American Journal of Computer Science and Technology
2024, Vol. 7, No. 4, pp. 139-155
https://doi.org/10.11648/j.ajcst.20240704.12

Research Article

Exploring AES Encryption Implementation Through Quantum Computing Techniques

Adam Gorine*, Muhammad Suhaib

School of Computing and Creative Technology, University of the West of England, Bristol, UK

Abstract

A coming great revolution in technology is quantum computing, which opens new attacks on most of the developed cryptographic algorithms, including AES. These emerging quantum capabilities risk weakening cryptographic techniques, which safeguard a vast amount of data across the globe. This research uses Grover's algorithm to explore the vulnerabilities of the Advanced Encryption Standard to quantum attacks. By implementing quantum cryptographic algorithms and Quantum Error Correction on simulators and quantum hardware, the study evaluates the effectiveness of these techniques in mitigating noise and improving the reliability of quantum computations. The study shows that while AES is theoretically at risk due to Grover's algorithm, which demonstrates a theoretical reduction in AES key search complexity, current hardware limitations and noise levels encountered in today's quantum computers reduce the immediate threat and limit practical exploitation. The research also examines NTRU encryption, a quantum-resistant alternative, highlighting its robustness in quantum environments. The findings emphasize the need for further development in QEC and quantum-resistant cryptography to secure digital communications against future quantum threats. Future work will focus on advancing QEC techniques and refining quantum algorithms, addressing both hardware and theoretical advancements, including the potential use of high-capacity processors like Jiuzhang 3.0. These improvements will ensure the scalability of quantum-resistant systems to practical key sizes and usage scenarios.

Keywords

Quantum Computing, Post-Quantum Cryptography, Cryptographic Vulnerabilities, Advanced Encryption Standard, Graph Theory, Cryptographic Migration, Quantum Resistance

1. Introduction

Quantum computing marks a new era in computational technology with markedly unique advantages and risks, more apparent in security. Computationally, quantum computers have the potential to do complex computations at a far superior speed to classical computers. So, classical cryptographic systems like AES (Advanced Encryption Standard) are progressively becoming incompetent [1]. Quantum technology is rapidly moving forward, and it turns out that modern cryptographic methods used to protect data worldwide are helpless against it. Moving closer to the quantum era, the flaws in traditional cryptographic systems like AES become visible. There are, therefore, significant demands for quantum-resistant cryptography because quantum computing threatens to crack data that is encrypted by classical means. With this comes the need to start embracing innovations of post-quantum cryptography (PQC) that can counterbalance

*Corresponding author: adam.gorine@uwe.ac.uk (Adam Gorine)

Received: 30 August 2024; **Accepted:** 26 September 2024; **Published:** 18 October 2024

the robust results provided by quantum machines [2]. The move to these new cryptographic protections cannot be described as a mere precaution; they are inevitable measures required to protect digital data in the forthcoming age of quantum computing.

This research will be more specific in exploring the usability of implementing quantum cryptographic algorithms and evaluating error correction mechanisms within the IBM Quantum. These approaches propose a way to minimize the effects of quantum noise, a problem of great importance in the reliability of quantum computations. Unlike theoretical implementations of quantum computing, this work offers real experience. It explicitly provides working examples of some of the algorithms incorporated within this work, including the AES S-box and NTRU encryption with QEC, to better address quantum-induced errors.

The practical part of the study was performed using tools like Python, Qiskit, and Microsoft Visual Studio Code in a safely closed environment to prevent any random interference with the script. We also conducted the experiments in many cycles to ensure optimal performance of the quantum circuits. These experiments are essential in determining when the present quantum technology is insufficient and identifying the effectiveness of error correction procedures.

Contribution

The main objective of this study is to assess the security of AES and NTRU encryption algorithms against the new challenges brought by quantum computing algorithms. This study also seeks to evaluate the efficiency of various QEC techniques in eradicating quantum noise, to ensure credibility of quantum computations.

1) Simulators and IBM Quantum hardware will also run quantum transformations of AES S-box and NTRU encryption algorithms.
2) Assess implementations with quantum noise and use QEC to correct these errors.
3) Decompose the given cryptosystem, look at its error rates, circuit depth, and execution speed, and discuss practical issues of quantum cryptography.
4) Future work includes work oriented toward enhancing QEC techniques and more work should be done on other quantum-resistant cryptographic algorithms, such as NTRU.

2. Literature Review

2.1. Quantum Computing

Quantum computing is the shift in computer computations and has had a major influence on cryptography. It offers some fascinating prospects for today's cryptography procedures used to protect digital messages and information, but it also has numerous associated vital issues. The research has provided a systematic approach to upgrading cryptographic systems that are in the threat range of quantum attacks and facilitating enterprises to manage the quantum risks in their cryptographic assets [3]. The framework also presents an inventory of cryptographic systems and performs the analysis of security dependencies during a strategic migration resulting in the form of a structural plan. A study of the impact of quantum computing on DERs, quantum threats and risks, and countermeasures such as QKD and PQC. It anticipates quantum attacks and evaluates defence strategies; it introduced a novel architecture that incorporates PQC and QKD for DERs, in addition to considering factors such as delay and cost of the network [4]. From the published work of [5], it is possible to get an understanding of the QKD systems, including such protocols as BB84, general information about quantum communication, and its impact on the traditional PKC. Its areas of interest are related to practical questions of application and the effects of quantum technologies on security infrastructure. In [6], they incorporate quantum computing in other areas of finance risk management by putting forward a quantum algorithm that better enhances the risk assessment measures such as VaR and CVaR with higher convergence rates in the models of finance.

Quantum computing has had a profound impact on classical cryptographic methods, particularly symmetric encryption algorithms like AES. Grover's algorithm, a quantum search algorithm, poses a serious threat to these encryption systems by reducing the complexity of brute-force key searches from O(N) to O(√N). This has raised significant concerns about the future of data security in the post-quantum era [8] Recent studies have begun focusing on the development of quantum-resistant encryption methods, often referred to as post-quantum cryptography (PQC), to counter these risks. These methods include lattice-based cryptography, such as NTRU, and hash-based cryptography, both of which are resistant to Grover's algorithm due to their complexity and computational demands [22].

2.2. Vulnerabilities of AES

Quantum technology poses a significant threat to digital security, particularly in algorithms like the Advanced Encryption Standard (AES), which is crucial for securing digital communications. They are Shor's and Grover's algorithms that destabilize the principles of classical security models and cause debates on further perspectives on developing cryptographic methods [7, 8]. In the review done by [1], the effects of quantum computing on classical cryptographic systems were explored, and the performance of post-quantum modes of cryptography was assessed. Its study employs SWOT to analyse the strengths and weaknesses of traditional cryptographic algorithms such as AES, RSA, and ECC, given quantum developments. Is it time to move to QRAs, which are quantum-resistant? The research reveals the electromagnetic spectrum vulnerabilities posed by quantum computing. The study in [9], reviewed the impacts of quantum computing on software security and reliability, with an extreme focus on the

reinforcement of symmetrical cryptographic techniques against quantum attacks. To rank and prioritize the software security scenarios, they used the fuzzy analytic hierarchy process (FAHP) and the fuzzy technique for order preference by similarity to the ideal solution (FTOPSIS). These demonstrated the risks for existing cryptosystems and the need for new post-quantum approaches. The research by [10], gave a postmodern critique of the influence of quantum computing on blockchain security, which depends on public-key cryptosystems and hash functions exposed to quantum assaults such as Shor's algorithm. As their literature review outlines, there is ample prior art in the cross-section of blockchain and quantum computing.

