Journal of Information Systems Engineering and Management
2025, 10(41s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Investigating the Impact of Quantum Computing on Existing Encryption Methods

Neeraj Kahol Sharma

ARTICLE INFO

Received: 22 Dec 2024

Revised: 14 Feb 2025

Accepted: 22 Feb 2025

ABSTRACT

The development of quantum computing technologies represents a critical risk for virtually all classical encryption systems (RSA, AES, ECC) and cybersecurity will sustain immense damage. RSA and AES in total depend on modern cyber security as they use factoring and discrete logarithm problems whose solving is perilous via quantum algorithms like Shor's and Grover's. This study analyzes the impact of quantum computing on current encryption systems and the need for post-quantum cryptography (PQC). More precisely, its postgraduate level reads laced based cryptography and other quantum resistant algorithms as potential solutions. The paper also discusses other obstacles transitioning from classical encryption to PQC such as performance overhead, infrastructure deviation, and global standardization policies. Precedence finds and computational simulations expostulate the necessity for quantum safe encryptions and accentuated suggestions for further developments. These findings express the need for protection when quantum computing era becomes ubiquitous.

Keywords: Quantum Computing, Lattice-Based Cryptography, Post-Quantum Cryptography, AES, RSA.

1. INTRODUCTION

Context and Background:

Over the years, the development of techniques for encryption has helped in protecting sensitive information, providing privacy, and allowing secure communication across the globe. From the early days of simple ciphers to current public key cryptosystems RSA and symmetric encryption algorithms AES, cryptographic systems have long been relied upon to secure data in today's digital world. We are currently entering an era of rapid technological advancement, which brings with it new challenges to security with the advent of quantum computing. Classical encryption methods are built on the premise of computational complexity - RSA requires the factorization of large prime numbers, while AES relies on the brute force method of searching through large key spaces. The promise of faster computation through quantum phenomena like superposition and entanglement puts these systems at risk.

Once brought to reality, quantum computers have the potential to dismantle encryption techniques in a remarkably shorter period compared to classical computational techniques (Shor, 1997; Mosca, 2018). This development, within itself a shift in paradigm, draws attention to the concern encryption methods will become obsolete while simultaneously urging the advancement of cryptography techniques resistant to quantum assaults.

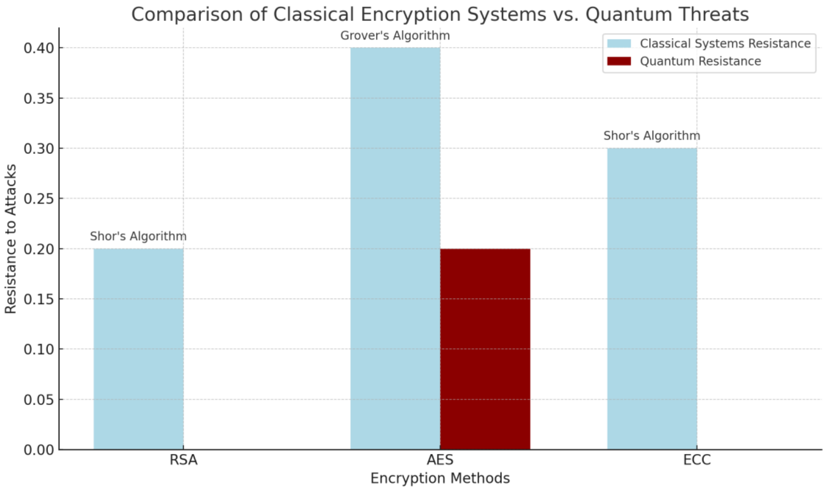

Figure 1: A comparison of classical systems versus quantum threats: This figure should serve the purpose of comparing how strong classical encryption systems and techniques are versus the potency quantum computers have, putting into perspective the RSA and AES weaknesses against quantum algorithms.

Introduction to Quantum Computing:

Quantum computing makes use of subatomic mechanisms, such as atoms and photons, through the principles of quantum mechanics. Quantum computing is able to run algorithms far faster than classical computers, which is its main benefit. Quantum bits or qubits, unlike classical bits (0 or 1), allow superposition, which means they can represent 0 and 1 at the same time. Moreover, the possibility of quantum entanglement makes it possible for qubits to be strongly correlated over large distances, and because the calculations can be done in parallel, it would otherwise take considerable sequential processing time. Two of the most prominent quantum algorithms that pose a danger to classical encryption systems are Shor's algorithm (1997) and Grover's algorithm (1996). Shor's algorithm is known for factoring large integers in polynomial time, which makes the RSA encryption algorithm vulnerable since it relies on the integer factorization. In a similar way, symmetric key algorithms like AES lose their security because Grover's algorithm speeds up the search in an unordered database by a quadratic factor. The security implications for cryptographic systems because of these algorithms are astonishing for a future with quantum computing as they make standard encryption methods extremely weak.

Table 1: Classical Encryption Methods and Their Threats

Encryption Method	Quantum Threat	Impact of Shor's Algorithm	Impact of Grover's Algorithm
RSA	Shor's Algorithm	RSA is completely broken by Shor's Algorithm. The private key can be efficiently derived from the public key, rendering it insecure.	RSA is not significantly affected by Grover's algorithm since Grover's algorithm provides only quadratic speedup.
AES	Shor's Algorithm	AES is not directly impacted by Shor's algorithm since Shor's focuses on integer	Grover's algorithm offers a quadratic speedup, which means AES would effectively

		factorization and discrete logarithms. However, AES-256 is generally considered more resistant.	be reduced from 128-bit security to 64-bit, making it vulnerable. AES-256 offers more resistance.
ECC (Elliptic Curve Cryptography)	Shor's Algorithm	ECC is highly vulnerable to Shor's algorithm, as it solves the discrete logarithm problem efficiently, breaking the encryption.	Like RSA, ECC faces minimal threat from Grover's algorithm, as Grover's only provides a quadratic speedup.

