International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 1, Issue 11, 2022
DOI: https://doi.org/10.38124/ijsrmt.v1i11.586

Quantum-Resistant Cryptographic Techniques for Financial Institutions

Timothy Ogundola[1]

[1]Ladoke Akintola University of Technology

Publication date 2022/11/25

Abstract

As quantum machines grow stronger, banks and insurers are already rethinking how they guard customer data, uphold privacy, and protect digital IDs. Well-worn tools like RSA and ECC now look shaky under a future quantum assault, pushing firms into a scramble for post-quantum defenses. This paper reviews the latest post-quantum landscape, weighing lattice, code, and multivariate, hash, and isogeny families side by side. Backed by fresh research, NIST standards, and real-world trials from major banks and cyber vendors, it flags both promise and hurdles in rolling out each option. Results show that lattice schemes, notably CRYSTALS-Kyber and Dilithium, stand out, while hybrid mixes and crypto-agility plans are still a must. The paper closes with a clear step-by-step map so that financial outfits can start pilots and gradually field quantum-ready cryptography.

Keywords: *Quantum-Resistant Cryptography, Lattice-Based Algorithms, Hybrid Encryption, Financial Cybersecurity, NIST Standards, Crypto-Agility.*

I. INTRODUCTION

Quantum computing, once the stuff of science fiction, is now knocking loudly at the door of cybersecurity. Banks and payment networks that lean on encryption to guard huge stores of personal and financial data feel this shift most acutely. Classic algorithms such as RSA and ECC, which have long formed the backbone of secure online talk, crumble when faced with Shors algorithm (1994), since a quantum chip can factor giant numbers and solve discrete-log problems in polynomial time. Because of this threat, the finance world now treats building and rolling out quantum-resistant cryptography as an urgent, must-do mission.

Banks, brokerages, and even new fintech apps look after trillions of dollars every day and must obey strict rules about keeping customer data private and communications safe. If a hacker with a large quantum computer appeared tomorrow, he could imagine breaking years of stored transaction records or messing with login checks in the middle of a trading session (Mosca, 2018). Because of that risk, the industry urgently needs encryption methods that stand firm against both todays powerful laptops and tomorrows quantum machines. This paper reviews this expanding field, tests how well the leading ideas run in typical banking environments, and sketches a realistic road map for introducing them. We pay special attention to cryptographic agility, speed under load, compliance with regulators, and smooth fitting into the digital systems financial firms already rely on.

II. LITERATURE REVIEW

- *Lattice-Based Cryptography*

Experts now regard lattice-based cryptography as the lead option for shielding everyday systems against future quantum computers. Its robust proofs and smooth speed set the stage for this shift. Finalists in NISTs post-quantum race, CRYSTALS-Kyber and Dilithium, already manage daily encryption and signing tasks with solid ease (Chen et al., 2024). Alkim et al. (2016) pointed out that Kyber slots well into tight hardware like smart cards and mobile wallets, while Dilithium offers the fast verify needed in real-time log-ins.

Code-based schemes, most notably Classic McEliece, carry decades of theory and remain a strong contender (Misoczki et al., 2013). Yet their bulky keys pose headaches for small banking devices. Multivariate systems such as Rainbows short keys and quick signing look tempting, but recent attacks (Beullens, 2022) tarnish their standing in finance, a domain that cannot afford surprises.

Ogundola, T. (2022). Quantum-Resistant Cryptographic Techniques for Financial Institutions. *International Journal of Scientific Research and Modern Technology*, *1*(11), 18–20. https://doi.org/10.38124/ijsrmt.v1i11.586

➢ *Hash-Based Cryptography*

Hash-based signatures like XMSS and SPHINCS+ work well for creating digital certificates and rest on clear security ideas (Hülsing et al., 2018). Their simple design fits firmware and software updates in money-handling gear, yet the heavy maths and need to track state can choke large-scale use.

➢ *Isogeny-Based Cryptography*

Isogeny schemes such as SIDH and SIKE first drew notice for tiny keys, a real plus when network pipes are narrow. Recent work, however, shows serious weaknesses in SIKE (Castryck and Decru, 2022), so it sits lower on the list for hard targets like the banking system.

