CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.casjournal.org/index.php/CAJMTCS
Volume: 07 Issue: 01 | January 2026 ISSN: 2660-5309

Article

A Post-Quantum Cryptography Framework for Securing Banking Communications in Iraq

Haroon Rashid Hammood Al Dallal[1]

1. Technical Institute of Najaf, Al-Furat Al-Awsat Technical University (Atu), Najaf, Iraq
* Correspondence: haroon.radhi.inj@atu.edu.iq

Abstract: Iraq's banking sector has grown very fast in recent years, with over 18.5 million bank cards and electronic payments above 2 trillion IQD each month by 2023. While this growth improves financial access but it also increases exposure to cyber threats, which are rising worldwide. Iraq's system of seven state owned and more than sixty private banks shows uneven cyber readiness, with private banks facing greater challenges. In addition, quantum computing threatens existing encryption methods like RSA and ECC. This paper analyzes Iraq's banking cyber risks and proposes a post-quantum cryptography (PQC) model to strengthen security, support both public and private banks, and prepare for future quantum-safe standards.

Keywords: private banks

Citation: Al Dallal, H. R. H A Post-Quantum Cryptography Framework for Securing Banking Communications in Iraq. Central Asian Journal of Mathematical Theory and Computer Sciences 2026, 7(1), 227-233.

Received: 21th Oct 2025
Revised: 15th Nov 2025
Accepted: 25th Dec 2025
Published: 04th Jan 2026

1. Introduction

Iraq's banking industry is undergoing rapid modernization, led by digital services. By 2023, the Central Bank of Iraq (CBI) reported about 70 licensed banks, including seven state-owned and the rest private [1]. Retail banking has experienced the greatest changes, where electronic payments and card services are growing rapidly. It is reported that by the end of 2023, more than 18.5 million cards had been issued by the banks in Iraq among which almost two million in that same year alone [2]. The number of activity on these platforms is also increasing; in August 2024, e-payments amounts hit IQD 2 trillion (equivalent to USD 1.5 billion) per month, indicating the pace at which the shift towards digitized financial practices is taking place [3].

Despite the fact that such developments are undeniable progress towards financial inclusion and financial modernization, they also create new risks. Increased reliance on online systems has expanded the scope of the attack in the cybercrime and cases of fraud, compliance lapses and cross-border transactions have been already reported in the Iraqi banking industry [4]. Another issue is the asymmetry between the state-owned and the privately-owned institutions: although the former has greater state support, a large number of the banks that are privately-owned have limited technical and financial resources, and thus cannot afford to enforce comprehensive cybersecurity systems [5].

Consequently, the small banks are particularly vulnerable to external risks. In the recent years, cyberattacks on financial institutions have increased across the world. The IMF mentions that there has been a consistent increase in cyber attacks targeting banks and payment systems, and in the case of emerging economies such as Iraq, this is of significant concern since national cybersecurity systems have only evolved [6], [7]. To respond to this, cybersecurity is a priority of the 20242026 strategy designed by the Central Bank of Iraq as

part of its efforts to enhance security and better collaborate with national entities, including the Iraq Cyber Events Response Team (IQ-CERT) [8], [9].

Financial security is an issue with long-term implications of quantum computing [10]. Modern encryption algorithms like RSA and ECC are based on problems that cannot be solved with a classical computer, but can be solved in the quantum algorithm like the Shor algorithm in polynomially time [11]. As quantum hardware advances, there is a possibility that the current standards of cryptography will become ineffective in the future; this could happen as soon as the next ten years.

With the expansion of the banking sector into the digital dimension of Iraq, quantum computing is a potential threat to the country as well. A solution is found with post-quantum cryptography (PQC) though the methods include lattice-based, code- based, and hash-based approaches that are now being considered by NIST [12], [13]. In the case of Iraq, this is slightly different. The digital services are rapidly growing, but the degree of cybersecurity preparedness is not even among institutions. Such a framework of PQC that is responsive to such local realities would not only enhance defenses against modern attacks but also equip banks with the resilience that they will require when quantum technologies are a reality [14].

This research paper has three major objectives. First, it summarizes and examines confirmed information regarding the exposure of banking sector in Iraq to cyber risks, and this information is further classified into state run institutions and those owned by individual investors. Second, it discusses the weaknesses associated with the continuous digitalization, specifically the development of card issuance and electronic payment systems. Third, it describes a post-quantum cryptography architecture that would help to ensure safety of communication channels in the financial sector of Iraq.

