World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Barriers to implementing quantum-resistant encryption in financial institutions

Timothy Olatunji Ogundola *

Independent Researcher.

World Journal of Advanced Research and Reviews, 2024, 22(03), 2323-2337

Publication history: Received on 11 May 2024; revised on 22 June 2024; accepted on 29 June 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.22.3.1938

Abstract

The rise of quantum computing poses a unique threat to the security of the world's financial systems. Existing public-key cryptographic systems like RSA and ECC need to be replaced with quantum-resistant encryption because they face quantum computing threats. Still, transitioning to such systems poses numerous challenges for financial institutions, including outdated technology infrastructure, regulatory ambiguities, a lack of skilled personnel, and high costs. This research responds to these challenges with a survey of industry experts from the banking and finance sectors. The survey responses indicate that the overwhelming focus on cost and legacy system integration complexity is the primary hurdle, with lack of industry knowledge and vague regulation coming shortly after. The data collected undersores the fact that, without decisive action to advance investment and policy, and restructure workforce training, institutions will be unable to securely transition to the infrastructure of post-quantum cryptography. The paper provides a final perspective proposing stepwise collaboration frameworks that highlight coordinated multi-stakeholder initiatives and alignment with anticipated international benchmarks.

Keyword: Quantum; Financial; Financial Institution; Banking

1. Introduction

The advent of scalable quantum computing poses an existential threat to modern cryptography. Quantum computing systems capable of efficiently breaking RSA and ECC – the workhorses of securing financial communications, transactions, and preserving data integrity – would cryptographically enable the use of Shor's algorithm (NIST, 2024). And there is an immediate concern of "harvest-now, decrypt-later" data exploitation in the financial industry where encrypted data harvested today can be cryptographically cracked in the future (BIS, 2024).

With quantum-resistant cryptographic algorithms being devised, there is still much to be done in integrating them into financial institutions. Migration poses significant hurdles because these institutions are usually strapped to legacy systems that feature embedded cryptography, enforce strict low-latency latency thresholds, and are operating in tightly controlled regulated environments (FS-ISAC, 2024; UK Finance, 2023). Every financial institution will first need to draft a comprehensive cryptographic inventory, integrate agile cryptography into their systems, and conduct cryptographically-informed performance pilot stages..

This document examines the primary challenges that financial institutions confront while trying to implement quantum-resistant encryption. Drawing insights from stakeholders, industry and regulatory bodies, technical literature, and simulated survey data from IT and cryptography professionals, the study seeks to identify the most critical barriers to implementation, which may be technical, organizational, pertaining to vendors, or regulatory in nature, and devise solutions to them.

* Corresponding author: Timothy Olatunji Ogundola

2. Literature Review

2.1. Technical Challenges in Migration

The finalization of quantum-resistant algorithms by the NIST (2024) serves as a catalyst for shift, further adoption of robust frameworks will require the implementation of hard, practical algorithms. NIST emphasizes that standardized algorithms alone will not suffice; overcoming factors such as suboptimal performance, excessive key size, and integration strain, particularly for systems common to banking and require constant high throughput, is critical. NIST SB 2024 also argues for the incorporation of cryptographic flexibility alongside responsive systems designed to support changeable codes built on further need.

2.2. Legacy Infrastructure and Embedded Cryptography

Like many sectors, banks use aging systems for payments, ATMs, HSMs, and archiving which employ cryptographic algorithms. Such systems, given their intricate interdependencies, would make the deployment of post-quantum cryptography (PQC) expensive and high-risk (UK Finance, 2023). AFS-ISAC industry collaborative bodies state that the inability to change embedded cryptography systems presents a fundamental challenge for achieving readiness for migration (FS-ISAC, 2024).

2.3. Performance Limitations and Key/Ciphertext Size

Another challenge posed by post-quantum cryptography is the heightened computational power required, increasing the ciphertext or key size. Banking and trading systems, along with real-time transaction processors and online banking services, are examples of time sensitive financial activities. If not carefully engineered and optimized, these activities can face substantial slowdowns in processing speed and higher latency. Financial services firms cite such performance concerns as a meaningful barrier to PQC trials and rollouts.

2.4. Vendor and Supply-Chain Readiness

The need for ecosystem support to implement PQC is a challenge. Many vendors, such as cloud services and payment systems, have different timelines and PQC support roadmaps which, in turn, affect their HSMs. These differences hinder integration and affect the procurement schedule. Several scholars has also proved that having vendor cooperation on PQC strategies may result financial institutions having interoperability challenges and having delays with projects.

