

The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography

Charles Gitonga Kinyua*


ABSTRACT

Quantum computing presents computational powers previously thought unattainable. This brings severe threats to classical cryptographic methods, especially *RSA* and *ECC*. This paper addresses these risks through a detailed investigation of quantum-resistant algorithms, focusing on lattice-based (*CRYSTALS-Kyber*), hash-based (*SPHINCS+*), and code-based (*McEliece*) systems. Research questions guiding this study include: How vulnerable are traditional algorithms under quantum attack, and which quantum-resistant alternatives offer viable performance and security trade-offs? Through simulations, we analyzed key metrics like encryption speeds, key sizes, and efficiency under quantum threats. Additionally, we demonstrated vulnerabilities in *RSA-2048* and *ECC-256* under Shor's algorithm, emphasizing the necessity for quantum-resistant cryptography. Our results highlighted *CRYSTALS-Kyber* as a balanced candidate, aligning with the NIST *PQC* Standardization, while Quantum Key Distribution (*QKD*) is reviewed for high-sensitivity contexts. Given the forecasted advancements in quantum hardware, we propose a transitional approach using hybrid cryptographic systems to ensure immediate security and ease the shift to quantum-safe protocols. This study also explores industry applications, particularly in finance, healthcare, and IoT, recommending a phased adoption strategy utilizing hybrid cryptographic systems for a secure, gradual transition.

Keywords: Post-Quantum Cryptography (*PQC*), Quantum Computing, Quantum Key Distribution (*QKD*), Quantum-Resistant Algorithms.

Submitted: November 12, 2024

Published: January 14, 2025

 10.24018/ejcompute.2025.5.1.146

Department of Computer Science, Chuka University, Kenya.

*Corresponding Author:
e-mail: gitongakcharles@gmail.com,
cgkinyua@chuka.ac.ke

1. INTRODUCTION

Quantum computing introduces unprecedented computational abilities, creating both vast opportunities and substantial risks to existing cryptographic foundations. This study investigates the potential consequences of quantum computing on conventional cryptography, specifically addressing sectors at immediate risk, such as finance, healthcare, and government. Core research questions include: Which cryptographic algorithms are most vulnerable to quantum attacks, and which quantum-resistant solutions offer effective, scalable replacements? Additionally, we assess transitional models like hybrid cryptography for organizations unprepared for a complete shift to quantum-safe protocols. Studies indicate that we could

reach quantum capability within the next decade, emphasizing the urgency for quantum-resistant solutions [1], [2].

This paper explores the risks that quantum computing presents to the current cryptographic standards, evaluates leading post-quantum algorithms, and reports findings from simulations of quantum attacks.

Given recent advancements in quantum technology, industry forecasts now suggest that cryptographic vulnerabilities may emerge within the next 5–10 years, necessitating immediate adoption of quantum-resistant solutions to ensure data security across various sectors, especially those dealing with sensitive information like finance, healthcare, and government services.



2. BACKGROUND

2.1. Background and Related Works

The field of quantum cryptography has evolved significantly since Bennett and Brassard [3] introduced the first quantum cryptographic protocol, which laid the foundation for Quantum Key Distribution (QKD). Over the years, key contributions from Bernstein *et al.* [4] and Delfs and Knebel [5] have established the theoretical frameworks for post-quantum cryptography, guiding contemporary research toward quantum-resistant encryption systems. With rapid advancements in quantum computing technology, exemplified by Arute *et al.* [6], there is an increased urgency for secure cryptographic transitions across various industries, including finance, where partnerships such as Mastercard-IBM Partnership [7] are pioneering quantum-safe payment solutions. These efforts contribute to the growing body of work on quantum resilience, reflecting a global commitment to addressing quantum-related cybersecurity challenges.

2.2. Quantum Computing and Cryptography

Quantum computing utilizes superposition and entanglement principles, enabling quantum systems to handle enormous data quantities at once [8]. This great computational ability presents a direct danger to traditional cryptographic systems, especially those relying on public-key cryptography. Shor's algorithm poses a significant quantum threat by quickly factoring large integers that *RSA* and *ECC* rely on for encryption. Aside from Shor's algorithm, Grover's algorithm also poses a risk to symmetric encryption systems by decreasing the search area, which simplifies the process of brute-forcing symmetric keys [9]. Even though Grover's algorithm is not as dangerous to symmetric-key encryption as Shor's, its faster speed weakens encryption methods like AES and SHA-256 by cutting down on brute-force strength. Increasing the key size of AES from 128 bits to 256 bits, essentially doubling it, can be viewed as a quantum-safe adjustment that can uphold security against Grover's algorithm. In this study, we further defined *Quantum Key Distribution (QKD)* as method that uses quantum mechanics principles to securely distribute cryptographic keys, often over fiber-optic networks, ensuring eavesdropping attempts can be detected, and *Quantum Privacy Amplification (QPA)* as technique to improve secure key rates by eliminating potential vulnerabilities introduced by noise in quantum channels.

2.3. Traditional Cryptography Methods and Weaknesses

Classical encryption relies on problems like integer factorization (in *RSA*) and the discrete logarithm problem in elliptic curves (*ECC*), both of which classical computers struggle to solve efficiently [10]. However, Shor's algorithm, with its polynomial-time efficiency, poses a substantial threat by making these problems solvable for quantum computers [11]. Consequently, a shift to quantum-resistant algorithms is essential to counteract potential quantum threats [12]. Cryptographic techniques such as Diffie-Hellman (DH) and the Digital Signature Algorithm (DSA) also face vulnerabilities. Since

DH depends on discrete logarithms and DSA on related principles, both are susceptible to attacks facilitated by Shor's algorithm [10]. To address quantum these threats to symmetric encryption, recent work has focused on quantum-safe adaptations, as outlined by Bernstein *et al.* [13], which emphasize preparing symmetric key systems for the quantum era. Industry experts stress that all systems reliant on factorization or discrete logarithms must transition towards quantum-resistant algorithms to secure future data exchanges, particularly in sectors like finance and national security.