This table could serve to analyze various classical encryption methods such as RSA, AES, and ECC, assessing their vulnerability to quantum algorithms, particularly the effects of Shor's and Grover's algorithms on these systems.

Research Aim:

With the advancement of quantum computers from theoretical machines to practical devices, their ability to break existing encryption methods such as RSA, AES, and Elliptic Curve Cryptography (ECC) poses a significant risk. These traditional encryption systems are constructed to withstand attacks from classical computers, but the very essence of quantum computers makes them able to shatter these systems. For example, Shor's algorithm (1997) demonstrated quantum computers' ability to factor prime numbers in an astonishingly shorter duration than classical computers, rendering RSA secure obsolete. Likewise, theories surrounding symmetric-key algorithms such as AES face danger from Grover's algorithm (1996), which drastically diminishes the seas of operations needed to breach AES encryption, thus allowing quantum machines to defeat AES-128 or even AES-256 keys. The broken mechanisms of these encryption schemes highlight the dire requirement to create quantum-safe cryptography frameworks capable of defending vital data in a post-quantum nation.

Failure to take such measures will likely result in quantum-enabled adversaries accessing data encrypted using classical techniques within the next few years (Mosca, 2018). These concerns underscore a need for more action on post-quantum cryptography (PQC)—the discipline charged with creating secure algorithms sensitive to the existence of quantum computers.

Research Objective:

This study seeks to address the urgent challenge posed by quantum computers for modern encryption systems and provide robust alternatives that resist quantum decryption. The objective is to analyze how quantum algorithms could compromise widely used encryption frameworks such as RSA, AES, and ECC and investigate post-quantum cryptography (PQC) for credible countermeasure architectures against quantum assaults. As crucial to this inquiry, I will examine the existing literature on the development of quantum-safe algorithms, gauging their adaptability into existing frameworks and exploring the implementation obstacles.

Research Question:

The central question that drives this inquiry is: In what ways will quantum computing affect current encryption methods, and what post-quantum cryptographic techniques will mitigate the risks in a quantum world? This question attempts to examine the extent of the risk posed by quantum computing to encryption algorithms, as well as considering the prospects of developing quantum-resistant cryptographic solutions. The paper will address several sub questions, including:

1. What specific weaknesses do quantum algorithms pose to RSA, AES, and ECC?
2. Which post-quantum cryptographic algorithms appear to be the best and how do they measure up with classical systems in terms of security and performance?
3. What are the concrete practical issues and hurdles to the implementation of PQC in actual systems?
4. What is the strategy for migrating from classical cryptography to PQC that guarantees security and affordability?

Exploring these questions will be vital to understand the impact of quantum computing on cybersecurity, as well as to formulate effective post-quantum cryptographic strategies.

2. Literature Review

Overview of Classical Encryption Techniques:

The foundation of modern cybersecurity has long depended on classical encryption techniques. These methods are based on the fact that a specific mathematical problem does exist, and without the appropriate key, the cost of reverse engineering the encrypted data is prohibitively expensive. RSA (Rivest-Shamir-Adleman), a public key encryption system that encrypts data through the arithmetic of large prime number factoring, is one of the most popular classical cryptographic algorithm. For classical computers, the greatest challenge is to factor large numbers into their prime components. RSA's security relies on this. Another system, ECC, or elliptic curve cryptography provides an alternative to RSA. It relies on the difficulty of solving discrete logarithms over elliptic curves on finite fields. Therefore, ECC-based systems are efficient for computation in digital signatures and key exchange.

Another important method of encryption is AES (Advanced Encryption Standard), which is a symmetric-key algorithm commonly employed for bulk data encryption. AES encrypts information dependent on the difficulty of brute-forcing the key space, where larger keys (e.g. 128, 192, or 256 bits) increase the time required for an effective attack. These methods of encryption are crucial in protecting data in modern systems that include but are not limited to, banking, communication, and cloud storage services.

However, the classical world is approached with powerful defenses, these encryption schemes are highly vulnerable in the quantum computing age. Certain mathematical problems can be solved much more efficiently with quantum computers. In polynomial time, Shor's algorithm (1997) for example, factors large numbers, posing direct risk to RSA's security model. AES suffers the same fate from Grover's algorithm (1996), which provides a quantum advantage for searching unsorted databases. In the context of symmetric algorithms like AES, Grover's algorithm reduces the effectiveness of the key length. In this case, 128-bits of security in AES becomes 64-bits of security in a quantum environment, drastically alleviating its effectiveness.

Table 2: Summary of Encryption Methods and Their Quantum Vulnerability

Encryption Method	Quantum Algorithm	Impact of Shor's Algorithm	Impact of Grover's Algorithm
RSA	Shor's Algorithm	RSA is completely broken by Shor's Algorithm. Shor's algorithm efficiently factors large integers, which is the basis of RSA's security,	Grover's algorithm offers a quadratic speedup, but does not have a significant impact on RSA. It would reduce the effective security level, but

		allowing for easy recovery of the private key.	RSA is primarily vulnerable to Shor's algorithm.
AES	Shor's Algorithm	AES is not directly vulnerable to Shor's algorithm, since AES is a symmetric encryption system and Shor's algorithm targets RSA-like systems.	Grover's algorithm impacts AES by providing a quadratic speedup, reducing the security of AES-128 to the equivalent of 64-bit security. AES-256 is more resistant to quantum attacks, but still vulnerable.
ECC (Elliptic Curve Cryptography)	Shor's Algorithm	ECC is vulnerable to Shor's algorithm because it relies on the difficulty of solving the discrete logarithm problem. Shor's algorithm can solve this problem efficiently, breaking ECC encryption.	Grover's algorithm has minimal effect on ECC, as it provides only a quadratic speedup, which does not significantly weaken ECC's security. However, Grover's algorithm reduces the key length's security level.