Literature Review

A. Cybersecurity Challenges in Iraqi Banking

The fast process of digitizing the financial system in Iraq has created new opportunities and brought some severe threats. Over 18.5 million bank cards were reported to be active and over 18.5 million monthly electronic payments had by mid-2023 already surpassed IQD 2 trillion (≈ USD 1.5 billion). This dependence on online platforms has brought about banks being more reliant on sound infrastructure, but it has also expanded the scope of attacks in committing fraud and cybercrime. According to recent evaluations, repetitive threats are observed to include money laundering, subpar compliance, and cyber supported fraud that, in certain instances, triggered the imposition of international restrictions on U.S. dollar dealings involving Iraqi institutions [15]. The distribution of these pressures is uneven: big state-owned banks have more powerful technical systems, and small privately owned banks have difficulties keeping up.

B. Central Bank of Iraq (CBI) and IQ-CERT Role

The Central Bank of Iraq (CBI) has taken over a key role in setting the cybersecurity policy in the financial sector. In its 20242026 plan the CBI lays great emphasis on the security posture of its systems and commercial bank systems [6]. Iraq Cyber Events Response Team (IQ-CERT) was established to facilitate the coordination of cyber incident responses with the national and global partners [9], [10]. Nevertheless, data regarding frequency and impact of attacks is scarce, resulting in the overall threat situation to Iraqi banks being only half-known.

C. International Perspectives on Financial-Sector Cyber Incidents

Cyberattacks on banks and other financial companies are still one of the main targets, which is observed in almost all locations. According to the International Monetary Fund (IMF) cases of attack on central banks and regulators have been increasing over the past 10 years or so [16]. Misunderstandings within financial institutions have, in most instances, provided entry to greater systemic risks. Glancing at Iraq specifically, the World bank believes that the banking system in the country is still lagging behind those in the region, and there are loopholes in its oversight systems and also defenses against technological

shocks are weak. These external evaluations aid in providing the context of the present state of affairs of the Iraqi country, particularly given the fact that there is little domestic reporting on cyber attacks.

D. Quantum Computing Threats to RSA and ECC

Even existing variants of cyber risks are already hard to control, but the creation of quantum computing is usually referred to as a game-changer. One is that quantum algorithms, best known by Shor, can solve number factorization, discrete logarithms, and many others with significantly more efficiency than classical computers can [17]. Should these types of machines be scaleable, popular encryption systems, such as RSA or elliptic curve cryptography (ECC), would be vulnerable. This is not something theoretical. Financial infrastructure in Iraq is still centralizing and the adoption of technologies that might soon crumble under quantum pressure will undermine trust and stability in the sector.

E. Post-Quantum Cryptography (PQC) Families

Efforts to address the quantum threat have led to the design of several post-quantum cryptographic (PQC) algorithm. Among them, lattice-based techniques are widely regarded as the strongest candidates, combining firm security assumptions with relatively efficient implementations. Code-based schemes, which originate from error-correcting codes, are backed by decades of study and are still considered reliable, though their large key sizes remain a drawback [18]. Hash-based approaches perform well for digital signatures but provide less flexibility for encryption tasks. In response to these trade-offs, the U.S. National Institute of Standards and Technology (NIST) has moved several PQC proposals into the final stages of evaluation, with lattice-based solutions, particularly CRYSTALS-Kyber, emerging as leading contenders.

F. Research Gap

Iraq has started to recognise the value of cybersecurity, mainly through the efforts of the Central Bank of Iraq (CBI) and the national response team, IQ-CERT. Even so, little detailed information is shared with the public about cyber incidents in either state-owned or private banks. This lack of openness makes it hard to measure specific weaknesses in the sector or to compare Iraq's situation with international practices. To address this gap, the present study brings together confirmed banking statistics with global benchmarks and then suggests a post-quantum cryptography (PQC) framework designed for Iraq's developing financial system.

2. Materials and Methods

G. Data Collection

This study uses primary and secondary data to examine cybersecurity in Iraq's banking sector. Data from the Central Bank of Iraq (CBI) on licensed banks, bank cards, and electronic payments highlight the rapid growth of digital services and provide a basis for assessing cyber risk.