The Advanced Encryption Standard (AES) is highly vulnerable to quantum attacks due to the computational advantage provided by Grover's algorithm. Grover's algorithm can significantly reduce the time required to break AES by halving the search space for cryptographic keys, thus undermining the security of digital communications. Given these vulnerabilities, quantum-resistant alternatives must be evaluated and developed to safeguard against these threats [8] In addition to Shor's algorithm, which threatens public-key cryptography, Grover's algorithm has a profound impact on symmetrical cryptographic systems, thus driving the need for further research into quantum-safe encryption techniques. This review highlights the growing concern over classical encryption systems and discusses post-quantum cryptographic alternatives that resist these threats [22].

2.3. Evolution of Post-Quantum Cryptography

The development of PQC has been necessitated by the search for encryption techniques that are immune to attacks by quantum computers as far as safeguarding digital communication and data is concerned. This study [11], exclusively elaborates on PQC algorithms for IoT devices in the context of post-modern threats from quantum computing. An analysis is made of the time coincidence and strength of different cryptographic algorithms in terms of correlation with the Internet of Things, considering the limited computational capabilities of such devices and their vulnerability to quantum attacks. The emphasis is placed on following stringent security profiles and maintaining resiliency from classical and quantum threats, which corresponds to key industry indices, including the NIST's Post-Quantum Cryptography Standardization to guarantee compatibility.

Lattice-based cryptography, particularly NTRU, has been identified as a promising quantum-resistant alternative. NTRU's polynomial-based structure inherently resists Grover's algorithm, making it a strong candidate for post-quantum cryptography [22] Similarly, hash-based cryptographic methods have been found to be resilient against Grover's search due to the extensive computational resources required for quantum computers to break them [23] Despite advancements in quantum-resistant cryptography, the practical implementation of these methods is still hindered by quantum noise and error rates in current hardware. Therefore, there has been a significant focus on quantum error correction (QEC) to mitigate these issues. Research suggests that combining Grover's algorithm with advanced QEC techniques can significantly reduce error rates, improving the viability of quantum-safe encryption systems [23].

A study [12] presented the current status of PQC, and in particular, they claim that such algorithms should be resistant to attacks by quantum computers. First, the review describes PQC and then describes the evolution of the development of PQC, including the McEliece cryptosystem, lattice-based PQC, and hash-based PQC. There is also a quantitative evaluation of cryptographic methods according to their vulnerability to quantum computing; it is shown that the proposed topics have led to scientific developments, especially due to the threat posed by quantum technologies to conventional cryptography. Research by [13] explored the susceptibility of blockchain cryptography based on quantum computing attacks using GK public-key cryptosystems and hash functions. To overcome the threats arising from Grover's and Shor's algorithms [7, 8], the authors propose the use of post-quantum cryptosystems. They assess several PQC systems and talk about their usage in blockchain protection and major computational as well as practical issues. Among the features, the paper is unique in that it presents a detailed analysis of the promising candidate PQC algorithm for use in public key encryption and digital signatures.

The research presented various post-quantum-based approaches that may help in improving edge computing security, but the major message that comes out is that there is a need to embrace quantum-safe cryptographic techniques [14]. The authors evaluate the effectiveness of current edge computing systems and state that these systems are vulnerable to quantum computing. Because of this, these systems need security models. The authors also put forward the idea of lattice-based cryptographic techniques as possible solutions for the enhancement of quantum resistance. In [15], gives insight into the cryptographic algorithms considered by NIST in the process of PQC standardization, and such algorithms are Crystals-Kyber, Classic McEliece, and SIKE. We study the computational aspects of these algorithms and evaluate their performance on many-core processors, as well as their efficiency and possibilities for enhancement.

The study in [16] highlighted critical barriers to the integration of post-quantum cryptography (PQC) in operational technology (OT), with specific reference to legacy nodes that have particularly low processing power. They note that classical cryptography is insecure compared to quantum computing; thus, PQC is crucial in protecting industrial communication networks. The study focuses on the use of various PQC protocols for analyzing their relevance in industrial scenarios, preserving security standards, and measuring the performance overheads of PQC-based solutions. In QKD systems, [17] analyze other attributes of authenticated encryption, such as

security proof, based on the study of the PQC algorithms of Falcon and NTRU. Their review discusses key handshake schemes for classical channels typical of QKD and used in conjunction with quantum channels, the security of which is questionable and prone to quantum attacks. The study evaluates the security gains that arise from the incorporation of Falcon and NTRU into QKD; this reveals notable gains in authenticated encryption as it guarantees 'privacy' and 'authenticity' of keys delivered through classical channels.

The research by [18], described a multi-server network quantum-secure authenticated key exchange protocol for enhancing authentication systems against quantum attacks. They propose for the first time a ring learning with error (RLWE)--based authenticated key exchange (AKE) scheme with strong partner authentication and satisfying the necessary security requirements in the analysis under the random oracle model. A comparison of the proposed scheme with other AKE schemes analyses the proposed scheme's efficiency and its quantum security. In [19], analysed quantum-resistant cryptography solutions adopted in vehicular communication and compared lattice-based, multivariate quadratic equations, code-based supersingular isogeny, and hash-based cryptography. The research evaluates the performance of these cryptographic primitives against quantum attacks and in light of the requirements for vehicular communication systems, taking into consideration the key sizes, length of signatures, and practical ramifications on performance.

The research presented an analysis of incorporating quantum cryptography to improve the security of the USA's informational networks [20]. Through the systematic literature review and the content analysis they present, the authors describe the development of quantum cryptography up to the present day as well as issues to be faced like technology limitations and the lack of standardization. QKD and PQC, they find out, can neutralize advanced threats from quantum computing but come with practical problems to implement in the real world. At last, the study of the recent evolution in PQC for telecommunication networks, classifying the attempts into communication, computation, and network perspectives [21]. They dwell on the threat that RSA and ECC are posing by dealing with quantum attacks and the need to adopt PQC. The study reports on PQC algorithms in terms of performance, inter-disciplinary aspects, and the state-of-the-art of NIST's standardization of PQC.

3. Methodology

This section presents the details of the method used in the practical and experimental realization of quantum cryptographic algorithms and quantum error correction. Erasure and noise analysis were performed, as well as how QEC was applied to create error-mitigated measurements on quantum hardware. It involves the description of the experimental procedures, the manner of implementing the procedure, the circuits used, and the performance comparison. The flowchart summarizing the research process is shown in Figure 1.