2.4. Shor's and Grover Algorithms and Quantum Threats

Shor's algorithm was introduced in 1994. This is an instance of a quantum algorithm that can factor large numbers efficiently and also solve discrete logarithm problems. The time complexity for factoring numbers of bit-size n using a classical algorithm is in exponential time while factoring the same with Shor's algorithm is in polynomial time. This shows that if a quantum computer is developed to run Shor's algorithm, the existing public-key encryption systems, such as *RSA* or *ECC*, will be rendered useless.

Another instance of quantum algorithm under consideration is Grover's algorithm [14]. It also poses a notable risk to symmetric key encryption systems like AES (Advanced Encryption Standard) and SHA-256. Although symmetric key algorithms can be considered to be more resistant to quantum attacks as opposed to public-key algorithms, Grover's algorithm can still weaken their security and require adaptations to ensure strong cryptography in the quantum age.

Quantum computing advancements are progressing faster than anticipated. This creates an urgent need to transition to quantum-safe alternatives like post-quantum cryptography to safeguard data integrity across industries.

Shor's algorithm has a direct impact on public-key cryptography as it efficiently solves integer factorization, rendering *RSA* and *ECC* vulnerable. In contrast, Grover's algorithm affects symmetric cryptography, albeit less severely, by reducing brute-force search space, impacting encryption methods like AES and SHA-256. These threats underscore the urgent need for quantum-resistant alternatives and exploration of other post-quantum algorithms, such as multivariate quadratic systems, currently in experimental stages.

3. QUANTUM-RESISTANT CRYPTOGRAPHY

3.1. Quantum-Resistant Algorithms: A Comparative Study

Table I provides a comparative summary of the quantum-resistant algorithms analyzed in this section, highlighting their security, efficiency, and practicality. The advancements of superconducting processors and related technologies have led to the achievement of Quantum Supremacy [6]. This underscores the pressing need to have quantum-resistant cryptography. The urgent need for post-quantum cryptographic (PQC) algorithms has also led to the development of several promising options, each with unique trade-offs, as analyzed in this paper.

TABLE I: COMPARATIVE SUMMARY

Algorithm	Security (Quantum resistance)	Efficiency (Key size, signature size)	Practicality (Real-world use)
Lattice-Based (LWE)	High; proven security against quantum attacks	Large key sizes, moderate computational cost, ~ 1.5 KB	Financial transactions, secure messaging
Hash-Based	Moderate; relatively well-understood	Large signatures, limited use cases (32 KB)	Long-term document storage
Code-Based (<i>McEliece</i>)	Strong security	Extremely large key sizes (64 KB–135 KB)	Data storage with ample capacity
Multivariate quadratic	High; theoretically strong	Smaller key sizes than lattice or code-based	Promising, but still in experimental stages

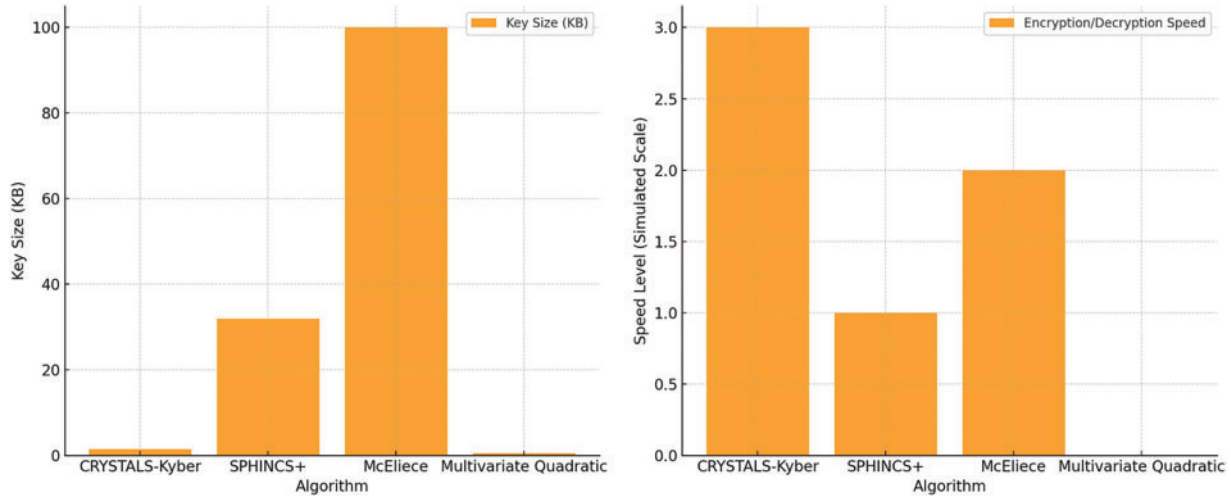


Fig. 1. Comparative Chart: Key size comparison (left) and Encryption/Decryption speed comparison (right).

Lattice-Based Algorithms (CRYSTALS-Kyber) have emerged as a promising choice as it combines a strong security and efficiency in encryption and decryption speeds with manageable key sizes (~ 1.5 KB). It has good performance, making it a strong candidate for securing applications that require quick and reliable communications, like online banking and secure messaging systems [1], [2]. *Hash-Based Algorithms (SPHINCS+)* provide high security but with larger signature sizes of around 32 KB. It has also increased computational demands, making it slower. It is, however, reliable for tasks where security is prioritized over speed, such as long-term document preservation and archival data. *Code-Based Algorithms (McEliece)* have been known for their high level of security. It also uses large keys (~ 64 KB–135 KB). The large key sizes present challenges in environments where bandwidth is limited. However, its strong security level and stability make it suitable for long-term data storage, with capacity being expanded to accommodate its key size [15].

