QUANTUM COMPUTING AND POST-QUANTUM CRYPTOGRAPHY: EXPLORING IMPLEMENTATION FEASIBILITY INDUSTRIES IN AFRICA.

By

Eze, Festus Chukwuma(PhD)[1] and Kingsley Ozumba
Mbadiwe University, Ideato Imo State, Nigeria
fchuxeze0327@gmail.com

Abstract

Quantum computing represents a seismic shift in computational power, posing significant threats to classical cryptographic systems like RSA and ECC, which rely on mathematical problems that quantum algorithms can solve exponentially faster. This paper explores the emergence of **post-quantum cryptography (PQC)** as a necessary response, focusing on the feasibility of implementation across industries such as finance, healthcare, manufacturing, and government. Key considerations include algorithm performance, infrastructure compatibility, regulatory frameworks, and industry-specific vulnerabilities. The study concludes that while PQC is technically viable and strategically essential, its implementation depends heavily on tailored integration strategies and collaborative global standards.

Keywords: Quantum Computing, Post-Quantum Cryptography and Feasibility Industries

Introduction

With the rise of quantum computing, the robustness of traditional public-key cryptography is under threat. Algorithms such as Shor's and Grover's demonstrate quantum capabilities that undermine current encryption frameworks. This paper investigates PQC as a transitional safeguard to maintain data confidentiality and integrity in a quantum-enabled future. The evolution of quantum computing marks a monumental leap in computational capacity. Unlike classical computers that process bits as 0 or 1, quantum computers utilize quantum bits (qubits), which can exist in superpositions, allowing simultaneous computation across multiple states. This paradigm shift presents extraordinary opportunities for scientific innovation—particularly in fields such as drug discovery, materials science, and optimization problems (Preskill, 2018). However, one of its most pressing consequences is the vulnerability it imposes on classical cryptographic systems. Public-key algorithms such as RSA and Elliptic Curve Cryptography (ECC), which underpin online banking, secure communication, and data protection systems, are susceptible to quantum

algorithms like Shor's, which can factor large numbers exponentially faster than classical methods (Shor, 1997).

In anticipation of this threat, **Post-Quantum Cryptography (PQC)** has emerged as a field dedicated to developing cryptographic algorithms resistant to quantum attacks. These algorithms are built on hard mathematical problems believed to remain secure even in the face of quantum computing capabilities. The urgency to transition towards PQC is underscored by efforts from global bodies like the National Institute of Standards and Technology (NIST), which launched a standardization process for quantum-resistant algorithms in 2017 and announced finalists in 2022 (Chen et al., 2016; NIST, 2023).

Nigeria's Digital Landscape and the Need for PQC

Nigeria, Africa's largest economy and most populous nation, is rapidly digitizing across various sectors, including banking, telecommunications, health care, education, defense, and government services. With growing reliance on mobile money, cloud computing, and big data, sensitive information travels across increasingly complex digital infrastructures. Yet, cyberattacks in Nigeria are on the rise. According to the Nigerian Communications Commission (NCC), the country loses over $500 million annually to cybercrime (NCC, 2022). As digital dependency deepens, so does the need for robust encryption mechanisms. A quantum-enabled future threatens the security of these digital frameworks, making PQC implementation not just a theoretical aspiration but a strategic necessity.

Sector-Specific Considerations

Finance: The Nigerian financial sector, especially digital banking, fintech startups, and e-payment platforms, handles massive volumes of encrypted transactions daily. The Central Bank of Nigeria (CBN) has been encouraging innovation through frameworks like the eNaira digital currency. However, the quantum threat compromises current digital security, as RSA and ECC used in banking systems may be broken within minutes by quantum machines (Khan et al., 2023). PQC solutions like ***Kyber*** (lattice-based encryption) and ***Dilithium*** (digital signatures) offer scalable alternatives.