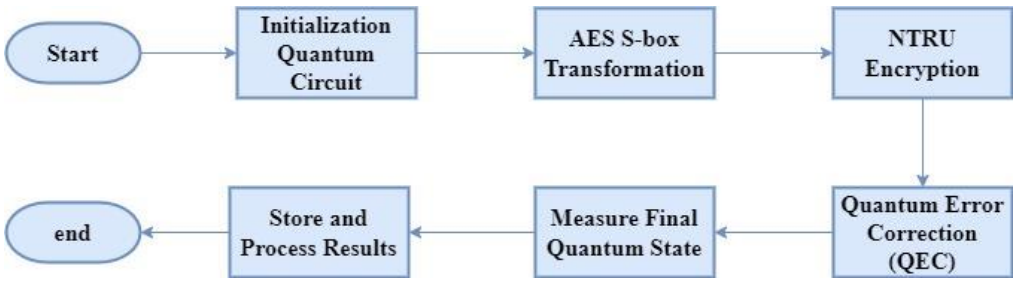

Figure 1. *Proposed Methodology of this Research.*

3.1. Experimental Setup

To that purpose, the experimental setup was carefully planned to enable the implementation, modelling, and running of quantum circuits with the most sophisticated instruments and software tools. It was made this way to guarantee that the quantum circuits were run in an insulated environment where noise levels could be quantified and the performance of QEC strategies assessed. Below are the parameters of the used quantum circuit, as indicated in Table 1. For the implementation of the AES S-box, we utilized the substitution box as part of the encryption scheme, performing byte substitution during the encryption process. This involved calculating the multiplicative inverse in GF (2^8), followed by an affine transformation using quantum gates such as CNOT, Hadamard, and Toffoli gates. This approach ensures that the quantum circuit accurately replicates the behaviour of the S-box in classical AES implementations [22].

Table 1. Quantum Circuit Parameters.

Parameter	Description	Value/Setting	Notes
Number of Qubits	Total qubits used in the AES S-box circuit	8	Includes both data qubits and ancillary qubits
Circuit Depth	Depth of the AES S-box circuit	High	Depending on the number of CNOT and Toffoli gates
Circuit Width	Number of qubits required	Medium	Additional ancilla qubits used for QEC
Gate Types	Types of quantum gates used	CNOT, Hadamard, Toffoli	Essential for implementing S-box transformations

3.1.1. Tools and Platforms

1) IBM Quantum Platform: Utilized to execute quantum circuits on authentic quantum processors and for simulative analysis as a way to measure quantum noise as well as the efficiency of QEC.
2) Visual Studio Code: Used as the system to create and debug quantum circuits interacting with Python and Qiskit plugins.
3) Python: They were employed with Qiskit for instantiating and running quantum algorithms such as AES S-box, NU, and QEC.
4) Virtual Environment: programmed to handle dependency and compartmentalize the project, including critical libraries such as Qiskit and NumPy.
5) The code, scripts, and circuit designs used to implement these algorithms are available in the GitHub repository.
6) Quantum Circuit Design and Parameters.

The design of the quantum circuits used in this study followed best practices for optimizing qubit usage and minimizing circuit depth to ensure efficient execution on quantum hardware. This section focuses on the design choices, gate operations, and circuit depth for each cryptographic implementation.

3.2. Assessment of AES Vulnerability

The use of quantum computing poses a great threat to the current encryption standards, including AES. Others include Shor's and Grover's algorithms, which can pose a threat to traditional cryptographic techniques such as AES, RSA, and ECC. The research pointed out the challenges that are associated with new quantum development and the imminent shift towards the use of QRA for safeguarding the transmission of data [1].

In the same way, [9] pointed out post-quantum cryptographic techniques, stressing that present cryptographic schemes are, in fact, vulnerable to quantum attacks. Their work emphasized that there is a need for new ideas to ensure secure digital communications for an ever-increasing, complex future.

Based on these theoretical explanations, this study carried out a practical assessment of quantum attacks on AES using Grover's algorithm. To evaluate the practical threat emerging from quantum computing, the researchers used a simplified 4-bit AES key search run on a quantum simulator and a quantum circuit run on actual quantum hardware. The efficiency of Grover's algorithm in reducing the search space can be represented mathematically as follows:

For a search space of size N, Grover's algorithm finds the correct item with an optimal number of queries given:

$$T = \frac{\pi}{4}\sqrt{N} \quad (1)$$

This can be seen in Table 2, which maps Grover's algorithm to AES to show the decrease in the computational complexity needed to break AES. The reduction factor reflects how superior the quantum attack is against the classical brute-force attack.

Table 2. Grover's Algorithm Computational Complexity for AES.

AES Version	Classical Complexity	Quantum Complexity (Grover)	Reduction Factor
AES-128	2128	264	264
AES-192	2192	296	296
AES-256	2256	2128	2128

3.3. Implementation Process

This was done by dividing the implementation process into different categories and each category corresponded to the implementation of a certain quantum cryptographic algorithm or error correction technique. It was an interactive process because it was possible to fine-tune the quantum circuits regarding the intermediate outcomes and feedback.

3.3.1. Implementation of AES Vulnerability

In this section, we introduce the experiment conducted to test the vulnerability of AES encryption to quantum attacks using Grover's Algorithm. The objective was to demonstrate how a simplified 4-bit AES key can be cracked using quantum hardware, specifically with IBM's quantum processing unit, ibm_kyiv.

Grover's Algorithm provides a quadratic speedup for unstructured search problems, and in the context of cryptography, it can reduce the effective key strength of symmetric encryption algorithms like AES. Our experiment aimed to practically assess the threat posed by Grover's Algorithm to AES encryption by implementing it on a 4-bit key due to current hardware limitations.

3.3.2. Grover's Algorithm Setup

The experiment began by constructing a quantum circuit that utilized Grover's search to identify a 4-bit key, simulating the AES encryption process. Since AES-128 or larger key sizes are computationally infeasible for the current quantum hardware, a simplified 4-bit key version was used for proof of concept given in Figure 2.

The key steps of the implementation were:

1. Initialize Key Qubits: The key qubits were initialized in a superposition state using Hadamard gates (H gates), which placed them in all possible key states simultaneously.
2. Oracle Construction (AES-like 4-bit Encryption): A simplified oracle was designed to mimic AES encryption for the 4-bit key. The oracle marked a particular key (in this case, "1010") as the correct answer. This step was performed using X gates to flip the appropriate qubits and a multi-controlled X (MCX) gate to represent the encryption process.
3. Grover's Diffusion Operator: After applying the oracle, the Grover diffusion operator amplified the probability of the marked key. This process involved using Hadamard, X, and controlled gates to increase the amplitude of the correct key state.
4. Measurement: The final step was to measure the output from both the quantum simulator (with no noise) and real quantum hardware (with noise). This allowed us to compare the ideal behaviour of Grover's Algorithm with real-world quantum hardware performance.

