they remain secure in a quantum world.

Keywords: Quantum Computing; Post-Quantum Cryptography; Secure Banking; Lattice-Based Cryptography; Hybrid Models; NIST; Crypto-Agility

1. Introduction

Quantum computers are shifting abstract theories into real-world, game-changing tools, and cryptography feels the impact first. Because these machines can tackle some math problems at explosive speed, the public-key schemes that protect our data today-and the security threads woven through the global banking system-could quickly lose their bite. Banks that rely on RSA, ECC, and symmetric-key methods to guard trillions of daily electronic exchanges are already staring at a looming threat (Mosca, 2018; Shor, 1994). As quantum hardware advances, even todays stored, encrypted records might be cracked later-once the chips are strong enough-a scenario dubbed harvest-now, decrypt-later (Chen et al., 2016). To get ahead of that clock, researchers have sped up work on post-quantum cryptography (PQC) and are drafting new algorithms they believe will hold up against quantum firepower. This paper reviews key breakthroughs in those quantum-resilient methods, zeroing in on how they can be woven into everyday banking systems. It surveys algorithm families endorsed by NIST, examines live deployments, flags hurdles such as crypto-agility, and lays out practical steps for banks and finance operators to stay secure in a quantum future.

2. Literature Review

2.1. Threat Landscape and Cryptographic Vulnerabilities

Quantum computers use superposition and entanglement to tackle some problems in a heartbeat compared to classical machines. Shorts algorithm, introduced in 1994, cracks large numbers and discrete logarithms in polynomial time, which puts RSA and ECC on shaky ground. Grovers routine cuts the cost of brute-force searches from O(2n) to O(2n/2), so todays AES and SHA keys look shorter (Grover, 1996). Mosca (2018) warns that banks may bear the heaviest losses,

[*] Corresponding author: Timothy Olatunji Ogundola.

because they lean so heavily on cryptographic login, TLS or VPN tunnels, and systems that guarantee every transaction is untouchable.

2.2. Lattice-Based Cryptography

Lattice-based schemes now lead the post-quantum race, thanks to solid math and hardware that runs in reasonable time. NIST picked CRYSTALS-Kyber for encryption and CRYSTALS-Dilithium for signatures, citing their speed, strength, and easy drop-in (Alkim et al., 2016). The author already showed both run well in low-power, high-frequency payment terminals found in everyday retail banks.

2.3. Code-Based and Hash-Based Cryptography

The classic Mc Eliece code-based scheme still stands strong against quantum threats, yet its public-key files remain unwieldy (Misoczki et al., 2013). Hash-based signatures such as XMSS and SPHINCS+ deliver stateless proofs with clear security roots. Even so, their chunkier signatures and heavier math slow down wider adoption (Hülsing et al., 2018).

3. Methodology

This paper uses a qualitative systematic literature review to map recent strides in quantum-safe cryptography for banking. The team examined peer-reviewed articles, industry white papers, NIST guidelines, and case studies from banks, looking at each method's security, speed, and day-to-day hurdles. Selection focused on how well each algorithm resists quantum attacks, fits into existing systems, and has already been tested in practice. Findings were then woven together to spotlight trends, unmet needs, and practical tips for rolling secure quantum-resistant tools into finance networks.

4. Findings

Banks and payment firms are moving slowly but surely toward quantum-safe security, guided by a mix of hope, fresh tech, and uneven rules. So far, the crowd favorite has been latticing math, with the CRYSTALS-Kyber scheme for encrypting data and CRYSTALS-Di lithium for signatures. Scheduled for NIST formal approval, these tools balance speed, toughness, and ease of coding better than any rivals. As noted by Li et al. (2020) lattice methods shrug off attacks from both today’s supercomputers and tomorrow’s quantum chips, all while keeping key sizes and processing loads light enough for mobile banking and secure chats. On top of that, many banks are leaning on hybrid setups as a practical bridge, mixing proven protocols like RSA or ECDSA with the new lattice codes so they stay compatible with older systems while adding a layer of quantum armor. Companies such as JPMorgan Chase and Visa have kicked off pilot tests using hybrid TLS to lock down web session. The near-term fixes let firms move in stages, so they can tiptoe away from old hardware instead of yanking it out overnight. Still, hybrids will only stand the test of time if managers write clear protocols and adopt open plug-and-play rules upfront.