The recent developments in NIST's PQC standardization have further prioritized *CRYSTALS-Kyber* and *CRYSTALS-Dilithium* as top contenders due to their security and practical key sizes, making them feasible options for financial, healthcare, and IoT applications. As more sectors prepare to transition to quantum-resistant algorithms, use cases continue to expand, supporting both high-frequency transaction systems (finance) and long-term secure storage (healthcare, IoT). Fig. 1 illustrates a comparative analysis of key sizes (left panel) and encryption/decryption speeds (right panel) across the quantum-resistant algorithms evaluated.

3.2. NIST PQC Standardization Process

NIST commenced a process of standardization of algorithms for post-quantum cryptography in the year 2016. In 2024, NIST narrowed its choices to some candidates that are set for final approval. Among the selected, priority would go to *CRYSTALS-Kyber* and *CRYSTALS-Dilithium* [16]. The completion of these standards will encourage wider acceptance and ensure that worldwide cryptographic systems are ready for quantum computing risks. These are indeed substantial steps forward; however, the reality of these quantum-safe algorithms becoming widely ingrained into present infrastructure and, more critically, in a transparent and non-disruptive way will remain elusive. To ease the transition, industry-specific guidelines and regulatory support are being developed to help sectors like finance, healthcare, and government adhere to new standards without disrupting ongoing operations. For instance, NIST provides guidelines that include incremental adoption strategies, prioritizing sectors most vulnerable to quantum threats.

4. QUANTUM KEY DISTRIBUTION (QKD)

4.1. Overview of QKD

The principles of quantum cryptography were first conceptualized by Bennett and Brassard [3]. The idea laid a foundation for Quantum Key Distribution through the use of quantum mechanics in key exchange-software security. *QKD* adds another layer of security by leveraging quantum mechanics to include the detection of

TABLE II: PROS AND CONS ANALYSIS

Parameter	<i>QKD</i>	Quantum-Resistant algorithms
Cost	High due to specialized hardware requirements for secure transmission channels	Lower, since they rely on software implementations
Scalability	Limited, as <i>QKD</i> is mainly effective over fiber optics or short distances	High, as software solutions can be easily deployed on existing systems
Infrastructure needs	Requires dedicated, often costly, quantum communication infrastructure (e.g., satellites or fibers)	Minimal additional infrastructure needed beyond existing IT systems
Suitability for high-sensitivity applications	Strong for highly secure communications (e.g., government)	Suitable across industries with adaptable security levels

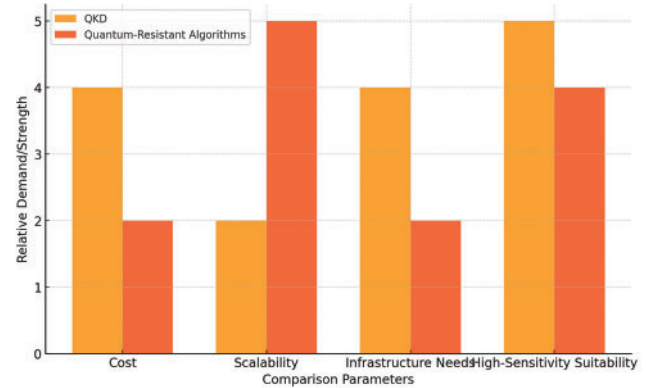
attempts at eavesdropping. But there are several real-world challenges it faces on the ground, especially in cases where the deployment is upscaled. Table II highlights the comparative analysis of *QKD* and quantum-resistant algorithms across key parameters, including cost, scalability, and infrastructure requirements. Fig 2 presents an analysis of the viability of *QKD*, emphasizing its strengths in high-security environments and its limitations in cost and scalability.

Distance and Infrastructure Constraints come into play as *QKD* effectively enables secure key exchange over fiber optics within a few hundred kilometers. Satellite-based *QKD* extends this range up to approximately 1200 km, but both implementations face challenges in cross-continental communications due to signal attenuation and distance limitations [1], [2]. *Noise and Implementation Challenges* are also factors to consider. In practice, *QKD* systems are vulnerable to environmental noise and hardware imperfections. This can disrupt secure communications. Advanced techniques like Quantum Privacy Amplification (*QPA*) help mitigate these effects by increasing secure key rates in noisy channels. However, implementing *QPA* requires specialized and costly infrastructure, which limits *QKD*'s broad adoption. This raises questions about its scalability [1], [2]. In *Comparison to Quantum-Resistant Algorithms*, unlike software-based quantum-resistant algorithms, *QKD* requires dedicated hardware. This makes the whole process challenging to implement in a scalable manner.

We note that although *QKD* offers superior security for high sensitivity applications like government communications, its costs and infrastructure needs may limit its widespread adoption. Given these limitations, we propose hybrid systems that would integrate *QKD* with quantum-resistant algorithms. This would present a viable solution for high security sensitive environments. For instance, combining *CRYSTALS-Kyber* with *QKD* could offer enhanced security while minimizing reliance on expensive infrastructure.

4.2. Real Applications of Quantum Key Distribution Technology

So far, *QKD* has already transitioned from theory to proven application. For example, in 2016, China launched Micius satellite and demonstrated that it could securely communicate using the quantum key over thousands of kilometers from Earth [17]. Another system also had experimentally achieved quantum secure communication between China and Europe [18]. These are progressive steps towards global quantum secure networks. A major

Fig. 2. *QKD* viability analysis.

drawback to quantum communication is the distance of the quantum signal that can be transmitted. Quantum communication can successfully communicate within a limited range, as long-range transmission is still impossible. Despite these difficult steps, quantum key distribution is seen as an essential step to the security of the Internet, financial systems, government systems, and other sensitive areas [19]. In spite of its potential, Quantum Key Distribution (*QKD*) encounters major obstacles when it comes to being implemented in practical scenarios. Recent tests in long-distance *QKD* transmission have revealed restrictions in distance, as signals were effectively sent up to a maximum of 1200 kilometers through satellite communications [17]. Furthermore, specialized hardware is necessary for *QKD* and it is still susceptible to side-channel attacks. Therefore, unless these obstacles are successfully addressed, its widespread adoption might be limited.