IMF data show a global rise in both the number and severity of cyberattacks on financial institutions. Reports from sources such as Reuters and the World Bank highlight Iraq-specific issues, including fraud, banking restrictions, and compliance challenges tied to weak governance and cybersecurity gaps. Where available, reports from IQ-CERT and its partner organisations are also considered, since these provide direct evidence of local incidents.

H. Data Analysis

The study looks at the data in three main ways. First, a simple table is used to compare state- owned and private banks in Iraq, showing structural differences that may explain why their cyber risks are not the same. Second, trends in digital banking are measured by tracking how many cards were issued and how monthly electronic payment volumes grew between 2019 and 2024, based on reports from the CBI. Third, records of cyber incidents,

fraud, and sanction- related breaches are reviewed to trace how Iraqi banks have faced actual threats.

Framework Development

This research introduces a post-quantum cryptography (PQC) framework dedicated to the banking sector of Iraq. The methods are focused on lattices, chiefly CRYSTALS-Kyber and CRYSTALS-Dilithium, which have recently been chosen by NIST for standardization due to their unparalleled security and efficiency.

The structure is built around the two most important aspects of bank communications, secure key exchange, and digital signatures, which are trustworthy. The utilization of PQC will ensure the confidentiality and the quantum-threats will not be able to break the trust. A layered approach is recommended wherein PQC is implemented on top of SSL/TLS and payment systems while keeping the older security tools during the transition phase. This enables the proposal to be in line with the current financial situation in Iraq while at the same time being aligned with the global progress in cryptography.

3. Results and Discussion

A. Iraqi Banking Sector Structure

Iraq's banks operate in two groups. A small cluster of state-owned institutions dominates the market, while dozens of private banks make up the rest. In 2023, records from the World Bank and the Central Bank of Iraq counted seven public banks and more than sixty private ones.

Table I. Licensed Banks in Iraq (2023)

Bank Type	Number of Banks	Share of Total Assets (%)
State-Owned	7	80%
Private	63	20%

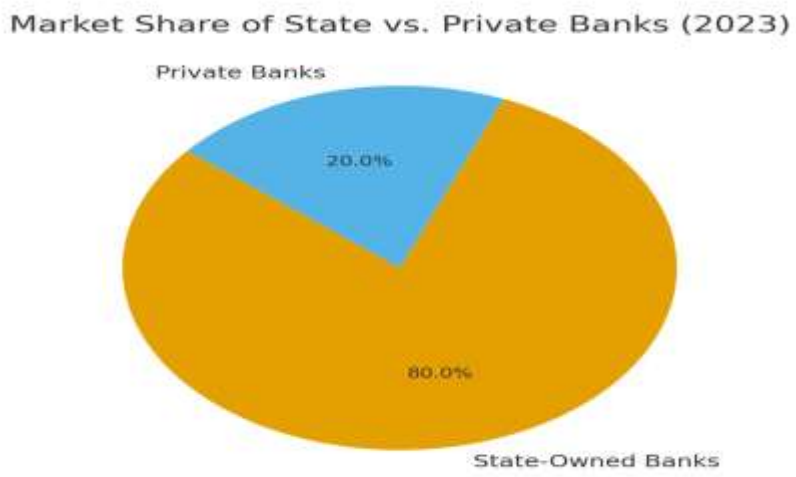

Figure 1. Market share of state vs. private banks (2023).

B. Growth of Bank Cards in Circulation

Digital services are spreading quickly, and card use is one of the clearest signs. Between 2019 and 2023, the number of active bank cards more than doubled. By the close of 2023, Iraq had around 18.5 million cards in circulation.

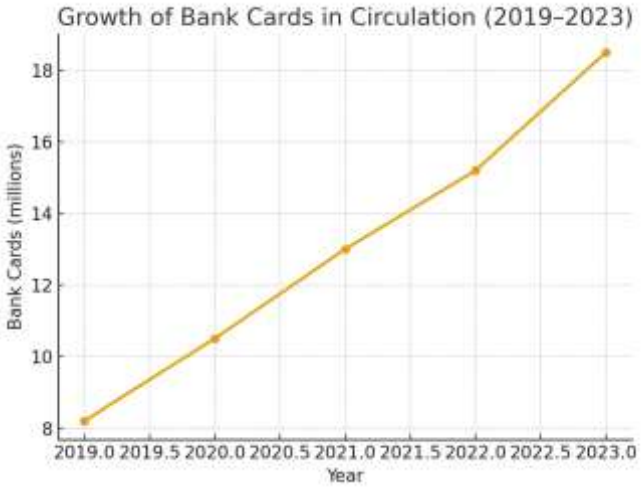

Figure 2. Growth of bank cards in circulation in Iraq

C. Monthly E-Payment Volumes

A similar surge can be seen in electronic payments. In 2022, the value of monthly transactions usually stayed below IQD 1 trillion. By 2024, however, the figure had climbed to over IQD 2 trillion, equal to about USD 1.5 billion.