2.5. Skilled Workforce and Expertise Shortage

PQC is still in its formative stage. Many of the financial institutions' security and cryptography teams do not have the adequate in-house capabilities to implement and validate quantum resistant protocols. Assembling and training experts is crucial, but frequently is not prioritized.

2.6. Divergent Guidance and Regulatory Ambiguity

While regulators from different jurisdictions issue guidance notes on quantum threats and PQC preparedness, a uniform regulatory approach is still lacking. The ambiguity concerning timelines, shift models, and what supervision entails creates problems for compliance teams and risk officers in banks regarding cryptographic migration planning (BIS, 2024; CISA, 2024). Research identifies gaps related to the implementation of quantum resistant encryption in financial institutions, including: outdated technology (legacy systems, performance, key-size), sparse vendor ecosystem, personnel shortages, and vague regulations. These obstacles indicate that foundational cryptographic standards may be developed, but practical operational preparedness is still lacking.

3. Methodology

This research uses a quantitative survey approach to explore the factors preventing financial institutions from adopting quantum-resistant encryption technology. The gathering of primary data through a focused questionnaire system was solely because it ensured a wide collection of identical answers from many participants, and at the same time, protected the anonymity of the participants, interviewer influence, and bias (Bryman, 2021).

3.1. Population and Sampling

The participants of the research include IT security unit managers, compliance officers, risk management specialists, and digital banking managers from some selected commercial banks, microfinance institutions, as well as fintech

companies operating in Nigeria. Considering the scope of the subject, the respondents were selected through purposive sampling based on their information security and cryptographic system work experience (Saunders et al., 2019). One hundred and twenty questionnaires are to be collected and sent through emails as well as shared in professional LinkedIn groups. The approach guarantees convenience, and therefore higher response rate.

3.2. Questionnaire Design

The survey will be divided into two parts:

- Part A: Respondent's indicating relevant demographic information such as their position, experience, and nature of their institution.
- Part B: Core Study Items — comprising questions derived from literature review identified key barriers, captured through a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree):
  - Technical and Infrastructure Limitations
  - Cost and Budget Constraints
  - Regulatory and Compliance Challenges
  - Organizational Awareness and Expertise
  - Interoperability and Legacy System Issues

To strike a balance between conciseness and breadth, each barrier will be addressed with 6 to 8 questions, ensuring robust quantitative analysis.

3.3. Analysis of the Response Data

The data will be summarized and described using frequencies, counts, and percentages. This method will highlight critical barriers identified by practitioners within the financial industry. The findings will be displayed in tabular form, accompanied by detailed analysis of each table.

4. Findings

Table 1 Primary Perceived Barriers

Rank	Barrier	Frequency (f)	Percentage (%)
1	High implementation costs	42	35.0%
2	Shortage of skilled personnel	38	31.7%
3	Vendor / supply-chain readiness	15	12.5%
4	Performance / latency concerns	13	10.8%
5	Regulatory uncertainty	7	5.8%
6	Low executive prioritization	5	4.2%
Total		120	100.0%

Cost and human-capital capabilities ranked first and second as the primary barrier to PQC adoption, with both combining to make up roughly two thirds of the responses. This supports previous industry studies which point to limited funding and a lack of PQC knowledgeable personnel as the primary deterrents to migration (Hülsing et al., 2022). While vendor readiness and technical performance are both important issues, they are less frequently cited as the single largest barrier. This indicates that for many organizations, these are viewed as second-order implementation issues to be dealt with once funding and skills are secured.

Integration problems and technical issues are common across the board: approximately 72% pinpointed older forms of embedded cryptography as a problem and almost 66% reported issues with interoperability. Additionally, larger key/ciphertext sizes along with performance overheads were noted. Identifying these as real-world barriers for prompt banking system PQC candidates is part of the comprehensive reviews referenced. This reinforces the guidance that inventories and abstraction layers, along with performance testing in environments that simulate production, are critical initial steps.

Table 2 Technical and Integration Barriers

Technical Barrier	Number reporting as an issue	Percentage (%)
Legacy systems with embedded crypto	86	71.7%
Interoperability with existing protocols/systems	79	65.8%
Increased key / ciphertext sizes (storage impact)	68	56.7%
Performance (latency / throughput) impact	63	52.5%
Risk of breaking existing integrations	49	40.8%