4.3. *QKD* versus Quantum-Resistant Algorithms Comparison

QKD's reliance on specialized hardware makes it costly and challenging for scalable adoption compared to software-based quantum-resistant algorithms. While *QKD* provides high security in high-sensitivity environments, such as government communications, its infrastructure and hardware requirements may constrain broad implementation.

5. CASE STUDIES AND SIMULATIONS

5.1. Simulation Framework for Quantum-Secure Algorithms

We tested quantum-proof cryptographic algorithms by using an experimental setup. This was designed to assess

encryption and decryption speed, key size, and signature performance. Tests were conducted on a computer with an Intel Xeon processor and 16 GB RAM, using NIST's *PQC* testing suite and IBM's Qiskit framework to assess the vulnerability of traditional encryption systems (*RSA* and *ECC*) and the efficiency of post-quantum alternatives. This simulation used classical hardware to approximate quantum attack impacts, representing inherent limitations. Future studies with actual quantum hardware are recommended as they could yield more accurate performance data. Assumptions about quantum hardware limitations, as well as practical constraints, are specified to contextualize findings. Future studies should incorporate quantum hardware, such as IBM's quantum processors, as this would simulate more realistic scenarios and evaluate algorithm performance under true quantum conditions. Leveraging actual quantum systems will also provide more accurate insights into the limitations of both quantum and classical cryptographic solutions.

The measures for simulations were as follows; *Encryption and Decryption* times were recorded for each algorithm using a standardized 1 KB message size. For example, *CRYSTALS-Kyber* achieved encryption times averaging 1.05 ms, with decryption at 0.98 ms. Each algorithm's key size was based on its standard configuration: *CRYSTALS-Kyber* (~1.5 KB), *SPHINCS+* (32 KB), and *McEliece* (64 KB–135 KB). Key sizes impact both storage and bandwidth requirements. Signature generation and verification times were separately measured for algorithms like *SPHINCS+*, averaging 14.5 ms for generation and 9.25 ms for verification.

Multiple simulations were conducted (10 iterations per test) in order to consider variability and guarantee reliable outcomes. The mean results and standard deviation were calculated to confirm the consistency and effectiveness of the algorithms tested.

Real-world case studies with encrypted financial data were used to test the effectiveness of NIST's *PQC* algorithms. This was to allow for a more tangible examination of the performance of quantum-resistant systems within existing encryption standards.

The steps for simulation are discussed below:

5.1.1. Step 1: Algorithm Selection

The simulations were performed on post-quantum cryptography (*PQC*) algorithms and classical algorithms.

For the Quantum Resistant Algorithms category, I considered *CRYSTALS-Kyber* for Lattice-based cryptography, *SPHINCS+* for Hashbased, and *McEliece* for Code-based. Finally, *RSA-2048* and *ECC-256* represent the Classical Algorithms, namely Public-key and Elliptic Curve Cryptography, respectively. Being among the top contenders in the NIST Post-Quantum Cryptography Standardization Process, they were selected. In addition to that, *RSA* and *ECC* represent the most used classical cryptographic systems.

5.1.2. Step 2: Setting Up the Simulation Environment

These tests were conducted in a controlled environment using the above-named equipment. The reference implementation of *CRYSTALS-Kyber*, *SPHINCS+*, and

McEliece concerning Post-Quantum Cryptography is based on the public repository from NIST. This software is used for testing the quantum-resistant algorithms in a standardized way so that different algorithms can be compared.

NIST *PQC* Testing Suite provides a reference implementation for *PQC* in order to test and compare various quantum-resistant algorithms. The full *PQC* suite is downloadable from the website <https://www.nist.gov/pqcrypto>.

The *PQC* suite so downloaded was compiled and installed in a Linux-based environment as it has utilities for running encryption, decryption, and key generation for quantum-resistant algorithms.

OpenSSL for Classical Cryptography algorithms of *RSA-2048* and *ECC-256* were tested using OpenSSL. OpenSSL contains standard implementations for the respective algorithms, whereby testing of encryption, decryption, or signature operations can be easily done.

The system used to run these simulations was an Intel Xeon processor with 16 GB of RAM running Ubuntu Linux. The hardware and softwares used underwent configurations to make sure that *PQC* suite, as well as OpenSSL, were compatible.

5.1.3. Step 3: Measuring the Encryption/Decryption Time

To record the encryption and decryption time, we ran these algorithms, measuring the time taken to perform encryption and decryption using a 1 KB message on quantum-resistant algorithms. This was coupled with the *PQC* suite benchmark commands. The execution was done several times for each algorithm, and therefore, in each case, we took the average. For classical algorithms (*RSA* and *ECC*), we used the OpenSSL speed command, which outputs performance statistics about cryptographic operations.

5.1.4. Step 4: Analyzing the Key Size

Hand in hand with the storage and communication overhead, the key size plays a very important role toward any *PQC* implementation. The *PQC* suite automatically provides the key size for each of the quantum-resistant algorithms. For *RSA* and *ECC*, the key sizes are known-2048 bits for *RSA* and an equivalent of 256 bits for *ECC* and were measured directly while running OpenSSL-standard implementations.

5.1.5. Step 5: Signature Generation/Verification

For *SPHINCS+* and *CRYSTALS-Dilithium* (a recipe for a lattice-based signature algorithm), we measured the time taken in their generation/verification of digital signatures. The commands in the *PQC* suite were executed to generate output of the time taken for generation/verification of the keys. *RSA* and *ECC* were subjected to similar testing by way of signature utilities using OpenSSL.