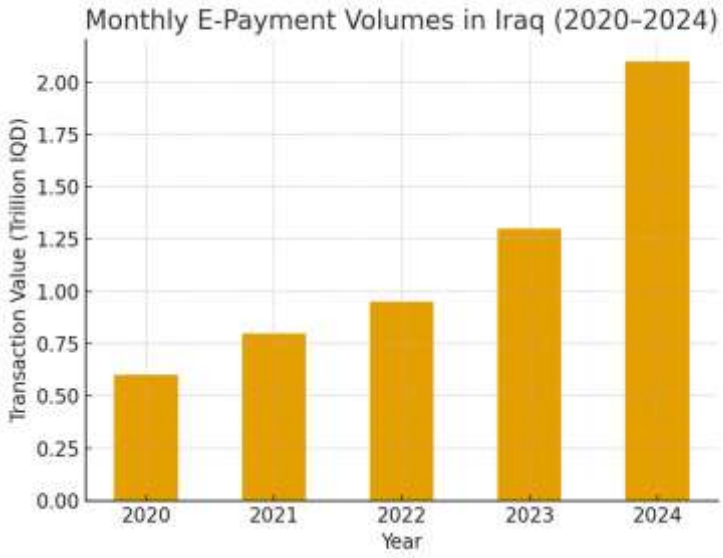

Figure 3. Monthly e-payment volumes in Iraq (2020–2024).

D. Verified Iraq-linked Cyber and Compliance Incidents

Reliable data on cyberattacks by bank category are limited. Still, several confirmed reports describe instances of non-compliance and fraud. These cases suggest that Iraqi banks are still struggling to build strong controls.

E. Reference Benchmark: IMF Global Data

The IMF reports a 250% rise in financial-sector cyber incidents between 2017 and 2022. Iraq's fast move into digital banking, combined with weaker oversight, makes its financial system more vulnerable than many peers.

Discussion

The findings indicate that the fast financial digitalisation in Iraq has increased the financial access as well as systemic vulnerability to cyber threats. In 2019, the number of bank cards in circulation was about 8.2 million, but in 2023, it reached 18.5 million, and monthly payments through e- payment have exceeded IQD 2 trillion in 2024. Although these numbers are positive signs of financial inclusion, they also represent an extremely

large digital attack surface, which is in line with IMF data that the financial industry has become a juicy target in cybercrime worldwide.

A. Differential Risk Between State and Private Banks

The banking system in Iraq is characterized by different risk evaluations of government and private banks. The state banks possess nearly 80% of the total assets and these banks still rely on old-fashioned methods but more centralized systems under strict CBI. Private banks are very fast in digitalization, but often their financial resources for security and compliance are not very good. The U.S. Treasury's 2023 prohibition on 14 private banks pointed out these weaknesses. In this way, the private banks are in danger of higher exposure because of weaker control and new, unproven systems.

B. Feasibility of PQC Framework Adoption

Definitely, the transition to post-quantum cryptography (PQC) will not be an easy process and problems will be the ones to stick with us. The current best practices for encryption, namely RSA and ECC, might indeed be rendered obsolete by a quantum computer that is already beyond the realm of fiction. To state the issue in even a harsher manner, NIST has unambiguously verified the acceptance of the lattice-based algorithms, CRYSTALS-Kyber and Dilithium, as the quantum-secure standards by bestowing upon them such conformance.

Iraq is no exception; the switch-over to PQC in the financial industry will not lead to a trouble-free situation. The financial aspect is the chief challenge that needs to be handled directly.Smaller private banks, which already operate with limited budgets, may struggle to replace or upgrade their cryptographic systems. Another issue is uneven technical capacity. Large state-owned banks are more likely to have staff and infrastructure to handle PQC, but many private banks do not. A final concern is policy alignment. Unless the Central Bank of Iraq (CBI) issues clear instructions that require PQC adoption, efforts will remain piecemeal and inconsistent.