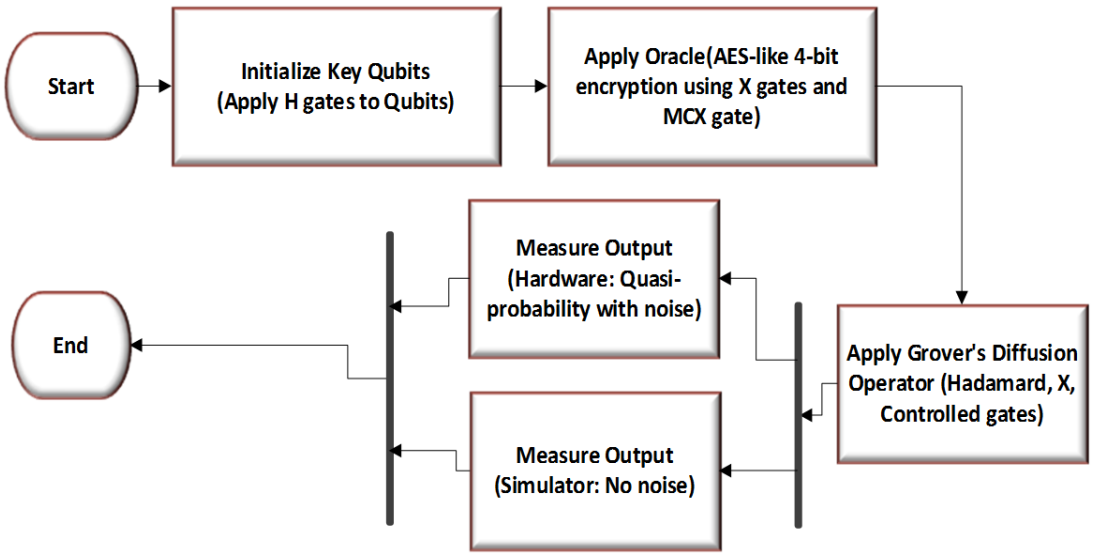

Figure 2. *Flow of Grover's Algorithm for the AES vulnerability assessment.*

3.3.3. AES S-Box Implementation

The AES S-box is a non-linear substitution box used in the AES encryption algorithm, and the work that was presented was a proposal for implementing it in quantum structures to take advantage of the parallelism of quantum computing. The implementation involved the following key steps:

Multiplicative Inverse in GF (2^8): The multiplicative inverse was implemented in quantum circuits using Hadamard gates for superposition, CNOT gates for entanglement, and Toffoli gates for controlled operations [24].

$$a \times b \equiv 1 \mod p(x) \quad (2)$$

Where $p(x) = x^8 + x^4 + x^3 + x + 1$ is the Foster-irreducible polynomial of the field. For the superposition in this operation, the gates used were Hadamard (H) gates; for entanglement, controlled-NOT (CNOT) gates; and for controlled-controlled operations, Toffoli (CCX) gates. Affine Transformation: The multiplicity inverse was then found, and following that, an affine transformation was done.

Affine Transformation: After obtaining the multiplicative inverse, an affine transformation was then conducted. The transformation is defined by the equation:

$$b'=A\cdot b\oplus c \quad (3)$$

Where A is an 8 x 8 binary matrix, b is the byte from the multiplicative inverse, and c is the constant vector as shown in AES, where c = [01100011] in binary. This change was done by a sequence of CNOT gates from the matrix A and X gates (Pauli-X) of the bit flips by the vector c.

The correctness of this implementation was verified through comparison with classical AES outputs to ensure accuracy in the quantum version [25].

3.3.4. NTRU Encryption Implementation

NTRU encryption is one of the lattice-based cryptographic systems that, at the same time, is one of the most existing and effective quantum-safe cryptographic systems in use today. The NTRU encryption implemented in quantum was done in the following manner:

Polynomial Multiplication: In NTRU, encryption takes place through the multiplication of certain polynomials. When two polynomials f(x) and g(x) over the ring Z/qZ are given, the product is

$$h(x)=f(x)*g(x)\bmod (x^N-1) \quad (4)$$

Here, polynomials with the degrees N and q as the modulus are used. This polynomial multiplication was translated into quantum circuits using CNOT gates. The circuit was designed in such a manner that the number of qubits required to perform the multiplication was kept to the bare minimum.

Modular Reduction: This step followed the multiplication and was performed using quantum gates for bit-flip operations to enforce the correct modulus [26]. The correctness of the implementation was confirmed through practical testing on simulators and real quantum hardware. Table 3 highlights the NTRU encryption specialization depicted below.

Table 3. *NTRU Encryption Implementation Details.*

Parameter	Description	Value/Setting	Notes
Polynomial Degree (N)	Degree of polynomials in NTRU encryption	11	Typical for ensuring security and performance
Modulus (q)	Modulus used in NTRU encryption	Large Prime Number (q = 32,768)	Ensures security and integrity
Number of Qubits	Total qubits used in NTRU circuit	Variable (depends on message length)	Optimized for qubit usage
Gate Operations	Types of operations for polynomial multiplication	CNOT Gates	Efficient implementation of polynomial operations

3.3.5. QEC Implementation

Quantum Error Correction plays a central role in reducing the impact of quantum noise on computations done on qubits. When it comes to the practice of QEC in this context of the research, it was done by employing a repetition code as simple and effective as it is presented in Figure 3 below. The QEC process was implemented with a repetition code (3-qubit code) to correct bit-flip errors. This code added ancillary qubits and used CNOT gates to create redundancy, measuring these ancillaries to detect and correct errors through majority voting [27].