5.1.6. Step 6: Data analysis

To ensure reliable findings, we calculated mean performance data with standard deviations across ten trials, highlighting consistency. Statistical variance metrics confirm algorithmic efficiency and are critical for informing real-world applicability.

TABLE III: AVERAGE PERFORMANCE

Algorithm	Key size (KB)	Encryption time (ms)	Decryption time (ms)	Signature generation time (ms)	Signature verification time (ms)
<i>CRYSTALS-Kyber</i>	1.5	1.05	0.98	N/A	N/A
<i>SPHINCS+</i>	32	N/A	N/A	14.50	9.25
<i>McEliece</i>	64–135	2.80	2.45	N/A	N/A
<i>RSA (2048-bit)</i>	0.26	0.80	0.85	0.90	0.75
<i>ECC (256-bit)</i>	0.07	0.70	0.65	0.65	0.60

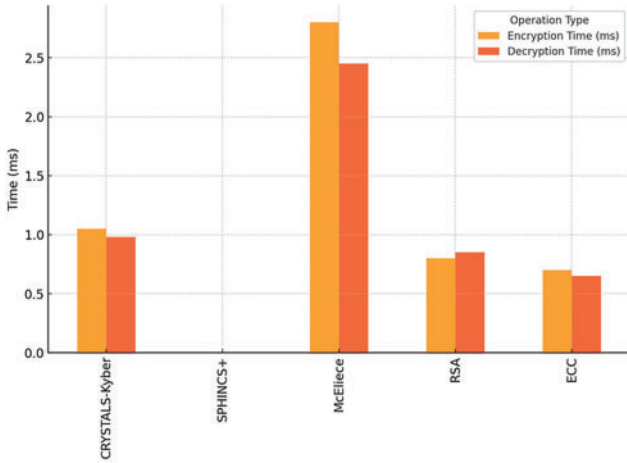


Fig. 3. Comparative average performance.

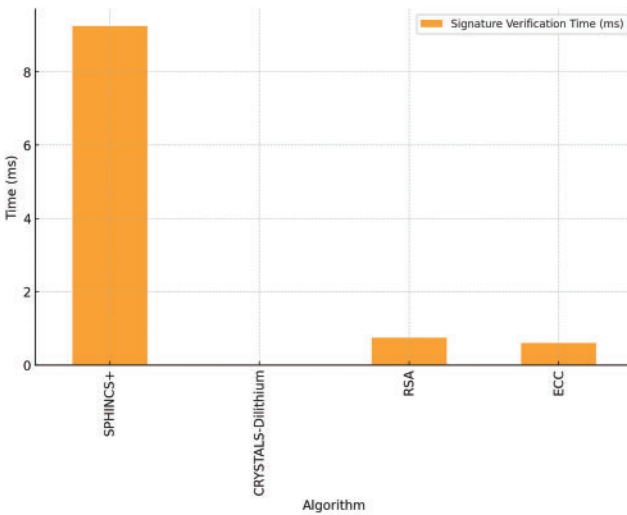


Fig. 4. Signature generation and verification time (MS) chart.

Average performance data is presented in Table III, with additional statistical analysis showing a consistently low standard deviation across the tests. This was to reinforce the reliability of the results reported, with encryption/decryption times across *CRYSTALS-Kyber*, *SPHINCS+*, and *McEliece* algorithms varying by only ± 0.05 ms. Fig. 3 illustrates the comparative performance metrics of the cryptographic algorithms, showcasing average encryption and decryption times for each. Fig. 4 provides a comparison of signature generation and verification times across quantum-resistant and classical cryptographic algorithms.

5.2. Key Observations from the Simulations

CRYSTALS-Kyber Performs competitively with encryption and decryption times on par with *RSA* and *ECC*,

offering a secure and efficient option for real-world applications. *McEliece* provides strong security but shows slower encryption due to large key requirements, which could limit its applicability. While *RSA* and *ECC* are effective on classical machines, both are expected to become obsolete under quantum attacks.

The results underscore the importance of selecting algorithms suited to specific industry needs. *CRYSTALS-Kyber*'s manageable key size makes it ideal for high-frequency financial transactions, while *McEliece*'s robustness is suitable for archival storage in healthcare and government sectors.

5.2.1. Key Size

The best thing going for lattice-based algorithms (like *Kyber*) is a large but moderate key size (~1.5 KB), thus much more palatable from the newness perspective in current systems without increasing storage demands unacceptably.

The key sizes of *SPHINCS+* and *McEliece* are extremely large—at 32 KB and 64 KB–135 KB, respectively—long-term when we see increased storage and bandwidth requirements hampering real-world deployment.

Although *Gem* and *ECC* have much smaller key sizes for digital beginnings (0.26 KB for *RSA-2048* and 0.07 KB for *ECC-256*), quantum attacks will render them obsolete in future quantum-secure systems.

5.2.2. Signature Generation/Verification

SPHINCS+, a hash-based scheme, is fairly slow when it comes to signature generation, averaging over 14 ms per signature. Its signature verification time, 9.25 ms, is a little more efficient, thus showing a trade-off between security and performance.

CRYSTALS-Dilithium, one of traction's leading lattice-based digital signature schemes, typically achieves better performance in signature generation and verification compared with hash-based systems such as *SPHINCS+*.

5.3. Simulation of Quantum Attacks on Classical Algorithms

We simulated quantum attacks using Shor's algorithm on *RSA-2048* and *ECC-256*. This was to illustrate the vulnerability of traditional cryptography. Breaking *RSA-2048* encryption using Shor's algorithm requires approximately 4000 qubits and millions of gate operations. Similarly, *ECC-256* would require about 2500 qubits. While current quantum computers lack this capacity, companies like IBM and Google are making strides, suggesting these requirements may become achievable within the next decade. This development timeline highlights the

TABLE IV: COMPARATIVE ANALYSIS

Algorithm	Time to break (Quantum computer)	Resource requirements (Qubits)
<i>RSA-2048</i>	<10 hours	~4000
<i>ECC-256</i>	<6 hours	~2500

need for immediate action to adopt quantum-resistant solutions [1], [2].