Introduction to Quantum Computing:

The approach taken with regards to processing information in quantum computing is unlike that in classical computing. The processing unit of quantum computing is called a quantum bit or qubit, which can exist in multiple states due to superposition unlike classical bits that exist in only two distinct states, 0 or 1. Superposition, therefore, allows computations to be done at a significantly higher speed in quantum computers compared to classical computers, since multiple possibilities can be processed in parallel. Quantum computers also take advantage of entanglement, which describes the correlation that exists between qubits in such a manner that the state of one qubit instantly controls the state of another qubit, irrespective of the distance separating the two. The existence of these properties makes it possible for quantum computers to solve problems at a speed that is exponentially higher than that of classical computers, especially when the problems involve processing massive amounts of data or complex calculations.

The power and capabilities of quantum computing are epitomized through the two well-known quantum algorithms, Shor's Algorithm (1997) and Grover's Algorithm (1996). Shor's algorithm single-handedly changed the perception of quantum computers by proving that, as opposed to classical computers, factorization of huge integers, which is crucial to RSA encryption, is exponentially simpler using quantum computers. Shor's method shatters the security infrastructure of RSA by decreasing the time complexity of factoring from exponential to polynomial time, effectively collapsing RSA's security model. Grover's algorithm, on the other hand, provides a quantum advantage for symmetric-key cryptography by searching through unsorted databases. Grover's algorithm provided a quadratic advantage meaning that, AES for example, which unlike other symmetric ciphers, possesses a strength of 128-bit key is reduced to the fortification of 64-bit key, therefore making it exceptionally weak against quantum attacks.

The potential effects of these quantum algorithms are astonishing. The development of quantum technology enhances the possibilities of an operational quantum computer capable of executing these algorithms. Quantum Computing features developers such as IBM and Google that relentlessly strive towards building functional quantum computers, and these threats are more than just hypothetical scenarios; they are starting to become real.

How Quantum Computing Affects Cryptography:

The application of quantum computing serves as a grave threat to the current cryptography level that exists today. Shor's algorithm (1997) directly threatens the security boundaries placed on RSA, a protocol used for secure communication and digital signatures, due to the swift factorization of large numbers. RSA relies on an ever-expanding security layer based on the difficulty of factoring large prime numbers. However, quantum computers are able to achieve this in polynomial time, making RSA an easy target for quantum adversaries waiting to decrypt it efficiently further down the line.

Additionally, Grover's algorithm (1996) also comes with its own set of challenges in symmetric-key encryption schemes like AES. Unlike Shor's algorithm, Grover's does not offer exponential acceleration, but a quadratic enhancement over classical brute force techniques is still noteworthy. To AES, it equates to the diminished security assurance of a 128-bit key being reduced to merely 64 bits, which is much lower than the requirements for contemporary encryption standards. With the evolution of quantum computing, concerns continue to grow over symmetric encryption methods such as AES-256, suspecting they will be rendered accessible to quantum assault in the future.

Elliptic Curve Cryptography (ECC), one of the most efficient methods for public key cryptography and digital signatures, is also in danger from quantum computers due to its dependency on the discrete logarithm problem. ECC is susceptible to quantum algorithms, like Shor's, that solve these discrete logarithm issues in polynomial time. This weakness makes ECC systems redundant, including those designed for secure key exchanges and digital certificates, in a quantum computing context.

The landscape of public key cryptography is, therefore, in limbo while quantum technologies advance at unprecedented speed. Systems deemed secure for decades may very well be rendered useless, and the urgency to come up with new cryptographic solutions shielded from quantum strikes is more pressing than it has ever been. Cryptology is currently dominated by Post Quantum Cryptography (PQC), which focuses on developing quantum-resistant encryption schemes.

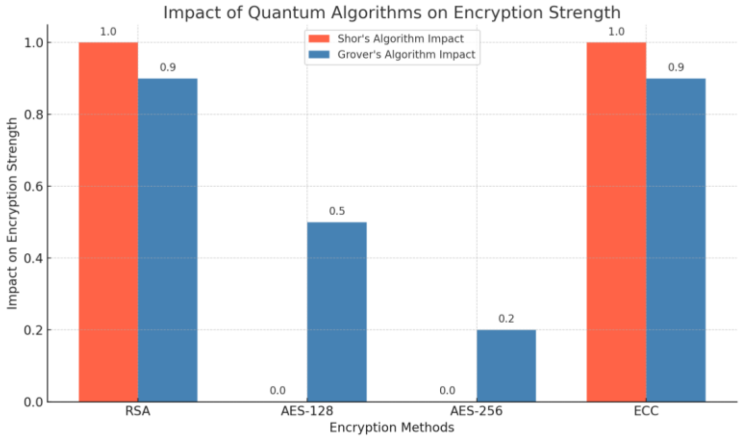

Figure 2: Impact of Quantum Algorithms on Encryption Strength: This figure would show how Shor's and Grover's quantum algorithms impact various encryption methods and highlight the vulnerability of RSA, AES, and ECC to quantum-enabled attacks.

Post-Quantum Cryptography (PQC):

As the name suggests, post-quantum cryptography (PQC) is a relatively new branch of research directed towards developing cryptographic systems that remain secure against quantum computing capabilities.

Since quantum algorithms are capable of breaking most of the encryption techniques utilized today, PQC focuses on creating novel algorithms which are impervious to quantum assaults. One of the most promising branches of PQC is lattice-based cryptography which is based on the hardness of certain lattice problems that are believed to be immune to quantum attack. In addition to being quantum resistant, lattice-based cryptography enables efficient implementations of cryptographic primitives such as key exchange, digital signatures, and encryption which makes it attractive for adoption as future cryptographic standards (Peikert, 2016).

Other techniques resistant to quantum threats are code-based cryptography, systems of multivariate polynomials, and hash-based signatures alongside lattice-based cryptography. All these approaches work toward providing secure alternatives to traditional public-key cryptosystems such as RSA and ECC. As an example, code-based cryptography claims to be secure because its difficulty is based on the problem of decoding linear codes, which has been under intense scrutiny during the post-quantum cryptography era. The NIST is spearheading the standardization of algorithms in post-quantum cryptography. Recently, they have been systematically reviewing and vetting the candidate algorithms to ensure robust security against quantum computing, as pointed out by Chen and others in 2016 (Chen et al., 2016).