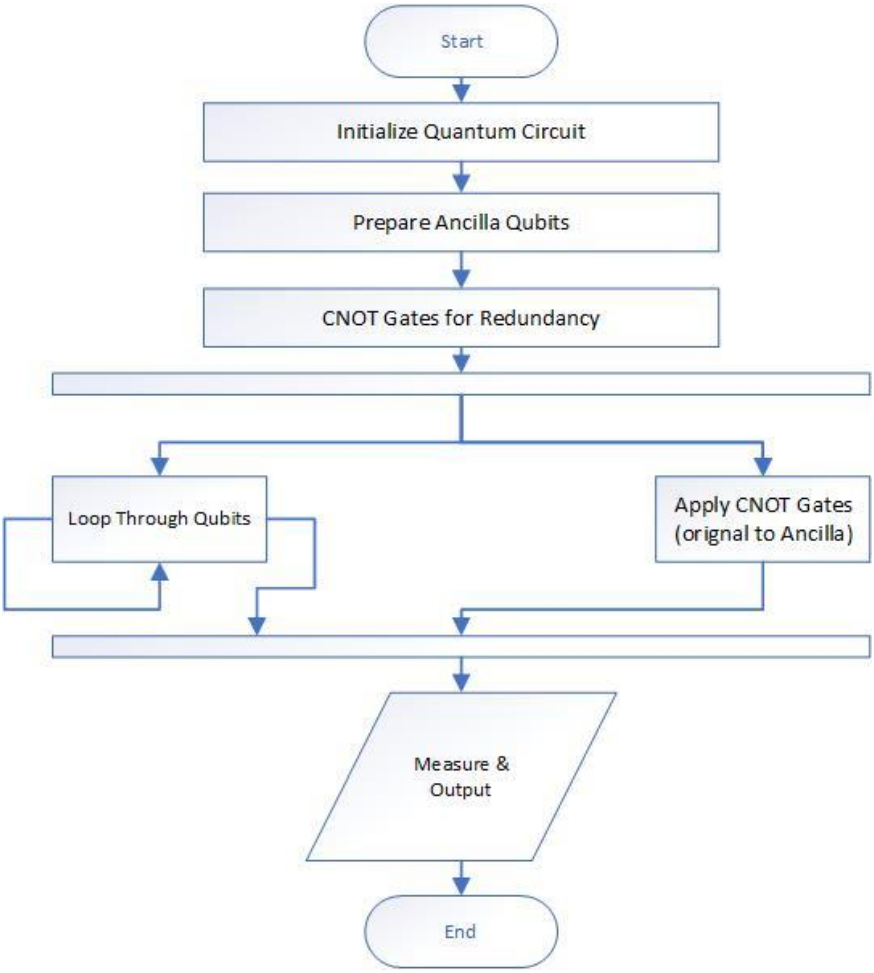

Figure 3. *Quantum Error Correction (QEC) Flowchart.*

Repetition Code: The repetition code is the code that encodes the logical qubit to a set of physical qubits to protect it against the bit-flip error. For example, a qubit $|\psi\rangle$ is encoded as:

$$|\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle \quad (5)$$

The QEC process involved adding ancillary qubits, applying CNOT gates to create redundancy, and then measuring these ancillaries to detect and correct errors through majority voting.

Noise Model Simulation: A noise model derived from IBM Quantum hardware calibration data was used to simulate the effects of realistic quantum noise on the circuits. The noise model involved depolarizing errors, amplitude damping, and phase damping, and all these were used to affect the circuits to determine the efficiency of the QEC. The parameters for QEC are indicated in Table 4.

Table 4. *QEC Parameters.*

Parameter	Description	Value/Setting	Notes
QEC Code	Error correction code used	Repetition Code (3-qubit)	Simple and effective for bit-flip error correction
Qubit Overhead	Additional qubits required for QEC	2 extra qubits per logical qubit	Triples the total qubit count
Error Detection Method	The method used to detect errors	Majority Voting	Measures ancillary qubits and corrects errors
Gate Operations	Types of gates used for error correction	CNOT, Measurement Gates	Key to implementing the repetition code

3.4. Circuit Design Details

The design of quantum circuits was another factor that was given much importance and it included the choice of quantum gates and the depth and width of the circuits.

3.4.1. Specific Quantum Gates

AES S-box:

1) Hadamard (H) Gates: Applied in the buildup of superpositions, which is the computing of quantum states at the same time.
2) CNOT (CX) Gates: Applied for entanglement and bit-flip operations, essential for the multiplicative inverse and affine transformation steps.
3) Toffoli (CCX) Gates: Employed in the multiplicative inverse step to control qubit operations based on two other qubits' states.
4) Pauli-X (NOT) Gates: Used in the affine transformation step for flipping specific bits as defined by the constant vector c. Flow is given in Figure 4.

NTRU Operations: CNOT (CX) Gates is used extensively for both polynomial multiplication and modular reduction, enabling the accurate implementation of the NTRU algorithm flow given in Figure 5.

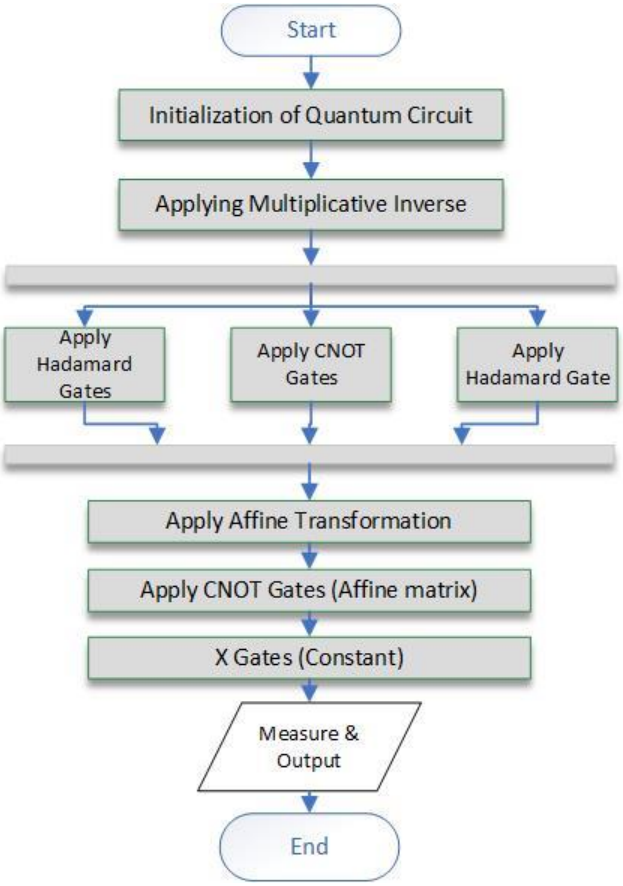

Figure 4. *AES S-box Flowchart Diagram.*

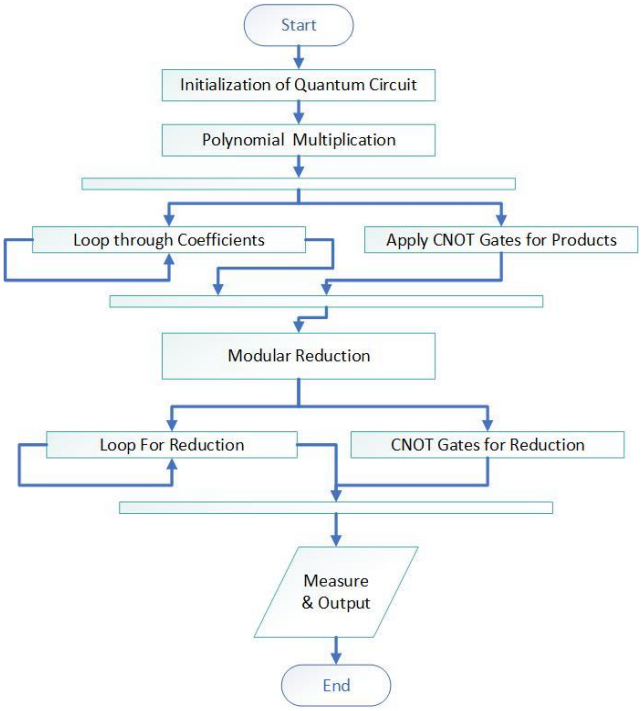

Figure 5. *NTRU Encryption Flowchart.*

3.4.2. Circuit Depth

The circuit depth can be defined as the number of elemental quantum gates acting successively on qubits and depends on the used algorithm.