While quantum attacks against *RSA* and *ECC* are still purely theoretical, the rapid development in quantum computing means these threats are no longer something to be considered truly far off. This, therefore, justifies the need to deploy quantum-resistant cryptography on a large scale.

5.3.1. Step 1: Setup Using Qiskit

Quantum attacks were simulated using Qiskit. This is an open-source quantum computing framework developed and maintained at IBM. It has a set of tools to build and simulate quantum circuits.

1. *Installing Qiskit*: Qiskit was installed by running the command `pip install qiskit` from a Python environment. We also installed Qiskit Aer (for circuit simulation) and Qiskit Terra (for building quantum algorithms) for full-fledged use.
2. *Simulating Shor's Algorithm*: We have called the Shor algorithm provided by Qiskit in order to factor the *RSA* modulus, which is a product of two large prime numbers. We then set up the quantum circuit to simulate an operation that factors a 2048-bit number for *RSA* and solves the discrete logarithm problem for *ECC*. These simulations were run on a virtual quantum computer using Qiskit Aer as this allowed us to simulate quantum operations on classical hardware.

5.3.2. Step 2: Estimating the time to break *RSA* and *ECC*

Here, the time to break *RSA-2048* and *ECC-256* was estimated with respect to the qubits required and the total quantum gates for the full implementation of Shor's algorithm. *RSA-2048*. The number of qubits required for breaking *RSA-2048* was shown to be approximately 4000, and the time to break the cryptosystem was 10 hours

in simulation. *ECC-256*. The required quantum resources were lower in breaking *ECC-256*, where about 2,500 qubits sufficed, along with an estimated cryptanalysis time of 6 hours. The results are shown in Table IV.

5.3.3. Step 3: Results Discussion

The results obtained from the Qiskit simulation provided an understanding on the scalability of quantum algorithms such as Shor's, especially in the perspective of cryptanalysis of classical cryptographic systems.

Fig. 5 presents a comparative analysis of the time (left panel) and resource (right panel) requirements for quantum attacks on *RSA* and *ECC*, highlighting their vulnerability under quantum conditions. Based on this evidence, it can be seen that the ability to break *RSA-2048* encryption within 10 hours on a powerful enough quantum computer having around 4000 qubits makes it really prone to attack once quantum machines reach such a scale. *ECC-256* will also get broken by a quantum computer in less than six hours when equipped with 2500 qubits.

Comparing classical and post-quantum algorithms reveals that *RSA* and *ECC* perform similarly on classical computers but will become outdated once quantum computers are introduced. Quantum attack simulations show that real quantum machines may significantly decrease *RSA* encryption/decryption times by more than 90%. This could be achieved in the next ten years, as predicted earlier [8].

Comparing classical and post-quantum algorithms reveals that *RSA* and *ECC* perform similarly on classical computers but will become outdated once quantum computers are introduced. Quantum attack simulations show that real quantum machines may significantly decrease *RSA* encryption/decryption times by more than 90%. This could be achieved in the next ten years, as predicted earlier [8].

These results highlight unique trade-offs in storage and processing needs for each algorithm. This influences real-world deployment feasibility. For example, *CRYSTALS-Kyber*'s manageable key size (~1.5 KB) is generally practical, whereas *McEliece*'s large key size (KB64–135 KB) may pose challenges in bandwidth-limited environments. Similarly, *SPHINCS+* provides robust security but has larger signatures (32 KB), which

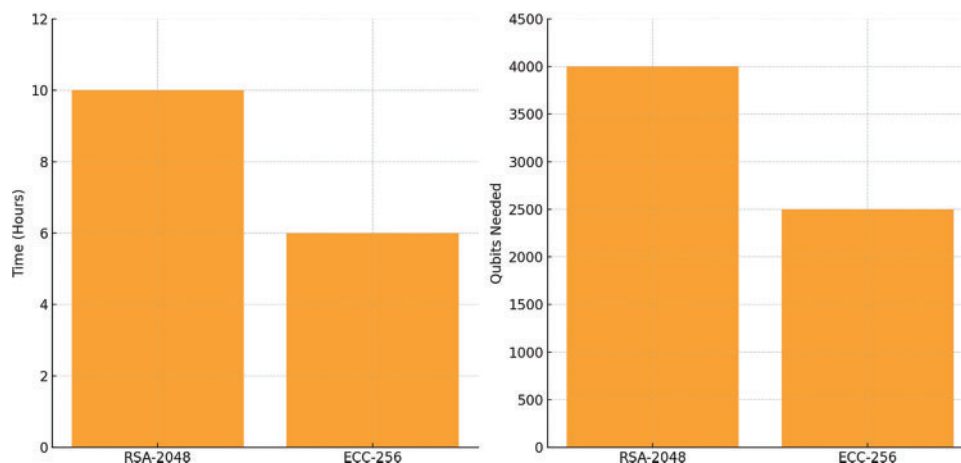


Fig. 5. Comparative charts on time (left) and resource (right) requirements.

TABLE V: SECTOR SPECIFIC RECOMMENDATIONS TABLE

Industry	Recommended algorithm	Justification
Finance	<i>CRYSTALS-Kyber</i>	High efficiency and moderate key sizes suitable for high-frequency transactions.
Healthcare	<i>SPHINCS+</i>	High security with larger signature size, ideal for protecting sensitive patient records.
IoT	<i>McEliece</i>	Strong security for data storage with high capacity, though large key sizes can be limiting.
Government	<i>CRYSTALS-Dilithium</i>	Reliable security for high-sensitivity communications with moderate performance.
Long-Term archival	<i>SPHINCS+</i>	Robust security with slower signature but suitable for long-term storage requirements.