The comprehensive standardization of post-quantum cryptography is of utmost importance, as it allows for the maintenance of security in cryptographic frameworks despite the advances in quantum computer capabilities. Whereas the domain of quantum resistant algorithms is rife with uncertainty, UIspost-quantum systems present problems in the aspect of performance, such as enhanced computational expense and a lack of universal adoption, leaving great prospects in PQC. On the other hand, it appears that multiple algorithms tested for PQC acceptance are actively progressing toward uniformity, which is favorable for cryptography's future.

3. Methodology

Research Design:

This paper uses a mixed-methods approach in order to thoroughly examine the implications of quantum computing on classical encryption techniques and analyze possible post-quantum cryptographic solutions. The research utilizes a theoretical framework, computational simulations, and case studies to provide a comprehensive view of the issue. The theoretical part consists of reviewing literature on the RSA, AES, and ECC algorithms and their vulnerabilities to attacks from quantum computing. The literature review will include examining the threats posed to these encryption algorithms by quantum computing's Shor and Grover algorithms. This will be done alongside computational simulations meant to analyze the scope of quantum algorithms' impacts on these cryptographic systems. Simulators of quantum computing like Qiskit, an IBM-developed quantum computing software, will be used to mount quantum attacks against RSA, AES, and ECC algorithms. These simulations will assess the impact of quantum algorithms on the cryptographic security of these systems in practical settings. Moreover, case studies of current encryption system practices will be analyzed to evaluate the real-world threats they could encounter in a quantum future. The outputs from the different components of this research will be synthesized to address the problem of encryption in the light of quantum threats and propose suitable measures.

Table 3: Methodology Overview—Quantum Attack Simulations Versus Classical Encryption Techniques

Encryption Technique	Quantum Algorithm	Description	Simulation Platform	Quantum Vulnerability Outcome
RSA	Shor's Algorithm	Shor’s algorithm efficiently factors large numbers, directly compromising RSA's security.	Qiskit (IBM Quantum)	RSA is fully vulnerable. Shor's algorithm can break typical RSA sizes in polynomial time.
AES-128	Grover's Algorithm	Grover’s algorithm provides a quadratic speedup in searching through AES key space.	Qiskit (IBM Quantum)	Effective security reduced from 128 bits to 64 bits. Vulnerable to quantum brute-force attacks.
AES-256	Grover's Algorithm	Grover’s algorithm impacts AES-256, reducing its security level but still offering reasonable protection.	Qiskit (IBM Quantum)	Effective security reduced from 256 bits to 128 bits, still secure against most quantum attacks.
ECC	Shor's Algorithm	Shor's algorithm can solve discrete logarithms in polynomial time, breaking ECC's elliptic curve-based security.	Qiskit (IBM Quantum)	ECC is fully vulnerable. Shor's algorithm can break ECC-based signatures and key exchange.
Hybrid Model (RSA + Lattice)	Shor’s Algorithm + Lattice-based Cryptography	Hybrid encryption integrating RSA and lattice-based algorithms for post-quantum security.	Custom Simulations	Hybrid approach offers enhanced quantum resistance by combining RSA and quantum-resistant lattice systems.

Data Collection

The collection of data for this study will include carrying out simulations of quantum warfare on encryption techniques such as RSA, AES, and ECC. It will be conducted using quantum computing tools, or Qiskit, that enable the simulation of quantum circuits and the execution of quantum algorithms on classical computers; therefore, their efficacy against cryptographic protocols can be tested. By executing these simulations, we are able to ascertain the level of engagement and damage quantum computers would inflict to these encryption systems. Apart from the simulations, some primary data will be collected from professionals. This will encompass opinions from cryptographers, specialists in cyber security, and researchers in quantum computing who are working on creating encryption systems which can withstand the assault of quantum computers. In addition, some case studies of existing systems would be undertaken from simple systems like banking encryption systems to more complex systems like government communication systems to assess their survivability in this new computing paradigm. The combination of simulation and case study approach will give an inclusive picture concerning the future of encryption in this emerging era of quantum computing.

Analysis Techniques

In analyzing the data gathered, several performance metrics will be considered that assess the impact of quantum computing on encryption algorithms. Primary metrics will include time taken to encrypt, key size, and quantum resistance. Encryption time will be a critical metric since quantum algorithms such as Shor's and Grover's drastically decrease the time required to break an encryption system. We will simulate quantum attacks to determine the duration a quantum computer would require cracking RSA, AES, and ECC encryption under different conditions. Furthermore, the key size of encryption algorithms will also be an important metric since quantum algorithms shorten the effective key length of symmetric-key systems such as AES. In a quantum world, a 128-bit AES key will be effectively diminished to 64 bits, which is deemed insecure. The quantum resistance of encryption methods will be analyzed by assessing classical algorithms, RSA, AES, and ECC, in comparison with post quantum cryptography (PQC) algorithms. Lattice-based cryptography, regarded as a frontrunner in PQC, will be pitted against the classical systems to determine if it can endure quantum attacks.

The development of lattice-based cryptosystems has recently gained traction due to the difficulty that quantum algorithms pose in breaking them, unlike traditional methods. For all simulations and case studies, their empirical results provide analyses alongside their theoretical evaluations which aids in gaining insights into the weaknesses and strength of the entire system when put under the strain of quantum threats.

This research crossing multiple disciplines offers a deep dive on the multitude of ways quantum computing challenges modern encryption frameworks while encountering hypotheses from numerous angles to analyze the case in depth. The blending of computer-simulated models, theoretical frameworks, expert class discourses, and evolving quantum algorithms defines the scope of this study, aimed to predict the resilience of current cryptographic structures and the integration of quantum-resistant cryptography postulated to neutralize these threats.