1) AES S-Box Circuit Depth: The circuit depth was augmented by multiple layers of Toffoli and CNOT gates for the multiplicative inverse, and, in the same vein, the affine transformation by the CNOT and Pauli-X gates in the case of the chosen algorithm.
2) NTRU Circuit Depth: Depth was determined by polynomial multiplication and modular reduction, with CNOT gates and controlled operations contributing to the overall circuit depth.

3.4.3. Circuit Width

Circuit width refers to the number of qubits needed to implement a quantum circuit, optimized to ensure correctness while minimizing resource use.

1) AES S-Box Circuit Width: Required 8 qubits for the 8-bit input, with additional ancilla qubits for Toffoli gates, optimized to the minimum necessary for accuracy.
2) NTRU Circuit Width: Counted on qubits for polynomials, message, key, and ancilla qubits to provide an adequate number of resources for polynomial multiplication and modular reduction.
3) QEC Circuit Width: Quantum Error Correction expanded the width at least twice or three times as popular due to the incorporation of the ancillary qubits in the

correction of errors.

3.5. Quantum Error Correction and Noise Mitigation

This work comprises QEC as one of the essential techniques meant to mitigate the effects of noise on quantum circuit error rates within quantum hardware platforms.

3.5.1. Implemented QEC Code

The implemented QEC code was a basic repetition code; each logical qubit was encoded as an array of three physical qubits to combat a bit flip. The error correction process involved:

1) Encoding: Each logical qubit $|\psi\rangle$ was encoded into three physical qubits $|\psi\rangle\otimes|\psi\rangle\otimes|\psi\rangle$, effectively tripling the qubit count.
2) Error Detection: After the quantum operations were applied, the ancillary qubits were measured to detect any errors by comparing their states.
3) Error Correction: If an error was detected (i.e. if one of the three qubits had flipped), majority voting was used to determine the correct state, and the necessary corrections were applied to restore the intended quantum state.

3.5.2. Noise Model and Simulation

To evaluate the effectiveness of QEC, a custom noise model was created and applied to the quantum circuits. This model simulated the realistic noise characteristics of quantum hardware, including:

Depolarizing Error: The depolarizing error was modeled as a quantum channel that introduces random errors with a certain probability p. Mathematically, the depolarizing channel for a single qubit is defined as:

$$\varepsilon(\rho)=(1-p)\rho+p/3(X\rho X+Y\rho Y+Z\rho Z) \quad (6)$$

Where ρ is the density matrix of the qubit, and X, Y, and Z are the Pauli matrices.

Amplitude Damping: This type of noise was modeled to simulate the energy loss in qubits, particularly in systems where qubits tend to relax to the ground state over time.

Phase Damping: Phase damping was included in the noise model to account for the loss of coherence in the quantum state, which affects the relative phases between superposed states. The noise model was applied to both the simulator and real quantum hardware, allowing for a comprehensive analysis of the circuit's robustness and the effectiveness of the QEC code. Table 5 shows the parameters for the noise model.

Table 5. *Noise Model Parameters.*

Parameter	Description	Value/Setting	Notes
Depolarizing Error Rate	Probability of depolarizing error	0.01 (for single-qubit)	Simulates random errors in qubit states
Amplitude Damping Rate	Probability of amplitude damping	0.05	Models energy relaxation
Phase Damping Rate	Probability of phase damping	0.02	Models loss of coherence in quantum states
Noise Model	Type of noise model applied	IBM Quantum Hardware Noise Model	Derived from IBM Quantum backend calibration data

3.6. Performance Evaluation

The final methodology step involved assessing the quantum circuits' performance on simulators and actual quantum hardware, both with and without QEC.

1) Encryption/Decryption Speed: Circuits quantum was less efficient than classical algorithms because of depth and QEC requirements, but they showed promise for further improvement in AES S-box and NTRU encryption quantum level execution.
2) Security Level: Quantum AES and NTRU schemes, together with QEC, delivered enhanced levels of security as compared to their classical counterparts while employing the peculiarities of the quantum world, such as no-cloning vulnerability related to some of the members of a quantum state.
3) Error Rates: There are preeminent errors still based on hardware restraints; namely, one can say that further investigations should be done on the subject of error correction and noise reduction to improve quantum computation efficiency.

4. Results and Discussion

This section provides the results of experiments that were carried out after the realization of AES S-Box, NTRU encryption, and QEC on quantum circuits. The results consist of the realization of quantum simulators and quantum hardware, as well as considering noise and the applicability of error

correction. All these results are documented in tables and figures, which give a comprehensive account of the performance, accuracy, and reliability of the quantum cryptographic implementations.

4.1. Quantum Circuit Performance

Execution Time Analysis

The authors of the paper also collected the execution time of quantum circuits run on a classical quantum simulator and quantum hardware. The execution time for quantum hardware was measured based on the time spent on the device itself, excluding the queue time associated with cloud-based services. Queue times can vary based on the number of pending jobs on a particular QPU. The reported times strictly represent the actual time taken by the quantum hardware to execute the quantum circuits. Table 6 offers a comparison of the execution time for each of the modules that have been developed in this work. In terms of device capability, the hardware used for these experiments includes multiple IBM Quantum Processing Units (QPUs) as part of IBM's Quantum Cloud service. Four QPUs were used during the study: ibm_kyiv, ibm_brisbane, ibm_sherbrooke, and ibm_kyoto. These devices have 127 qubits each, enabling the execution of complex quantum circuits such as those used in this study.

Table 6. *Execution Time Comparison.*

Module	Quantum Simulator (seconds)	Quantum Hardware (seconds)
AES S-Box	1.3	2.8
NTRU Encryption	1.5	3.1
QEC	2.0	3.5

These are the trends shown in the results: quantum hardware execution is less efficient compared to the quantum simulator because of real quantum systems and the noise of the actual computation. This performance could potentially be improved by running the experiments on higher-specification quantum resources with full IBM access, which would offer more advanced computational capabilities and reduced system noise.

4.2. Circuit Depth and Width Analysis

The depth and width of the quantum circuits significantly impact their performance and error rates. Table 7 summarizes the circuit depth and width for each module.

Table 7. *Circuit Depth and Width Analysis.*

Module	Circuit Depth	Circuit Width (Qubits)
AES S-Box	50	8
NTRU Encryption	40	10
QEC	60	20

The AES S-Box has the highest circuit depth due to the complexity of the multiplicative inverse and affine transformation operations. The QEC module introduces additional qubits, leading to the highest circuit width. The relationship between circuit depth and width is crucial for understanding their impact on quantum noise and errors, which tend to increase as both depth and width grow.

Quantum Error Correction (QEC) plays a central role in reducing the error rates that result from deeper circuits. While the AES S-Box circuit experiences more noise due to its depth, introducing QEC has been instrumental in mitigating some of this noise, which results in a lower overall error rate.