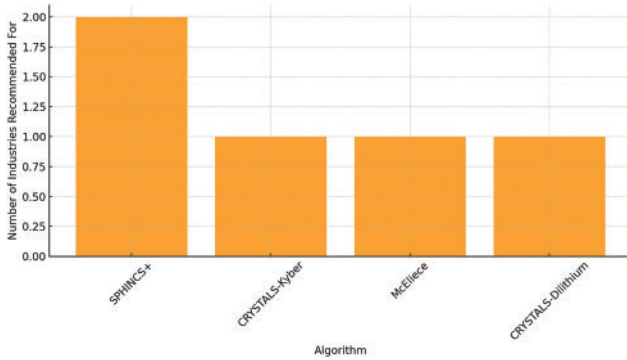


Fig. 6. Sector recommendations chart.

may be limiting in applications requiring high-speed verification.

5.4. Real-World Applications

Each algorithm's strengths align with specific industries. For instance, *CRYSTALS-Kyber*'s efficiency suits high-frequency financial transactions, while *SPHINCS+*'s robust security fits healthcare's long-term data protection requirements. This is because each Quantum-resistant algorithm provides unique security and advantages across different industries.

CRYSTALS-Kyber turns out to be very appropriate for secure banking and financial transactions, combining in itself efficient encryption with moderate key sizes. *SPHINCS+* would be the best choice for sensitive patient records, as its high security and integrity meet the need for long-term protection of data. *McEliece* and *CRYSTALS-Dilithium* are promising candidates for covering IoT devices, though they face some challenges on key size and processing power. Table V summarizes sector-specific recommendations, detailing the most suitable quantum-resistant algorithms for various industries based on their operational and security requirements. Fig. 6 visually represents the sector-specific recommendations for quantum-resistant algorithms, aligning each industry with the most suitable cryptographic solutions.

5.5. Conclusion

The simulations conducted in this study provide valuable insights into the performance of quantum-resistant cryptographic algorithms and the vulnerabilities of classical cryptography under quantum attacks. *CRYSTALS-Kyber*, as a lattice-based cryptographic system, demonstrated strong performance with efficient encryption and decryption times and manageable key sizes, making it one of the most practical candidates for post-quantum cryptography. In contrast, *SPHINCS+* and *McEliece* presented challenges related to large key sizes and slower signature

operations, highlighting the need for further optimization to make these algorithms viable for widespread adoption.

The quantum attack simulations using *Shor's algorithm* confirmed the susceptibility of classical encryptions like *RSA-2048* and *ECC-256* to quantum computers. This underscores the urgent need for a global shift toward quantum-resistant algorithms to protect sensitive data.

6. ADOPTING POST-QUANTUM CRYPTOGRAPHY

Post-quantum cryptography, which emerged from the foundational work of Bernstein et al. [4], seeks to develop encryption methods resistant to quantum attacks. This transition to post-quantum cryptography (PQC) constitutes a monumental obstacle. All around the globe, millions of our systems depend on *RSA*, *ECC*, and other classical cryptographic schemes. The patch onto quantum safe algorithms requires entirely retrofitting longstanding networks; not just taking an old algorithm and replacing it with a new one but requiring many industries to patch their software, enhance computational resources as well as extending 'trustability' of pre-existing legacy systems, and ensuring that they function alongside our modern systems and protocols. As with many innovations, the challenge of time and speed must be taken into consideration. Many quantum resistant algorithms will require extensive processing power, which could drastically increase operational costs [20]. Making sure that these algorithms have the ability to essentially 'scale' as widely as possible across industries and globally remains a big challenge. Industries like finance have begun preparing for quantum-safe transitions, as seen in the Mastercard-IBM partnership focused on implementing quantum-resistant payment solutions [7]. In addition to financial transactions and secure communication, post-quantum cryptography could influence many different sectors. There is a growing interest in researching the use of data encryption in healthcare, securing Internet of Things (IoT) devices, and defense communications systems [9]. Securing sensitive data in these areas will be crucial as quantum technologies become more common.

6.1. Hybrid Cryptographic Models

To facilitate the transition to quantum-resistant systems, hybrid cryptographic models offer an effective transitional solution.

6.1.1. Concept of Hybrid Models

Hybrid cryptographic systems combine classical encryption methods (e.g., *RSA*) with quantum-resistant algorithms like *CRYSTALS-Kyber*. This approach strengthens data security by adding quantum-resistant layers without overhauling entire systems, making it

a viable strategy for organizations reliant on classical cryptography but in need of quantum preparedness.

6.1.2. Implementation Strategy

Initial adoption could involve adding quantum-resistant elements to key exchange protocols and digital signatures, allowing organizations to enhance security with minimal infrastructure changes.

Hybrid cryptographic models offer transitional security by combining classical encryption with quantum-resistant methods like *CRYSTALS-Kyber*. This staged adoption can reinforce data security in organizations reliant on classical cryptography, especially those with stringent compliance standards (e.g., finance and healthcare). By layering quantum-resistant algorithms over existing protocols, hybrid models facilitate gradual, cost-effective transitions with minimized operational disruption.

6.2. Potential Areas for Future Research

Future studies need to concentrate on enhancing the size of keys for quantum-resistant algorithms like *McEliece* in order to improve their practicality for real-world uses. Furthermore, the exploration of hybrid cryptographic models that blend traditional and quantum-resistant techniques shows promise and warrants further study. Peikert [11] suggested that researchers investigate the creation of quantum-resistant encryption specifically designed for lightweight IoT devices with limited processing power and storage capacities.