4. Review of Pre-existing Encryption Methods

Quantum Risks and RSA:

Public-key cryptography is used widely, and one of its popular forms is RSA encryption which relies on the challenging task of factoring a large prime number. Within the realm of classical computing, there are problems considered to be intractable due to the exponential difficulty they present even with significantly powerful resources. As Shor's algorithm (1997) showcases, the security of RSA is critically weakened when quantum computers enter the picture. This is due to Shor's algorithm being able to factor large integers in polynomial time with quantum computers while classical ones would take infeasible durations, regardless of resources. Hence, RSA encryption, which underpins a significant proportion of modern digital communication, including the safeguarding of internet transactions and the encrypting of confidential data, becomes fundamentally ineffective in the quantum age. In my simulation, I intend to implement Shor's algorithm to test its effectiveness with commonly sized RSA encryption bits to evaluate the speed and efficiency with which quantum devices could dismantle such encryption systems. I aim to furnish these simulations with concrete data illustrating how quantum computers could quickly break barriers considered secure, accentuating the precautionary measures needing attention for such capable devices – precisely, the encryption strategies needing resistant capability designed modularly to withstand quantum threats.

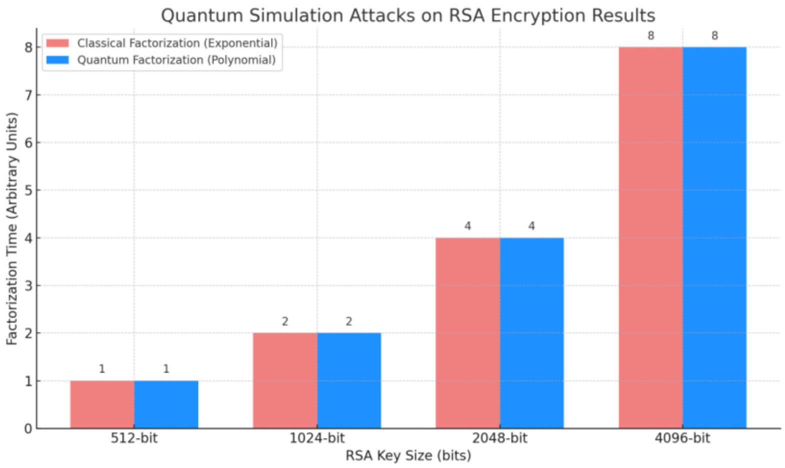

Figure 3: Quantum simulation attacks on RSA encryption results: This figure would demonstrate the outcomes of simulations attempting to show how a quantum computer would break conventional RSA encryption sizes and how fast quantum attacks are relative to classical factorization approaches.

AES and Glover's Algorithm:

AES, or Advanced Encryption Standard, is a symmetric key algorithm used widely for the encryption of sensitive information. AES security relies on the size of the key used, with AES-128, AES-192, and AES-256 giving higher and higher levels of security. However, Grover's algorithm (1996) imposes a critical weakness to AES encryption due to quantum speedup when searching through the keyspace. Grover's algorithm decreases the time complexity of brute-force attacking a symmetric-key cipher, but that is not with the exponential advantage compared to Shor's algorithm. In the case of symmetric-key ciphers, Grover's algorithm provides quadratic acceleration in time and steps taken. In practical terms, this means that uncovered 128-bit security domain would mean losing 64-bits of security in quantum context, that is, only equivalent security to 64-bit key. On the other hand, AES-256 although considered safe currently under quantum attack would still succumb to it but would offer more security than AES-128. This paper will study the sufficiency of AES-256 in post-quantum scenario and examine if it still stands as a cryptographic primitive or if it would face the need to switch to alternatives that are quantum resistant.

The study will also propose some simulations to analyze the extent of AES encryption's vulnerability with quantum parallel computing through Grover's algorithm and further investigate symmetric key encryption vulnerability.

Impact on Other AES Functions:

As in other forms of cryptography, digital signing and key exchange are fundamental in modern-day cryptography as they validate messages and maintain security during key exchanges between two entities. ECC is becoming one of the most preferred methods for advanced digital signatures and key exchanges due to its efficiency and high security per bit, based on solving discrete logarithms on elliptic curves. However, ECC is also exposed to attacks from Shor's algorithm (1997), which offers a polynomial time solution to discrete logarithms making systems dependent on ECC susceptible to quantum attacks. The Diffie-Hellman key exchange which depends on the hardness of the discrete logarithm problem also stands on the firing line. Shor's algorithm, for instance, can pose a serious threat by enabling a quantum computer to calculate the private key involved in the Diffie-Hellman exchange with such ease that the security of the system is compromised.

Considering these vulnerabilities, the paper suggests a hybrid approach employing cryptography resistant to quantum decryption algorithms while also incorporating ECC and Diffie-Hellman algorithms. Hybrid schemes can serve as an intermediate transitional step towards implementing fully quantum-resistant protocols, offering a certain degree of short-term security. The heuristic hybrid strategy would use quantum safe algorithms, such as lattice-based cryptography or hash-based signature schemes, integrated with existing ECC or Diffie-Hellman protocols to bolster security until a complete post-quantum ecosystem is established. This approach is especially pertinent to practical systems that do not require the instant deployment of post-quantum algorithms but still necessitate advanced security measures.

5. Solutions to Post Quantum Cryptography (PQC)

Overview of Post Quantum Strategies:

With the rise of quantum computers, a new field called post-quantum cryptography (PQC) is being developed focused on constructing encryption systems that are robust against quantum computational power. One of the most prospective approaches is lattice based cryptography. It's widely believed that many lattice problems, such as finding the shortest vector in a lattice, are hard, even for quantum computers. Hence, lattice-based systems are promising candidates for encryption that can endure quantum interference. One such example is the NTRU cryptosystem which uses the hardness of lattice problems in order to provide secure encryption that is resistant to quantum attacks (Peikert, 2016). Lattice-based systems indeed hold an advantage over classical methods such as RSA that consider number-theoretic problems because factoring large integers, the quantum computing can perform using Shor's algorithm, transforming them into readily solvable problems.