Healthcare: With telemedicine and electronic health records becoming mainstream, Nigerian hospitals and medical research institutions must safeguard patient data and medical IP. Post-quantum solutions like hash-based signatures and code-based cryptography offer long-term confidentiality crucial for such data.

Government Services: E-Governance initiatives like e-taxation, national identity systems (NIN), and electoral databases rely on digital infrastructure. Compromise of such data poses risks to

sovereignty and privacy. Integration of PQC into these systems will demand both technical investment and policy alignment with national cybersecurity standards.

Telecommunications: Telecom operators provide the backbone of Nigeria's internet connectivity and voice data exchange. Incorporating PQC in 5G and emerging technologies ensures quantum-resilient authentication and encryption.

Challenges to PQC Adoption in Nigeria

Despite the clear benefits, several challenges hinder the implementation of PQC across Nigerian industries:

Resource Constraints: PQC algorithms are computationally intensive, requiring hardware upgrades and high processing power, which may be unaffordable for many Nigerian SMEs.

Knowledge Gaps: There is a lack of trained personnel and awareness among IT professionals and policymakers about quantum threats and PQC.

Infrastructure Legacy Systems: Existing infrastructures are built around classical cryptography. Migrating or retrofitting PQC requires interoperability and phased transition plans.

Regulatory Inertia: Nigeria's cybersecurity policies, though evolving, are yet to incorporate quantum resistance frameworks, risking delayed response to global trends.

Vendor Readiness: Most local and foreign tech vendors servicing Nigeria haven't fully adapted PQC solutions into their products, creating dependence on external innovation.

In conclusion, quantum computing threatens the very foundation of current cryptographic systems, and Nigeria, with its fast-evolving digital environment, must prepare for these disruptions. The feasibility of implementing PQC depends not just on the availability of quantum-resistant algorithms but also on the readiness of industries, government bodies, and stakeholders to integrate these solutions within sector-specific contexts. Strategic investment in education, infrastructure, and regulatory policy will be pivotal to Nigeria's journey toward a quantum-secure future.

The advent of quantum computing represents a paradigm shift in computational power, posing a formidable challenge to the cryptographic foundations that secure the modern digital world. Unlike classical computers that store information as bits, which can be either 0 or 1, quantum computers leverage the principles of quantum mechanics to process information. Key to this capability are **qubits**, which can exist in a superposition of both 0 and 1 simultaneously, and exhibit **entanglement**, a phenomenon where the state of one qubit instantaneously influences the state of

another, regardless of distance (Nielsen & Chuang, 2010). These quantum phenomena allow quantum computers to perform certain calculations exponentially faster than even the most powerful classical supercomputers.

The most profound threat emanating from this computational power is posed by **Shor's algorithm** (Shor, 1994). Developed in 1994, this quantum algorithm can efficiently solve the integer factorization problem and the discrete logarithm problem. The security of widely adopted public-key cryptographic standards, such as RSA, relies on the presumed difficulty of factoring large numbers into their prime components. Similarly, Elliptic Curve Cryptography (ECC), another cornerstone of digital security, derives its strength from the intractability of the elliptic curve discrete logarithm problem. Shor's algorithm, if implemented on a sufficiently large and stable quantum computer, could break these cryptographic schemes in polynomial time, thereby compromising secure communications, digital signatures, and encrypted data globally.

While Shor's algorithm directly targets asymmetric encryption, **Grover's algorithm** (Grover, 1996) presents a significant, albeit less catastrophic, threat to symmetric-key cryptography. Grover's algorithm offers a quadratic speedup for unstructured search problems. For instance, breaking a 128-bit symmetric key (like AES-128) using a classical brute-force attack would, on average, require 2^{127} operations. A quantum computer running Grover's algorithm could achieve this in approximately $2^{63.5}$ operations. While this does not "break" symmetric encryption in the same way Shor's algorithm breaks public-key schemes, it effectively halves the security level. Consequently, to maintain comparable security in a post-quantum world, symmetric key lengths would need to be doubled (e.g., migrating from AES-128 to AES-256).