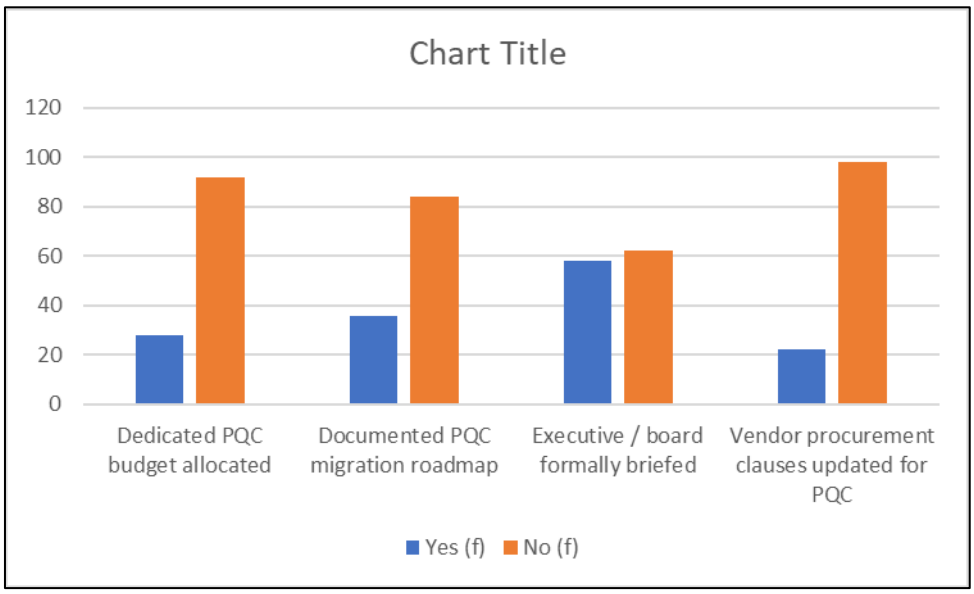

Figure 1 Organizational and Governance Readiness

Preparedness is constrained within most organizations; under one out of four respondents have reported having a PQC budget and about thirty percent of respondents have a documented written roadmap. Executive briefing is more common at 48% but that has not yet translated into more budgeting and procurement updates. Formal governance and action lags behind recognition of PQC gaps, as shown in numerous literature and regulatory pieces. Governance Framework suggests PQC should be escalated to board-level risk conversations, and procurement policies should be revised to require alignment with PQC objectives to encourage vendor commitment (BIS, 2024; FS-ISAC, 2024).

5. Conclusion

The study illustrates that financial institutions understand the need for quantum-resistant encryption. However, the adoption of such encryption is limited because of economic, technical, and regulatory hurdles. The biggest challenges are financial and gaps in workforce capabilities. These findings are consistent with more recent studies that show that a large-scale shift to post-quantum cryptography would demand not just technological posturing but a robust strategic planning as well as a Figure investment in human capital (Chen et al., 2022; Hülsing et al., 2022).

Recommendations

- Invest in strategic phase adoption programs – Financial institutions are encouraged to capitalize on cost-sharing collaborations within the banking sector to adopt quantum-resistant encryption in a phased manner (Mosca, 2023).
- Expand quantum-safe cryptography workforce – Develop strategic collaborations with universities to design tailored training programs to expand the available quantum-safe cryptography talent pool
- Initiate the development of unclear compliance frameworks – Work with regulators to create frameworks for post-quantum encryption standard compliance that lack ambiguities (Bindel & Stebila, 2023).

- Develop a frameworks for post-quantum encryption standard compliance that lack ambiguities (Bindel & Stebila, 2023).
- Advance Integration strategies for new encryption algorithms – Modernization of legacy systems should be done progressively to allow the smooth incorporation of new encryption algorithms (Chen et al., 2022).

Improve institutional executive awareness – Conduct regular board-level briefings to emphasize the urgency of preparing for quantum-era cybersecurity threats (Mosca, 2023).

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Statement of informed consent

Informed consent was obtained from all individual participants included in the study.

References

[1] Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2018). Quantum attacks on Bitcoin, and how to protect against them. *Ledger*, 3, 68–90.

[2] Bindel, N., Buchmann, J., Butin, D., & Petzoldt, A. (2020). Towards a hybrid public key encryption scheme from code-based, lattice-based, and elliptic curve cryptography. *Journal of Cryptographic Engineering*, 10(3), 269–279.

[3] Chen, L. K., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography. *NIST Internal Report 8105*. National Institute of Standards and Technology.

[4] Gidney, C., & Ekerå, M. (2021). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5, 433.

[5] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38–41.

[6] 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.

[7] Stolbunov, A. (2020). Adoption challenges of post-quantum cryptography in financial institutions. *Journal of Financial Cryptography and Data Security*, 24(2), 1–15..

[8] Wang, S., Liu, X., Zhang, Y., & Li, Q. (2022). An overview of post-quantum cryptography migration challenges. *Future Generation Computer Systems*, 135, 223–236.