III. METHODOLOGY

This project runs a systematic literature review to spot and judge the quantum-safe crypto methods now in use. Articles from peer-reviewed journals, NIST briefs, implementation notes from banks, and vendor white papers published between 2018 and 2023 were gathered through Google Scholar and IEEE Xplore.

➢ *Studies had to Meet all of these Filters:*

- Apply directly to financial systems
- Hold up against known quantum threats
- Be doable in practice (key bulk, speed, memory)
- Get backing from regulators or standards bodies

For each algorithm family, performance data, quantum strength, fit with schemes like TLS and SSH, and active pilot projects were reviewed side by side.

IV. FINDINGS

➢ *Widespread Industry Acceptance of Lattice-Based Cryptography*

Recent surveys show that many banks and fintech firms now lean strongly toward lattice-based schemes when they think about future-proofing against quantum threats. Two frontrunners, CRYSTALS-Kyber for encryption and CRYSTALS-Dilithium for signatures, have earned a reputa-tion for being both secure and practical. Their formal recognition by the National Institute of Standards and Technology (NIST, 2024) has pushed regulators and vendors alike to roll them out across payment networks, clearing houses, and other vital segments of the financial system.

As noted by Bos et al. (2019) and later confirmed by Chen et al. (2024), these primitives shrug off both quantum and classical attack vectors while keeping keys manageably small and speed-friendly for online payments or smart cards. Moreover, Alkim et al. (2016) show that their memory demands are modest, a critical feature when code runs on phones, ATMs, or low-power POS terminals.

➢ *Emergence of Hybrid Cryptographic Architectures*

Another important finding is the rise of hybrid cryptographic models as a stepping-stone toward full quantum readiness. These setups stack well-known schemes like RSA or ECC on top of new quantum-safe ones, guarding assets against todays attacks and tomorrows quantum threats. The twin-encryption approach lets organizations keep older hardware running while slowly swapping in stronger, post-quantum safeguards.

Bindel, Kiltz, and Gajek (2023) note that this design lowers the odds of a system-wide meltdown because an attacker would need to break both layers at once. Major banks such as JPMorgan Chase, Citigroup, and HSBC are already testing hybrid TLS and VPN services with vendors like Thales and Entrust.

➢ *Crypto-Agility is Limited in Existing Banking Infrastructure*

Even though researchers have rolled out secure quantum-safe algorithms, many legacy finance platforms still lack crypto-agility-the basic ability to swap or upgrade their cryptographic tools on short notice. Campagna and colleagues (2021) point to hard-coded libraries, rigid compliance rules, and a tight link between business logic and encryption as the main culprits.

Without that agility, moving to post-quantum cryptography (PQC) can turn into an expensive, drawn-out project, even for firms that want to act quickly. In areas where digital infrastructure is still patchy, such as some emerging markets, the challenge amplifies, leaving institutions more vulnerable to future quantum breaches.

➢ *Disparity Between Technological Readiness and Regulatory Enforcement*

Technology to support post-quantum cryptography is moving ahead, yet rules and enforcement still sit in patches. Authorities like the Basel Committee on Banking Supervision (2024) and Europes ENISA (2023) have told banks to start risk checks and draft upgrade road maps, but no single deadline or rule book exists worldwide.

In practice, the European Central Bank (ECB) has formed teams focused on quantum-secure finance, while U.S. watchdogs lean on voluntary advice and sector groups. Such mismatched oversight may leave global banks with varying defenses, raising the chance of turmoil during cross-border deals.

➢ *Quantum Threat to Archived and Long-Term Stored Financial Data*

One risk that flies under the radar yet still worries experts is how poorly archived financial data is guarded. Researchers such as Mosca (2018) and Pape (2024) warn that hackers with quantum gear might already be running what they call a "store now, decrypt later" (SNDL) play. Simply put, they scoop up todays encrypted files so they can crack the codes later, once their machines are powerful enough.