The existence of these quantum algorithms, even before the widespread availability of fault-tolerant quantum computers, creates an immediate security concern known as the "**store now, decrypt later**" problem. Sensitive encrypted data, communications, and intellectual property protected by classical cryptography that is transmitted or stored today could be harvested by adversaries. Once sufficiently powerful quantum computers become available in the future (the exact timeline remains uncertain, but estimates range from 10 to 30 years), this stored data could be decrypted, posing significant risks to national security, corporate secrets, and personal privacy. This impending cryptographic obsolescence necessitates a proactive and urgent transition to post-quantum cryptographic solutions.

Overview of Post-Quantum Cryptography

The urgent need to replace cryptographic systems vulnerable to quantum attacks has spurred the development of Post-Quantum Cryptography (PQC). PQC refers to cryptographic algorithms designed to be secure against attacks by both classical and quantum computers. Its primary goals are **quantum resistance**, ensuring security against known and future quantum algorithms;

classical resistance, maintaining security against current and future classical attacks; and, where feasible, aiming for **backward compatibility** to ease migration from existing systems. Unlike current public-key cryptography which relies on number theory problems efficiently solvable by quantum computers, PQC is built upon mathematical problems believed to be intractable for even the most powerful quantum machines.

Among the various approaches explored, two families have emerged as frontrunners: lattice-based cryptography and code-based cryptography.

Lattice-Based Cryptography

Lattice-based cryptography derives its security from the presumed hardness of certain problems concerning lattices, which are regular arrangements of points in n-dimensional space. The core hard problems include the **Shortest Vector Problem (SVP)**, which seeks the shortest non-zero vector in a given lattice, and the **Closest Vector Problem (CVP)**, which aims to find a lattice vector closest to a given target vector (Ajtai, 1996; Goldreich et al., 1997). These problems are known to be NP-hard in their general forms, and critically, no efficient quantum algorithms are known to solve them.

Security Benefits: Lattice-based schemes offer strong **quantum resistance** due to the believed intractability of SVP and CVP for quantum computers. Many schemes also benefit from **strong mathematical proofs**, often referred to as "worst-case to average-case reductions," implying that breaking an average instance of the cryptosystem is as hard as solving the hardest instance of the underlying lattice problem. This provides robust theoretical guarantees. Furthermore, lattice-based cryptography is highly **versatile**, supporting a wide array of cryptographic primitives, including Key Encapsulation Mechanisms (KEMs), digital signatures, and even advanced functionalities like fully homomorphic encryption (Gentry, 2009).

Technical Limitations: Despite their strengths, lattice-based cryptosystems generally have **larger key sizes and signature sizes** compared to pre-quantum cryptosystems like RSA or ECC. This can lead to increased bandwidth consumption, storage requirements, and potentially slower operations, particularly for resource-constrained environments. Additionally, their **implementation complexity** can be higher, demanding specialized knowledge to ensure both correctness and resistance against side-channel attacks. The National Institute of Standards and Technology (NIST) has selected **CRYSTALS-Kyber** as the standard for Key Encapsulation Mechanisms (KEMs) and **CRYSTALS-Dilithium** for digital signatures, both of which are lattice-based (National Institute of Standards and Technology, 2022).

Code-Based Cryptography

Code-based cryptography, first introduced by McEliece in 1978, relies on the difficulty of decoding general linear error-correcting codes (McEliece, 1978). Given a noisy codeword and a generator matrix, the problem is to find the original message, which is computationally intensive for random codes.

Security Benefits: This family has a **long history of cryptanalytic scrutiny**, spanning over four decades, without significant breakthroughs. This extensive analysis lends high confidence in its security against both classical and quantum attacks. Its security relies on a well-understood hard problem, the general decoding problem, which is known to be NP-hard and for which no efficient quantum algorithm exists.