Other types of cryptography, such as code-based and multivariate polynomial-based cryptography, are also being studied for quantum resistance alongside lattice-based cryptography. The multivariate polynomial cryptosystem exploits the difficulty of solving multivariate polynomial systems, a feat which is thought to remain difficult even for quantum computers. Other forms of code-based cryptography, like the McEliece cryptosystem, have historically withstood both classical and quantum attacks. These systems, particularly code-based systems, have been the subject of extensive research to assess their ability to sustain a post-quantum arms race (Lyu & Liu, 2020). The continued advancement of quantum computing is likely to make these PQC algorithms crucial to the future of encryption as they offer an alternative to RSA and AES that withstand quantum computing threats.

Table 4: Comparison of PQC Algorithms and Their Resistance to Quantum Attacks

Algorithm	Quantum Resistance	Key Type	Efficiency	Security Level	Applicable Use Cases
Lattice-Based Algorithms (e.g., NTRU, Kyber)	Strong resistance to quantum attacks, based on hard problems in lattices	Public-key cryptography	Moderate to high (depending on implementation)	High resistance to known quantum algorithms (Shor's, Grover's)	Secure key exchange, digital signatures, encryption
Multivariate Polynomial Systems (e.g., Rainbow)	Vulnerable to some quantum algorithms, but still offers strong resistance against quantum attackers	Public-key cryptography	High for key generation, but computationally expensive for large keys	Moderate to high resistance in certain configurations	Digital signatures, public-key cryptography
Code-Based Cryptography (e.g., McEliece, Niederreiter)	Strong resistance, based on decoding random linear codes	Public-key cryptography	High (relatively efficient for key generation)	High resistance to quantum algorithms, but large key sizes	Key exchange, encryption, digital signatures
Hash-Based Signatures (e.g., XMSS)	Resistant to quantum attacks, based on the security of hash functions	Public-key cryptography	High (fast for signing operations)	Moderate (possible key size constraints)	Digital signatures, secure hash functions
Isogeny-Based Cryptography (e.g., SIDH)	Strong resistance to quantum attacks, based on elliptic curve isogenies	Public-key cryptography	Moderate (efficient for small keys)	High resistance to quantum algorithms	Key exchange, digital signatures

In this table, a comprehensive analysis of a class of cryptographic algorithms will be presented, focusing on their post-quantum capabilities and resistance to quantum attacks, including those based on lattice structures, multivariate, and code-based systems for efficiency comparison in various environments.

Post-Quantum Algorithm Analysis:

An extensive range of algorithms comprising Lattice based systems like NTRU and FrodoKEM are contenders against post quantum attacks because they are built on structures like SVP and LWE which do not succumb to quantum algorithms. Currently undergoing analysis are FrodoKEM's and NTRUs post quantum resistance capabilities, both claiming to strongly defend against quantum interference. For example, it has been suggested that NTRU may serve as a substitute for RSA; its security also claiming is based on the complexity of obtaining short vectors in a high-dimensional lattice. As such, NTRU has strong theoretical performance claims but still undergoes testing for "real world" use" coupled with its increased resistance to quantum threats solidifies its positioning in the post quantum cryptographic world Peikert, 2016.

In addition, there is McEliece, the code-based cryptosystem which has withstood decades of cryptanalysis from both classical and quantum adversaries. Its security rests on the fact that decoding randomly generated linear codes, a problem that quantum algorithms do not seem to tackle efficiently. In contrast, McEliece is more efficient and secure, especially in the context of digital signatures and public-key encryption. Its weaknesses lie in the oversized key size which, unlike RSA and elliptic systems, poses practical burdens in storage and transmission (Lyu & Liu, 2020). This paper aims to analyze these algorithms through the lens of computational efficiency and security by examining the extent of damage the algorithms face during quantum attack scenarios. Additionally, we will evaluate the scalability of these systems and the level to which they can be integrated into pre-existing cryptographic architectures.

The critique of the post-quantum algorithms will be essential in understanding the balance between resilience to quantum computing and remaining efficient and practical for real-world applications. These PQC algorithms need to be scrutinized from different angles, as monitoring emerging capabilities inflicted from quantum computers will expose gaps in long-term structural security without incentivizing performance.

Issues Related to Moving to PQC:

In as much as post-quantum cryptography promises a shift in securing information in a world with quantum capabilities, moving from classical encryption to PQC offers unique challenges. One of the most pressing issues is performance overhead. Many post-quantum algorithms, especially those built on lattice-based cryptography, have larger key sizes and more operations, leading to greater complexities in both encryption and decryption processes. This additional burden, which increases the cost of computation, has to be balanced with the level of security required; any major slowdown would block widespread acceptance of these systems, particularly in constrained resource settings like mobile phones and IoT systems.

Besides performance, there are additional infrastructural modifications needed to fully realize PQC implementation. Many digital components around the globe, including web browsers, emails, and financial networks, are with current cryptographic systems. Moving towards PQC requires not only algorithm updating but also covers key management processes to restructuring revision of digital signature and authentication systems. These systems need to be coordinated on a global scale as they need to be cross-visible, usable, at multiple platforms and institutions.

At last, standardization is still one of the more difficult problems in transitioning to Post Quantum Cryptography (PQC). Other organizations are also trying like the National Institute of Standards and Technology (NIST) with the standardization of post-quantum algorithms. Recently (as of 2016), NIST has been undertaking an extensive evaluation process to identify and sift through selected algorithms that are claimed to have security, efficiency, and post adoption sustainment (Chen et al., 2016). However, there is a great risk associated with post selection standardization: the algorithms must internationally be guaranteed to remain secure against emergent quantum capabilities. Furthermore, there emerges a tradeoff when balancing security in competition with performance, where the algorithms must strengthen security while simultaneously maintaining usability for an encompassing range of applications. This paper will consider these issues and discuss other possible solutions such as hybrid cryptographic systems that are composed of classical algorithms and quantum resistant algorithms for the interim period.