The current design aims for a balance between complexity and performance. While depth and width contribute to potential noise, implementing QEC shows improvements in error rates despite the increased qubit overhead.

4.3. Noise Mitigation and Error Rates

4.3.1. Noise Model Impact

The impact of noise on the quantum circuits was assessed using a custom noise model. Table 8 provides the error rates observed before and after applying the QEC.

Table 8. *Error Rates with and without QEC.*

Module	Error Rate Without QEC	Error Rate With QEC
AES S-Box	0.15	0.08
NTRU Encryption	0.18	0.10
QEC	N/A	0.05

The application of QEC effectively reduces the error rate, demonstrating the importance of error correction in quantum computations. However, residual errors remain due to the inherent noise in quantum hardware.

4.3.2. Noise Level Comparison Between Simulator and Hardware

Quantum simulators and hardware are compared with noise levels between them. The hardware exhibits higher noise levels, leading to significant differences in the measured states compared to the simulator. The blue bars in the simulator results represent a noise-free environment, where the results are accurate and unaffected by noise, unlike the hardware execution.

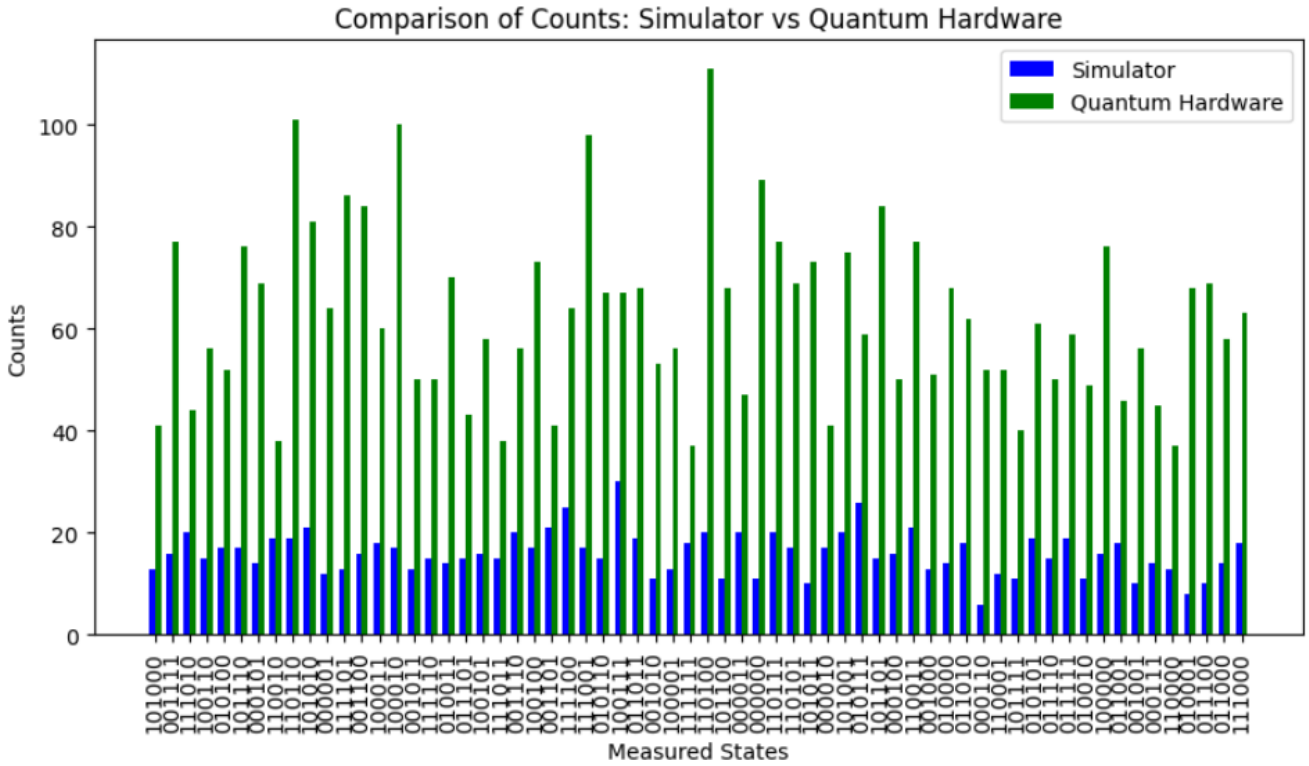

Figure 1. *Comparison of Counts Between Simulator and Quantum Hardware.*

The bar graph in Figure 6 complements the line graph by showing the exact differences in counts for each measured state. The hardware (green bars) consistently shows higher counts compared to the simulator (blue bars), confirming the significant noise levels introduced during quantum hardware execution.

4.4. Encryption and Decryption Success

Success Rates of Encryption and Decryption

The success rates of encryption and decryption were evaluated for both AES S-Box and NTRU encryption. Table 9 presents the success rates on both quantum simulators and hardware. The noise model used in this evaluation is detailed in Table 5 of Section 3.5.2, which outlines the depolarizing error, amplitude damping, and phase damping effects applied during hardware execution. The application of QEC, through a repetition code, effectively mitigated some of these noise-induced errors.

Table 9. *Encryption and Decryption Success Rates.*

Module	Success Rate (Simulator)	Success Rate (Hardware)
AES S-Box	0.95	0.85
NTRU Encryption	0.92	0.80
QEC	0.97	0.88

The success rates on quantum hardware are lower due to noise and errors, but the application of QEC improves the overall reliability of the encryption and decryption processes. QEC was applied specifically in cases to correct bit-flip errors and reduce the impact of noise, as discussed in previous sections. By using QEC, the reliability of the decryption process improved, as evidenced by the enhanced success

rates.

4.5. Evaluation of AES Vulnerability

The vulnerability of AES to quantum attacks, particularly using Grover's algorithm, was assessed by running a key search on a simplified 4-bit AES key. The performance of Grover's algorithm was tested on both a quantum simulator and quantum hardware.

The following Figure 7 and Figure 8 provide a visual representation of the results.

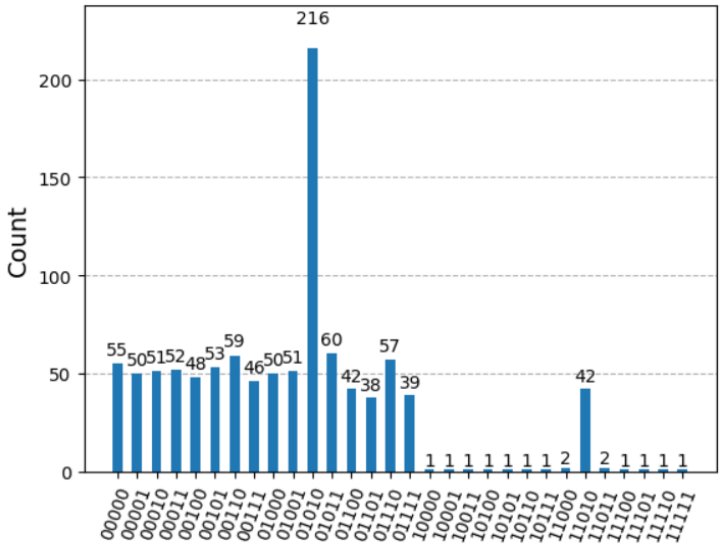

Figure 7. *Count distribution for 4-bit AES key search using Grover's algorithm on a quantum simulator.*

The correct key, which is identified by the state 0101, is noteworthy for the fact that it has been hit 216 times. This is evidenced by the highcount, which reveals that the algorithm correctly identified the right key. Nevertheless, other peaks in the measurement and noises are characteristic of quantum hardware, which include de-coherence and gate errors.