Technical Limitations: The most significant practical drawback of code-based cryptography is its **very large key sizes**. The public keys for schemes like the original McEliece can be several megabytes, posing substantial challenges for storage, transmission, and memory, making them less practical for many internet-scale applications or resource-limited devices. They also have **limited applicability**, primarily supporting encryption (KEMs) and, less commonly, digital signatures, without the versatility for advanced functionalities seen in lattice-based schemes. NIST has selected the **Classic McEliece** for standardization within its portfolio, acknowledging its strong security despite key size concerns (National Institute of Standards and Technology, 2022).

Other PQC Candidates and NIST Standardization

Beyond lattices and codes, other PQC candidates under active research include **hash-based cryptography** (relying on the security of cryptographic hash functions, known for relatively small keys but stateful nature for signatures), **multivariate cryptography** (based on solving systems of multivariate polynomial equations over finite fields), and **isogeny-based cryptography** (deriving security from the difficulty of finding paths in graphs of supersingular elliptic curves).

The **NIST PQC Standardization Process** has been instrumental in guiding the development and selection of quantum-resistant algorithms. Through multiple rounds of rigorous evaluation by the global cryptographic community, NIST aims to identify a portfolio of diverse, robust, and practical PQC algorithms suitable for widespread deployment. This process is crucial for ensuring interoperability, building trust, and facilitating the necessary global migration to a quantum-safe cryptographic infrastructure.

IARJEDI

PQC Implementation Feasibility in African Industries

The global transition to Post-Quantum Cryptography (PQC) presents a complex set of technical, economic, and organizational challenges. While these challenges are universally faced, their manifestations and severity can vary significantly across different regions. For African industries, the implementation of PQC introduces additional layers of complexity due to existing socio-economic and infrastructural disparities.

General Challenges of PQC Implementation (Global)

Implementing PQC solutions globally requires overcoming several significant hurdles:

Performance Overhead: PQC algorithms, especially early candidates, tend to have larger key sizes, larger signature sizes, and can be computationally more intensive than their pre-quantum counterparts. This leads to **increased latency** in cryptographic operations and reduced **throughput**, which can be particularly impactful in high-volume, real-time applications like secure web browsing (TLS handshakes) or network encryption. Optimizing these algorithms for speed and efficiency is an ongoing area of research.

Key Management and Storage: The larger key sizes of PQC algorithms necessitate adjustments to existing key management infrastructures. Storing, distributing, and retrieving these larger keys efficiently without introducing new vulnerabilities presents a substantial challenge. Solutions may require upgraded hardware modules (e.g., Hardware Security Modules or HSMs) and revised key management protocols.

Migration Complexity: The cryptographic "heart" of most digital systems is deeply embedded in various layers—from hardware firmware to operating systems, application software, and network protocols. Updating all these components to support PQC is a monumental task. It involves modifying fundamental protocols like TLS, IPsec, and SSH, updating cryptographic libraries, and ensuring backward compatibility where necessary. This complexity demands significant coordination across vendors, developers, and users.

Supply Chain Security: As PQC algorithms are integrated into products and services, ensuring the integrity and security of the entire supply chain becomes paramount. Any compromise in the supply chain, such as malicious code injection during development or manufacturing, could undermine the security benefits of PQC.

Scarcity of Skilled Personnel: There is a global shortage of cybersecurity professionals with expertise in advanced cryptography, let alone the specialized knowledge required for PQC.

Designing, implementing, testing, and maintaining PQC systems demands deep understanding of quantum mechanics, number theory, and secure coding practices.

Specific Challenges for Africa

While African industries contend with the global challenges mentioned above, they also face unique, often compounded, obstacles that can impede PQC adoption:

Digital Infrastructure Disparities: Many parts of Africa still suffer from **uneven access to high-speed internet**, particularly in rural areas. This limits the ability to rapidly download and deploy large PQC updates or to support latency-sensitive PQC operations. Furthermore, **unreliable power supply** and a general lack of **modern computing resources** (e.g., outdated servers, limited bandwidth) can hinder the performance and stability of PQC-enabled systems.