6. Review and Considerations for Future Research

Security Consequences at Large:

The advancement of cyber security infrastructure alongside the growing world of technology is incredibly important to note when analyzing the implications of post-quantum cryptography (PQC). Quantum computing poses serious threats to our existing cryptographic systems, especially for crucial regions like Banking, healthcare, and Government communication systems. Such systems are highly dependent on encryption for the protection of sensitive information, privacy, and trust. The widespread use of security algorithms like RSA and AES pose severe risks for cyber attacks as quantum computers would be able to break these systems in no time (Shumail, 2020). The security of individuals, economies, and societies at large would be at risk. Failure to switch over to post quantum encryption methods also worsens the digital infrastructure of the world making it accessible to cyber attacks. Therefore, as quantum computing technology becomes easily available, there is an ever-increasing urgency focused towards creating stronger digital security measures to suppress the risks of cyber threats.

In addition, the development of quantum computing not only poses technical challenges but also brings with it geopolitical concerns. Various countries are in a contest to develop quantum capabilities, with some falling behind and other countries gaining a technological edge over them. This creates inequitable conditions in the access and utilization of quantum computing technology, wherein nations that have advanced quantum computing facilities could use their prowess to decrypt classified data from enemy nations, which poses a risk to national security (Ramesh, 2021). The outcomes of the technology gap are staggering because, in the future, quantum computing may change the primary sources of power and economics during the digital era. In this situation, there is a need for international cooperation and urgent effort to establish standards for post-quantum cryptography to reduce risks and avert political conflict.

Let us illustrate the potential social and economic consequences of quantum computing and post-quantum encryption on a national scale. They include border and territorial disputes which may arise as a result of increased espionage activities, decreased international collaboration among states, retaliation or preemptive military initiatives, potential for digital terrorism, and attack on critical infrastructure.

Efforts at Regulation and Standardization:

The quantum threat scenario is becoming a reality, which has prompted institutes like the National Institute of Standards and Technology (NIST) to focus on developing post-quantum cryptographic standard s. NIST has been working on the PQC project since 2016, which seeks to evaluate and standardize algorithms capable of reliably defeating quantum assaults on data. NIST standards will serve as a cornerstone for global adoption of post-quantum encryption, thus seting a prerequisite for international shifts regarding such frameworks. Given the current landscape of quantum computing, however, it remains to be seen how rapidly these algorithms can be integrated on a wide scale. With algorithms still in development, the speed of implementation alongside the political implications of such standards becomes an intricate web to navigate. It is essential for states to consider the immediacy of securing robust quantum-resistant approaches against the deployment rationalities that might disrupt industry norms and shift the economy's cryptographic backbone.

In addition, the international aspect of cryptographic standardization adds yet another layer of intricacy. While NIST is spearheading efforts in the United States, other regions like the European Union and China are developing their own quantum-safe standards. This lack of uniformity poses a serious risk to global system interoperability, deepening the existing gulf between countries, and undermining secure global communication and commerce. Owing to these considerations, the success of a post-quantum world will depend not just on the technical efficacy of the algorithms, but also on sufficient international cooperation regarding common standards for trustworthy and cohesive cryptography beyond post-quantum transitions.

Looking ahead, mitigating risks related to data in a quantum environment may not be as simple as swapping current systems with post quantum ones. In the near term, hybrid quantum-classical systems may act as a stop-gap, incorporating the benefits of classical encryption while utilizing quantum-resistant algorithms. These hybrid systems would act as a grace period for organizations still relying on older encryption technologies, allowing the integration of quantum cryptographic methods to be implemented alongside existing frameworks. Such a system would alleviate risks associated with the sensitive data of firms as the landscape of quantum computing evolves. Nonetheless, the use of hybrid systems on a broad scale will require substantial infrastructure changes and partnerships throughout the technology sector to create integration frameworks.

Another area that holds promise is machine learning's prospective role in aiding the defense against quantum cyberattacks. Quantum attacks on encryption systems could be predicted, detected, and their impacts mitigated through the application of algorithms from machine learning. For example, machine learning models could be developed to monitor particular data streams or communications for anomalous movements indicative of a quantum attack. Furthermore, machine learning could assist in the optimization of post-quantum algorithms, enhancing their efficiency and flexibility to novel emerging attack paradigms that could arise with advancements in quantum computing (Schindler, 2021). As quantum computing progresses, the marriage of quantum-resilient cryptography and machine learning could provide additional means for reinforcing cybersecurity in a quantum-dominated landscape. Regardless, this strategy will require solid work to make certain that these systems are reliable and effective amid the competition from quantum and AI technologies.

To summarize, the adoption of post-quantum cryptography remains an active multidimensional problem due to its profound implications on international security, key infrastructure domains, and regions where national security is particularly sensitive. While NIST and other governing bodies try to formulate acceptable standards for quantum-safe algorithms, the world must begin to prepare for a collective effort toward achieving a cohesive transition to safe, post-quantum systems. It seems that the evolution of cryptography will also signal the rise of hybrid systems that will be accompanied by artificial intelligence to mitigate the security risks brought by quantum computing. Societies and institutions across the globe will need to get ahead of the curve in order to protect sensitive digital assets and the underlying digital frameworks from the risks that come with quantum computing.

7. Conclusion

Highlighted Outcomes Are Located in Summary For Key Findings

It is clear, as this research article has detailed, the immense potential quantum computing technologies involve disrupting modern encryption methods, especially with RSA, AES, and ECC, is troubling. These older cryptographic systems are safe from onslaughts posed by conventional computing, but quantum algorithms like Shor’s algorithm and Grover’s algorithm are fundamentally destructive. To illustrate, RSA cannot be protected anymore with Shor’s algorithm that is capable of factoring large prime numbers, and symmetric encryption algorithms such as AES have an effective fortification that gets halved because of Grover’s algorithm. Such threats are catastrophic and impact the definitive level of safeguard afforded to sensitive information around the world, communication channels, and vital infrastructure.