C. Comparison with Conventional Cryptography

RSA and ECC have been used to protect bank transactions for a long time. Their security comes from hard math problems, like factoring large numbers or solving discrete logarithms. But these methods could fail once quantum computers become strong enough to run Shor’s algorithm. PQC works in a different way. It relies on problems with lattices, codes, or hashes that quantum computers cannot solve yet. Using PQC now might seem early, but it could save Iraq a lot of trouble in the future.

Iraq’s banks have made big steps in digital services. At the same time, this growth also brings risks. Smaller private banks are still weaker and more likely to face compliance or security problems. A careful plan for PQC, led by the Central Bank, following international guidance, and adjusted to Iraq’s mix of state and private banks, could make the system safer. Interestingly, starting early now might prevent serious problems later.

4. Conclusion

The reports indicate that the challenges to Iraq's banking security mainly due to the advances in quantum computing were evaluated. In 2024, Iraq was already using more than 18.5 million bank cards and the total volume of e-payments during the month was above IQD 2 trillion. These developments, albeit beneficial, have also resulted in the opening up of more and more digital entry points for the attackers just like it is the case all over the world.

The research revealed that there are very distinct differences between the state and private banks in Iraq. The major part of the assets is held by the state banks that are under stricter supervision; whereas, the private banks tend to quickly adopt digital platforms but very often fall short of being compliant and having strong security systems in place. The difference in these aspects underlines the necessity of having more advanced and adaptable security systems in place.

One important and inevitable long-term solution is post-quantum cryptography (PQC). NIST has already approved some algorithms such as CRYSTALS-Kyber and Dilithium that will eventually be used to deter quantum attacks and secure financial communications. For Iraq, the process of adoption should be slow with the Central Bank issuing regulations and IQ-CERT aiding in the implementation.

The way to move forward will involve running pilot projects to see how PQC works in a secure connection between state banks and the CBI. After the trials demonstrate positive results, the system can then be implemented across the whole sector with private banks getting extra assistance. Moreover, Iraq should be forming partnerships with international cybersecurity organizations and including PQC as part of its national digital strategy to build trust and ensure that it meets global quantum security standards.

REFERENCES

[1] Central Bank of Iraq, *Banking Sector Statistics (2023 Sector Composition)*. Baghdad: CBI, 2024.

[2] Central Bank of Iraq, *CBI Annual Statistical Bulletin 2023*. Baghdad: CBI, 2023.

[3] Central Bank of Iraq, *CBI Strategy 2024–2026*. Baghdad: CBI, 2024.

[4] Jummar Media, "Shaimaa and Muhammad's concerns about digital payment," Apr. 3, 2025.

[5] FintechNews Middle East, "Iraq introduces new regulations to modernize payments and banking," Oct. 1, 2024.

[6] Reuters, "U.S. Treasury official says Iraq must act to avoid further action on banks," Sep. 14, 2023.

[7] World Bank, *Iraqi Banking Sector Market Structure (December 2019)*. Washington, DC: World Bank, 2019.

[8] International Monetary Fund, *Global Financial Stability Report: Cyber Risk in the Financial Sector (Online Annex to Chapter 3)*. Washington, DC: IMF, Apr. 2024.

[9] Cybil Portal, "Iraq Cyber Events Response Team (IQ-CERT)," 2025.

[10] Resecurity, "Resecurity partners with Iraq Cyber Events Response Team (IQ-CERT)," Business Wire, Jul. 23, 2025.

[11] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 1994, pp. 124–134.

[12] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[13] C. Peikert, "A decade of lattice cryptography," *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016.

[14] R. Overbeck and N. Sendrier, "Code-based cryptography," in *Post-Quantum Cryptography*,

[15] J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin: Springer, 2009, pp. 95–145.

[16] A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen, "XMSS: eXtended Merkle signature scheme," RFC 8391, IETF, May 2018.

[17] National Institute of Standards and Technology, *Post-Quantum Cryptography Standardization: Finalist Algorithms Overview*. Gaithersburg, MD: NIST, 2023.

[18] J. Bos et al., "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, London, UK, 2018, pp. 353–367.