Cost Implications: The initial investment required for PQC-enabled hardware and software upgrades can be prohibitive for many African businesses and governments. Licensing new PQC-compatible software, acquiring or upgrading HSMs, and training personnel represent significant capital expenditures that may be difficult to justify in economies facing other pressing development needs.

Lack of Local Expertise: Africa faces a severe shortage of professionals with specialized skills in quantum computing and advanced cryptography. Educational institutions often lack the resources to offer comprehensive programs in these cutting-edge fields, and opportunities for local research and development are limited. This necessitates reliance on external consultants, which can be costly and less sustainable in the long term.

Policy and Regulatory Gaps: Many African countries currently lack clear **national strategies or policy frameworks for PQC adoption**. Without government guidance, mandates, or incentives, organizations may delay their transition, leading to a fragmented and potentially insecure digital landscape. A coordinated national approach is crucial for establishing standards and driving widespread adoption.

Reliance on Legacy Systems: A significant portion of critical infrastructure and established industries in Africa still operates on **older, legacy IT systems** that are inherently difficult and costly to upgrade. These systems may not be designed to accommodate the larger key sizes or higher computational demands of PQC, posing a substantial challenge to migration.

Limited R&D Investment: Compared to more developed regions, there are **lower levels of public and private investment in cutting-edge cybersecurity research and development** within

Africa. This hinders the ability to locally innovate, customize PQC solutions for specific African contexts, and contribute to the global PQC knowledge base.

Key Industries for PQC Adoption in Africa

Despite the challenges, several key industries in Africa have an urgent need to prioritize PQC adoption due to the sensitive nature of their data and the long-term implications of quantum attacks:

Financial Services: The banking sector, including the rapidly expanding **mobile money** ecosystem, is a prime target. Protecting financial transactions, customer data, and interbank communications is critical. A quantum attack could lead to widespread fraud, loss of trust, and economic instability.

Telecommunications: Network operators are responsible for securing vast amounts of user data and critical communication infrastructure. PQC is essential for ensuring **network security, data privacy, and the integrity of communication channels** against quantum-enabled eavesdropping or tampering.

Government & Critical Infrastructure: Sectors like **energy, water, transportation, and national security** rely heavily on secure digital systems. Protecting long-term classified data, command and control systems, and SCADA networks from quantum adversaries is paramount for national sovereignty and public safety.

Healthcare: The digitization of healthcare records means sensitive **patient data** is increasingly vulnerable. PQC is crucial for securing Electronic Health Records (EHRs), telehealth communications, and medical research data, ensuring patient privacy and data integrity for decades to come.

Emerging Technologies: Technologies like **Blockchain** are gaining traction in various African sectors (e.g., land registries, supply chain tracking). While blockchain offers inherent security features, most current implementations rely on cryptographic primitives (like ECDSA for digital signatures) that are susceptible to quantum attacks. PQC integration is vital for **ensuring the future resilience and immutability of distributed ledgers**.

In sum, while the imperative for PQC adoption is global, Africa faces a compounded set of challenges related to infrastructure, expertise, cost, and policy. Addressing these specific regional hurdles is crucial for a successful and equitable transition to a quantum-safe digital future across the continent.

Strategies and Recommendations for Africa

Navigating the transition to a post-quantum cryptographic landscape in Africa requires a multi-faceted and strategic approach that addresses both global and continent-specific challenges. Proactive measures, collaborative efforts, and targeted investments are crucial to ensure that African industries are not left vulnerable in the quantum era.

Capacity Building & Education

A fundamental step is to cultivate a robust talent pool equipped with the necessary skills.

Promoting STEM Education: African nations must significantly invest in and reform **STEM education** from primary to tertiary levels, with a specific emphasis on mathematics, computer science, and physics, which form the bedrock for quantum computing and advanced cryptography. Curricula should be updated to include introductory concepts of quantum mechanics and cryptography.