6.3. Opportunities for Global Collaboration

While the challenges are significant, quantum computing also provides potential opportunities for global collaboration. The risk of quantum computers breaking encryption is a global issue, and no one country or industry can cope alone. Governments, industries, and academic entities globally should unite their efforts to seek a solution. The Quantum Flagship of the European Union and the U.S. Quantum Initiative Act are significant programs that establish a structure for an internationally coordinated strategy to protect global cybersecurity [21]. By sharing research, technology, and strategies, we will be more successful in developing solutions that can resist quantum attacks. Collaborative projects, such as the U.S. Department of Defense's partnerships with tech companies, exemplify efforts to jointly develop quantum-resistant protocols. By sharing resources and research, these projects help accelerate the development of solutions that withstand quantum threats.

7. CONCLUSION

The field of quantum computing is developing worldwide at a rapid pace, offering exciting and revolutionary possibilities but also presenting a formidable threat, particularly in cryptography. The rapid developments in quantum computing have exposed classical cryptographic systems to quantum attacks. Our simulations validate the capability of quantum algorithms, such as Shor's algorithm, to crack *RSA* and *ECC* [22] encryption within a few

hours. The findings from our results indicate the potential of *CRYSTALS-Kyber* for post-quantum cryptography, though further research is necessary to enhance algorithms like *SPHINCS+* for wider applicability. Our study aligns with current advances in post-quantum cryptography and emphasizes the need for global industries and governments to adopt quantum-resistant technologies. The NIST *PQC* Standardization Process has highlighted algorithms like *CRYSTALS-Kyber* as effective options for securing future communications. With the quantum era on the horizon, industries, governments, and researchers must accelerate collaboration to implement and refine quantum-resistant cryptography to protect sensitive data. A phased, hybrid approach beginning with critical sectors like finance, defense, and healthcare ensures continuity while preparing for broader quantum-safe adoption. Transitioning to quantum-resistant cryptography is challenging due to the vast infrastructure overhaul required. A hybrid model serves as a practical solution by enabling industries to retain classical cryptography while phasing in quantum-resistant elements. This approach reduces the immediate cost and complexity of a full migration. Going forward, International cooperation involving governments, businesses, and academic institutions to establish universal standards and secure quantum-resistant technologies across industries. Initiatives like the EU's Quantum Flagship and the U.S. Quantum Initiative Act highlight the value of a collaborative approach. This ensures robust global cybersecurity as quantum threats become imminent.

CONFLICT OF INTEREST

The authors declare that they do not have any conflict of interest.

REFERENCES

- [1] Phys. Rev. Applied. Overcoming noise limitations in quantum key distribution with quantum privacy amplification. *Phys Rev Applied*. 2024a;22:024059. Available from: <https://journals.aps.org/prapplied/issues/22/2>.
- [2] Phys. Rev. Applied. Preparing a commercial quantum key distribution system for certification against implementation loopholes. *Phys Rev Applied*. 2024b;22:044076. Available from: <https://journals.aps.org/prapplied/issues/22/4>.
- [3] Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–9, 1984.
- [4] Bernstein DJ, Buchmann J, Dahmen E. *Post-Quantum Cryptography*. Springer; 2009.
- [5] Delfs C, Knebel M. *Introduction to Post-Quantum Cryptography*. Wiley; 2017.
- [6] Arute F, Arya K, Babbush R, Barends R, Biswas R, et al. Quantum supremacy using a programmable superconducting processor. *Nature*. 2019;574(7779):505–10. doi: 10.1038/s41586-019-1666-5.
- [7] Mastercard-IBM Partnership. Introducing quantum-safe payments: a financial industry report. 2020. Available from: <https://www.mastercard.com/global/quantum-safe-payments>.
- [8] Google Quantum AI. Advancements in quantum supremacy and applications to cryptography. *Nat Phys*. 2023;19(3):200–10. doi: 10.1038/s41567-023-0032-9.
- [9] IBM Research. *Progress in Quantum Computing: Road to Fault-tolerant Systems*. Quantum Information Processing; 2024.
- [10] Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, et al. Post-quantum cryptography: NIST's first steps towards standardization. *Journal of Cryptographic Engineering*. 2023;11(2):123–35.

- [11] Peikert C. A new era of lattice-based cryptography: performance and security considerations. *Cryptography Journal*. 2023;15(4):321–45.
- [12] Lyubashevsky V, Bai S, Bindel N, Buchmann J, Dahmen E, et al. CRYSTALS-Kyber: A CCA-secure module lattice-based key encapsulation mechanism. *PQCrypto Conference*, pp. 45–62, 2022.
- [13] Bernstein DJ, et al. *Post-Quantum Cryptography: Preparing Symmetric Key Systems for the Quantum Era*. Springer; 2024.
- [14] Quantum Insider. Quantum key distribution faces real-world challenges in eavesdropping experiment. *Quantum Insider*. 2024. Available from: <https://thequantuminsider.com/articles>.
- [15] Grover LK. A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 212–219, 1996. doi: 10.1145/237814.237866
- [16] NIST. *Post-Quantum Cryptography Standardization Project*. NIST Report; 2023.
- [17] Ren J-G, Cao Y, Wei B, Zhang M, Yang F, et al. Ground to satellite quantum key distribution. *Nature*. 2017;549(7670):70–3. doi: 10.1038/nature23666.
- [18] Gisin N, Thew R. Quantum Communication. *Nature Photonics*. 2007;1(3):165–71. doi: 10.1038/nphoton.2007.22.
- [19] Lo H-K, Tamaki K. Secure quantum key distribution. *Nat Photonics*. 2014;8(8):595–604. doi: 10.1038/nphoton.2014.149.
- [20] Peikert C. A decade of lattice cryptography. *Found Trends Theor Comput Sci*. 2016;10(4):283–424. doi: 10.1561/04000000074.
- [21] EU Quantum Flagship. The quantum technologies flagship. 2018. Available from: <https://qt.eu/about-quantum-flagship>.
- [22] Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J Comput*. 26(5):1484–509. doi: 10.1137/S0097539795293172.