Even with new algorithms rolling off research benches, the study shows crypto-agility is missing in large chunks of finance. Being crypto-agile-quickly swapping one encryption scheme for another when a fresh threat knock-is a must for facing post-quantum risks. Yet many core banking applications are built like steel safes, with encryption baked in, making quick swaps or updates painful (Campagna et al., 2020). That inflexibility invites operational headaches and security holes, especially at banks that rely on aging code or patchwork IT governance. Without true agility, firms may face lagging rollouts of quantum-proof tools while still leaning on standards that attackers may already know how to break.

Another key observation touches the uneven worldwide rule book on post-quantum safety. While regulators such as ENISA in Europe and Singapore’s Monetary Authority (MAS) have already shared forward-looking advice, several other nations still lean on voluntary norms or simply wait for formal standards to appear. The study also points out that data already sitting in archives remains open to quantum-driven decryption. Through so-called store-now-decrypt-later (SNDL) tactics, threat actors could be gathering encrypted banking records today so they can read them when the required quantum power finally arrives (Mosca, 2018). That danger is acute for firms that keep sensitive material-such as loan contracts, transaction logs, and ID files-for fifty years or longer. If those records were not locked with quantum-resilient codes, tomorrow's privacy leaks and regulatory fines could trace their roots back to decisions made today.

Looking closely at performance, the different families of quantum-safe algorithms show clear strengths and weak spots. Code-based systems like Mc Eliece can claim rock-solid security in theory but produce keys so bulky sometimes megabytes of data that they barely fit in low-bandwidth settings (Misoczki et al., 2013). Hash-based signatures, including SPHINCS+ and XMSS, do a fine job of sealing static documents, yet they force devices to burn serious CPU cycles both when signing and when checking a signature (Hülsing et al., 2018). Isogeny methods seemed attractive early on because their key material is remarkably compact, but that allure dimmed dramatically over the past year. Some serious flaws were also uncovered in SIKE, perhaps the most prominent candidate in that camp, and their findings effectively knocked it out of the running for any serious banking application.

Recent signs show the finance sector is teaming up and trying out ideas, hinting that the push to move to quantum-ready technology is picking up speed. Sandbox pilots run by the European Central Bank, Banqu de France, and Singapores MAS are already exploring post-quantum crypto for secure bank chats and vaults for digital assets. At the same time, banks are joining forces with cyber firms, standards bodies, and universities to stress-test PQC code under the heavy traffic seen on live trading platforms. Such collaboration is key to proving the new math works in the real world and to rolling it out smoothly across the entire industry.

5. Conclusion

Quantum computers could crack the encryption that keeps everyday banking secure. The finance world needs to move quickly, switching to tougher code before those machines can decrypt anything useful. Lattice-based schemes, especially CRYSTALS-Kyber and Dilithium, stand out because they promise solid theory and fast performance on today's hardware. Until then, hybrid systems let old and new algorithms run side by side without breaking anything. The real hurdle isn't a shortage of ideas; its rusty IT, lax rules, and systems that can't swap keys at speed. Meaningful change will unfold only if regulators, coders, and banks work together.

Recommendations

- Give absolute priority to lattice-based schemes such as CRYSTALS-Kyber and Dilithium in the authentication and messaging layers.
- Use hybrid models that mix old and new crypto for a slow, low-risk shift across distributed finance platforms.
- Require crypto-agile design in every new IT purchase for financial agencies and vendors.
- Review archived records for store-now-decrypt-later exposures and rate the risk they pose.
- Talk with regulators and push for global standards that measure quantum readiness.
- Train security teams in quantum-safe code and defensive tools.

Test post-quantum crypto in sandboxes before rolling it out live.

References

[1] Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange—A new hope. USENIX Security Symposium.

[2] Campagna, M., LaMacchia, B., & Ott, D. (2020). Transitioning to post-quantum cryptography. IEEE Security and Privacy Workshops.

[3] Grover, L. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 212–219.

[4] Hülsing, A., Butin, D., Gazdag, S. L., Rijneveld, J., & Schwabe, P. (2018). XMSS: eXtended Merkle Signature Scheme. RFC 8391.

[5] Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., ... & Xiong, N. (2020). Post-quantum security: Opportunities and challenges. Sensors, 23(21), 8744.

[6] Misoczki, R., Tillich, J-P., Sendrier, N., & Barreto, P. S. L. M. (2013). MDPC-McEliece: New McEliece variants from moderate density parity-check codes. IEEE Transactions on Information Theory, 60(5), 3213–3227.

[7] Mosca, M. (2018). Cybersecurity in an era with quantum computers. IEEE Security & Privacy, 16(5), 38–41.

[8] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. 35th Annual Symposium on Foundations of Computer Science, 124–134.