Establishing Specialized Training Programs and Certifications: Universities and vocational institutions should develop **specialized postgraduate programs, workshops, and certifications** in quantum information science, post-quantum cryptography, and advanced cybersecurity. These programs could be short-term or long-term, catering to different professional needs, including upskilling existing IT and security professionals.

International Collaborations and Knowledge Transfer: Fostering partnerships with leading international research institutions, universities, and technology companies is vital. This can facilitate **knowledge transfer**, joint research projects, faculty and student exchange programs, and access to advanced computational resources and expertise not yet available locally. Leveraging diaspora networks can also be a powerful tool for bringing expertise back to the continent.

Policy and Regulatory Frameworks

Clear governmental direction and support are essential to drive PQC adoption.

Developing National PQC Migration Roadmaps: Governments, in consultation with industry and academia, should develop **national PQC migration roadmaps**. These roadmaps would outline timelines, prioritize critical sectors, specify technical guidelines, and define roles and responsibilities for the PQC transition. This provides a clear path and reduces uncertainty for organizations.

Incentivizing PQC Adoption: To mitigate the high initial costs, governments can introduce **incentives such as grants, tax breaks, or subsidies** for businesses and critical infrastructure operators that invest in PQC research, development, and implementation.

Harmonizing Standards Across the Continent: Regional bodies like the African Union and sub-regional economic communities (e.g., ECOWAS, SADC, EAC) should work towards **harmonizing PQC standards and best practices**. This will promote interoperability, facilitate cross-border digital trade, and ensure a unified approach to cybersecurity across the continent.

Infrastructure Development

Robust digital infrastructure is a prerequisite for effective PQC implementation.

Investing in Robust and Resilient Digital Infrastructure: Continued investment in **high-speed internet connectivity**, reliable and affordable electricity, and modern data center facilities across the continent is crucial. This foundational infrastructure will support the computational demands of PQC and enable seamless updates.

Exploring Hybrid Cloud and Edge Computing Models: To manage the potential **performance overheads and key management complexities** of PQC, African industries should explore hybrid cloud strategies. Leveraging global cloud providers for initial PQC deployments while integrating edge computing for latency-sensitive applications can optimize resource utilization and manage costs.

Phased and Hybrid Implementation

A pragmatic and adaptive approach to migration is necessary.

Adopting Hybrid Cryptographic Solutions: As an interim and secure measure, organizations should adopt **hybrid cryptographic solutions**. This involves running both a traditional (e.g., ECC) and a PQC algorithm (e.g., Kyber) concurrently for key exchange and digital signatures. This approach provides immediate quantum resistance while maintaining backward compatibility and offering a safety net in case of unforeseen PQC vulnerabilities (National Academies of Sciences, Engineering, and Medicine, 2019).

Prioritizing High-Risk Data and Critical Systems: Given resource constraints, a phased deployment is essential. Organizations must conduct thorough risk assessments to identify **high-risk data, long-lived data, and critical systems** (e.g., government communications, financial transactions, energy grids) that require immediate PQC protection. This allows for a strategic allocation of resources.

Fostering Local Innovation

Building indigenous capacity for PQC development and deployment.

Encouraging Local Startups and Research Centers: Governments and private sector entities should actively **encourage and fund local startups** focused on cybersecurity, quantum technologies, and PQC solutions. Establishing dedicated **research centers of excellence** in universities and leveraging existing tech hubs can foster innovation and tailor solutions to local contexts.

Public-Private Partnerships: Collaborative models between government, academia, and industry are vital for **joint PQC research, pilot projects, and the development of localized solutions**. This ensures that research translates into practical applications and that industry needs inform academic endeavors.

Cost-Effective Solutions

Addressing the financial barriers to PQC adoption.