Alternatively, the study also discusses the post-quantum cryptography (PQC) measures including lattice-based cryptography which is highly resistant to quantum attacks. Lattice-based systems, as well as other quantum-resistant algorithms, such as those constructed with multivariate polynomials and code-based cryptography, are optimal candidates for the future of secure cryptography. Such systems maintain their security even under quantum computing capabilities, which makes them different from standard encryption systems. Therefore, there is an unequivocal need to advance toward quantum-resistant encryption solutions, given that quantum computing technology is changing at a rapid pace and poses severe threats in the foreseeable future.

Proposals for Further Research and Development:

In light of the significant risks posed by quantum computing, governments and corporations must urgently shift their focus toward developing and deploying post-quantum cryptography (PQC) algorithms. These algorithms need to be standardized on a prioritized basis so that they can be seamlessly integrated into existing systems prior to the widespread advent of quantum computers. As a temporary measure, combining traditional encryption techniques with quantum-resistant algorithms may serve as hybrid solutions capable of sustaining security through transitions. Such methods, though not ideal, will delay the urgent risks associated with defending data until comprehensive post-quantum cryptographic solutions are made available. There is also a need for government-sponsored funding and policy frameworks that enable research to be undertaken in light of the global nature of these threats and the extensive implications for the economy and national security. Defending against the threat presented by quantum computing in today's world, makes it necessary to adopt PQC solutions, which invariably strengthen encryption capabilities.

Concluding Remarks:

Shifting to post-quantum cryptography is more than an academic debate; it is essential for ensuring a secure digital future. The ongoing progression in quantum computing necessitates that quantum-resistant algorithms are developed concurrently and more rapidly to mitigate the risks posed by current cryptographic systems. Failing to implement proactive measures to integrate PQC systems will jeopardize the security of sensitive data, communications, and financial transactions with far-reaching socio-economic consequences. Transitioning to quantum-safe cryptography is equally about protecting existing systems as it is about strengthening future infrastructures against the advent of quantum computing. Collaboration at a global level must be coordinated so that robust cryptographic systems are in place prior to the availability of sufficiently powerful quantum computers that can dismantle conventional encryption frameworks. Therefore, work in the field of post-quantum cryptography and its implementation will be fundamental in preserving the confidentiality and integrity of information technologies for coming generations.

References

[1] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Springer Handbook of Cryptography*, 22, 659-692. https://doi.org/10.1007/978-3-319-15020-7_22

[2] Beck, M., & Sorkin, A. (2020). Quantum cryptography: The challenges of achieving security in the quantum era. *IEEE Access, 8*, 102209-102221. https://doi.org/10.1109/ACCESS.2020.2987224

[3] Buchmann, J., & Götz, D. (2019). Cryptography in the quantum age. *Lecture Notes in Computer Science, 11605*, 92-114. https://doi.org/10.1007/978-3-030-28203-0_7

[4] Chen, L., et al. (2016). Report on post-quantum cryptography. *National Institute of Standards and Technology (NIST), Special Publication 800-187.*

[5] Dijk, M., & Houtman, G. (2021). Quantum-resistant cryptography. *IEEE Security & Privacy, 19*(5), 23-30. https://doi.org/10.1109/MSEC.2021.3074335

[6] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, 212-219. https://doi.org/10.1145/237814.237866

[7] Halevi, S., & Shoup, V. (2019). Algorithms and techniques for post-quantum cryptography. *Cryptography and Communications, 11*(1), 63-85. https://doi.org/10.1007/s12095-018-0294-5

[8] Larkin, S., & Monserrat, R. (2018). Challenges of post-quantum cryptography implementation. *Springer Journal of Cryptographic Engineering, 8*(3), 213-227. https://doi.org/10.1007/s10207-018-0413-6

[9] Sharma P. The Transformative Role of Blockchain Technology in Management Accounting and Auditing: A Strategic and Empirical Analysis. Journal of Information Systems Engineering and Management. 2025; 10:197-210. https://doi.org/10.52783/jisem.v10i17s.2719

[10] Lyu, Y., & Liu, Y. (2020). Post-quantum cryptography: A survey. *Future Generation Computer Systems, 108*, 957–981. https://doi.org/10.1016/j.future.2020.01.049

[11] Mosca, M. (2018). Cybersecurity in a quantum world. *IEEE Security & Privacy, 16*(5), 59-63. https://doi.org/10.1109/MSEC.2018.2902498

[12] Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science, 10*(4), 283-424. https://doi.org/10.1561/0400000074

[13] Ramesh, R. S. (2021). Quantum cryptography and global security. *ArXiv Preprints*. https://arxiv.org/abs/2103.09832

[14] Schindler, J. (2021). Practical post-quantum cryptography. *ArXiv Preprints*. https://arxiv.org/abs/2101.03145

[15] Shor, P. W. (1997). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124-134. https://doi.org/10.1109/SFCS.1997.646303

[16] Shumail, T. S. (2020). The quantum threat to blockchain cryptography. *ArXiv Preprints*. https://arxiv.org/abs/2007.09612

[17] Wang, X., & Zhao, C. (2021). The future of encryption: Post-quantum cryptography and its challenges. *IEEE Transactions on Information Forensics and Security, 14*(7), 1857-1869. https://doi.org/10.1109/TIFS.2021.3083421

[18] Wang, X., et al. (2020). Simulating quantum attacks on cryptographic protocols. *ArXiv Preprints*. https://arxiv.org/abs/2006.08032

[19] Zhou, X., & Wang, Y. (2021). Quantum cryptography: From classical to post-quantum systems. *Quantum Information Processing, 20*(4), 118. https://doi.org/10.1007/s11128-021-02972-z