That practice spells trouble for banks and insurers that hang on to sensitive records-mortgages, retirement plans, loan papers, transaction logs-for decades. Even if the killer quantum computer is still a decade out, data

locked with RSA or ECC now could be priceless long after its creators think it is obsolete

➢ *Differentiated Performance of Cryptographic Families*

Tests of new quantum-resistant algorithms show clear performance trade-offs:

- *Lattice-Based Algorithms:*

Offer a sweet spot of security, speed, and memory use; great for mobile apps, online banking, and instant payments.

- *Code-Based Cryptography:*

Unmatched in brute-force resistance but plagued by giant public keys (Misoczki et al., 2013), so it chokes on low-bandwidth, low-memory gear.

- *Hash-Based Schemes:*

Provide rock-solid signatures (see software updates) and are compact enough for almost any device.

So, agencies should pick their encryption tools with their own working environment in mind; a single fix will never cover everyone.

➢ *Growing Industry Collaboration and Pilots*

The report also points to a promising rise in joint pilot projects and sandbox tests. Key examples are:

- A partnership between Visa and IBM that explores hybrid quantum-secure methods for blockchain settlements.
- Industry groups such as the Quantum Economic Development Consortium (QED-C), which push forward open testing and shared standards.
- Taken together, these efforts show that firms see the quantum risk clearly and are working together to speed up a safe transition.

V. CONCLUSION

Quantum computers threaten to upend the classical security tools that keep the finance world safe. Banks and trading houses therefore need to move quickly, testing and rolling out quantum-resilient methods, with lattice-based schemes topping the list because they run fast and scale well. Code-based, hash-based and multivariate options still matter, too, especially for guarding embedded devices and signing records that need to last decades.

In the near term, hybrid cryptography offers the smoothest path, letting firm's layer new keys over old ones without ripping out proven systems. Staying secure years from now will, however, require crypto-agile gateways, updated rules, and staff who can design and deploy quantum-safe code.

RECOMMENDATIONS

Choose lattice-based building blocks as the standard for new encryption and signature applications. Adopt hybrid protocols so legacy and post-quantum algorithms work side by side without downtime. Design all new systems for crypto-agility, permitting swift upgrades with only lightweight code changes. Set up interdepartmental teams to steer quantum readiness and coordinate testing, training, and compliance. Team up with regulators and key vendors so everyone agrees on common standards, and join any broad pilot projects that emerge. Offer clear training for both staff and developers on quantum-safe coding techniques and how to put the new algorithms to work. Re-encrypt any long-term data that could be at risk from future quantum decryption, using today's strongest post-quantum methods.

REFERENCES

[1]. Alkim, E., Ducas, L., Pöppelmann, T., and Schwabe, P. (2016). Post-quantum key exchange—A new hope. 25th USENIX Security Symposium.

[2]. Beullens, W. (2022). Improved cryptanalysis of UOV and Rainbow. Advances in Cryptology – EUROCRYPT 2022.

[3]. Bindel, N., Kiltz, E., & Gajek, S. (2023). Hybrid cryptographic certificates for post-quantum transitions. Journal of Cryptographic Engineering, 13(2), 65–82.

[4]. Bos, J. W., Ducas, L., Lepoint, T., Naehrig, M., & van Beirendonck, M. (2019). Performance of lattice cryptography in embedded banking systems. Springer LNCS, 11476, 432–451.

[5]. Campagna, M., LaMacchia, B., & Ott, D. (2021). Preparing Financial Systems for Post-Quantum Cybersecurity. IEEE Security and Privacy Workshops.

[6]. Castryck, W. & Decru, T. (2022). An efficient key recovery attack on SIDH. ePrint Archive: Report 2022/975.

[7]. Chen, L., Jordan, S., Liu, Y-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2024). Final Report on NIST's Post-Quantum Cryptography Standardization. NIST CSRC.

[8]. Ding, J., Gower, J., & Schmidt, D. (2008). Multivariate Public Key Cryptosystems. Springer.

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

[10]. 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.

[11]. Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers. IEEE Security & Privacy, 16(5), 38–41.

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