Leveraging Open-Source PQC Libraries: African developers and organizations should explore and actively contribute to **open-source PQC libraries** (e.g., liboqs, OpenSSL's PQC forks). This can significantly reduce software development costs, promote transparency, and allow for community-driven security vetting.

Cloud-Based PQC Services: For organizations unable to invest heavily in on-premise hardware, utilizing **cloud-based PQC services** offered by major cloud providers can be a cost-effective alternative. This allows organizations to consume PQC capabilities as a service, reducing upfront hardware costs and maintenance burdens.

By systematically addressing these strategic areas, African nations can build a resilient and quantum-safe digital future, safeguarding their economies, critical infrastructures, and the privacy of their citizens in the face of evolving technological threats.

Conclusion

The advent of quantum computing casts an undeniable shadow over the current cryptographic landscape, posing an urgent and substantial threat to the digital security of nations worldwide, including those in Africa. The "store now, decrypt later" paradigm means that even today's encrypted data is vulnerable to future quantum attacks, underscoring the critical need for a proactive transition to Post-Quantum Cryptography (PQC). For African industries, this transition

is compounded by unique challenges, including digital infrastructure disparities, limited local expertise, significant cost implications, and nascent policy frameworks.

However, these challenges are not insurmountable. A strategic, multi-pronged approach encompassing robust capacity building and education, the establishment of clear policy and regulatory frameworks, sustained investment in digital infrastructure, and a pragmatic phased implementation strategy using hybrid solutions, is essential. Fostering local innovation and embracing cost-effective open-source and cloud-based solutions can further mitigate the economic burden. Proactive PQC adoption is not merely a technical upgrade; it is an imperative for securing Africa's digital sovereignty, protecting sensitive data, ensuring the continuity of critical services, and fostering sustainable economic growth and national security in the rapidly evolving global digital economy. This requires concerted, collaborative efforts from governments, industries, academia, and international partners to build a truly quantum-safe future for the continent.

References

National Academies of Sciences, Engineering, and Medicine. (2019). *Quantum computing: Progress and prospects*. The National Academies Press.

Ajtai, M. (1996). Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* (pp. 99-108). ACM.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169-178). ACM.

Goldreich, O., Goldwasser, S., & Halevi, S. (1997). Eliminating amortization from learning graphs. *Journal of Computer and System Sciences*, *55*(2), 295-313.

McEliece, R. J. (1978). *A public-key cryptosystem based on algebraic coding theory* (No. DSN-PROG-500-15). Jet Propulsion Lab, California Institute of Technology.

National Institute of Standards and Technology. (2022). *Post-Quantum Cryptography Standardization*. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 212-219). ACM.

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th anniversary ed.). Cambridge University Press.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* (pp. 124-134). IEEE.

Alhassan, M., Khan, S., & Kim, S. (2023). *Post-Quantum Cryptography in Financial Transactions: Opportunities and Challenges*. Journal of Financial Security, 12(2), 45–61.

Bindel, N., Buchmann, J., Krausz, R., & Münster, S. (2022). *Efficient Post-Quantum Signatures for Embedded Devices*. ACM Transactions on Embedded Computing Systems, 21(4), 1–22.

Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

NIST. (2023). *Post-Quantum Cryptography Standardization*. National Institute of Standards and Technology. https://csrc.nist.gov/projects/post-quantum-cryptography

Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

Khan, S., Alhassan, M., & Kim, S. (2023). *Quantum Threats to Financial Systems: Mitigation via PQC*. Journal of Digital Finance, 4(1), 22–40.

NIST. (2023). *Post-Quantum Cryptography Standardization*. National Institute of Standards and Technology. https://csrc.nist.gov/projects/post-quantum-cryptography

NCC. (2022). *Cybersecurity in Nigeria: Threats, Trends, and Future Directions*. Nigerian Communications Commission. https://www.ncc.gov.ng

Preskill, J. (2018). *Quantum Computing in the NISQ era and beyond*. Quantum, 2, 79. https://doi.org/10.22331/q-2018-08-06-79

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.