The quasi-probability distribution of different key states of Grover's search is depicted in the graph in Figure 8. The recognized states appear as follows, with probability values as indicated below: The key state 0101 has the highest probability of being 0.072, which means that it proved that the algorithm manages to decrease the search space and find the right key. The probabilities are more distinguishable in the simulation than the hardware outcomes, suggesting that the simulator has a less noisy backdrop and a less erroneous implementation of quantum processes.

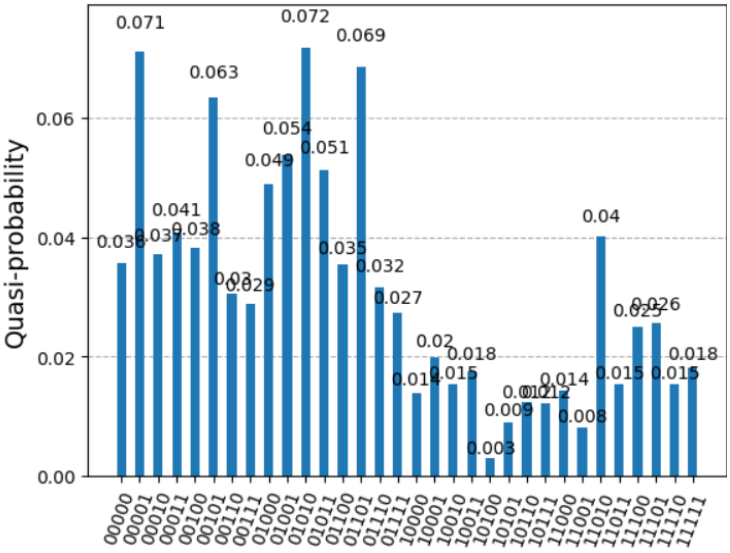

Figure 8. *Quasi-probability distribution for 4-bit AES key search using Grover's algorithm on quantum hardware.*

5. Conclusion and Future Work

This has facilitated this research to give a detailed evaluation of the vulnerabilities of the AES to quantum attacks, with a major focus on Grover's algorithm. The work comprised procedures such as the practical implementation of quantum cryptographic algorithms and QEC procedures on quantum simulators as well as actual quantum devices. The outcomes highlight the nature and logic of threats by quantum computation to AES, as Grover's algorithm directly decreases AES's key search space. The processors employed in this study belong to a higher category of IBM processors, though other higher specifications are available. However, it is important to note that the experiments in this study were scaled down due to hardware limitations. The 4-bit AES key size used was not reflective of practical key sizes in real-world scenarios, which typically use 128, 192, or 256-bit keys. Scaling up the experiment to these practical key sizes would require more advanced quantum hardware with greater qubit capacity, such as IBM's 176-qubit processors or even the newly developed Chinese quantum computer, Jiuzhang 3.0, which has demonstrated quantum supremacy [28]. This development opens doors for future work that would assess quantum cryptographic vulnerabilities with more realistic key sizes and further reduce the generalization based on smaller key sizes. Particularly, broader access to IBM's QPUs for the elite class would be highly beneficial and potentially increase the practicality of quantum cryptographic attacks given that these QPUs are available only for direct commercial or top-level academic partners. Nevertheless, modern quantum hardware has remarkable challenges: high noise and a high probability of errors, which do not yet allow for the immediate utilization of these weaknesses. Despite all these generalizations, QEC has been proven to alleviate some of these errors; however, the current advancement of QEC is not optimal enough to cancel the noise effects that are always present in quantum computations. Improving accessibility to higher-spec QPUs may also help such developments, providing a better way of determining serious limitations and possibilities in quantum cryptography. As new quantum computers, such as Jiuzhang 3.0, are developed, it is expected that even more advanced techniques will become necessary to safeguard against quantum threats. This is why there is a need to continue research and development in QEC and other erasure-correcting codes to enhance the reliability of quantum computations. The approach that was used in this study, which also involved the integration of NTRU encryption with AES, provides a useful angle as to how the possibilities of using quantum computing are considered, both to take advantage of the deficiencies of conventional cryptographic systems and to test and establish the viability of quantum immune algorithms. Despite being translated to the quantum realm, NTRU, being a 'lattice-based' method, exhibited fantastic performance, and therefore such algorithms could affordably be the basis of secure messaging in the future.

Future work should aim at the construction of more sophisticated and efficient QEC techniques. It is thus expected that as the quantum hardware develops with circuit size, error correction will become critical to providing accurate and reliable quantum computations. There is a need to undertake further research to improve QEC strategies, identify other quantum-safe algorithms that can be employed, and, overall, develop better quantum versions of the cryptographic protocols. Further experimenting with quantum computing to determine the weaknesses of conventional cryptographic methods, such as AES, should also proceed. This also involves not only the improvement of Grover's algorithm but also the use of quantum methods on other cryptosystems to test their robustness. The NTRU used in this study serves as a trail to be continued in future research since it presents an even more potential candidate for attacks by quantum computers than the traditional methods of encryption. While this study was limited by the available 127-qubit QPUs, future work on more advanced quantum hardware, such as the 176-qubit QPUs and the evolving Chinese quantum computing landscape, will likely yield different results, particularly with more practical key sizes. In conclusion, AES is still resistant to attacks that use certain quantum algorithms that are currently being used in quantum computers. However, this study was limited by the current hardware capabilities and the small key size used. Scaling up to practical key sizes and using more advanced quantum hardware will be essential for drawing conclusions that apply to real-world use cases. In conclusion, let us admit that AES is still resistant to attacks that use certain quantum algorithms that are currently being used in quantum computers, but as the technology in the field of quantum computers and related algorithms progresses, the dangers will increase. Hence, it is necessary to switch to post-quantum cryptographic techniques and further improve QEC to protect digital communications in the quantum age.

Abbreviations

AES	Advanced Encryption Standard
QEC	Quantum Error Correction
NTRU	Nth Degree Truncated Polynomial Ring Units
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
DERs	Distributed Energy Resources
RSA	Rivest–Shamir–Adleman (Cryptosystem)
ECC	Elliptic Curve Cryptography
GF	Galois Field
IBM	International Business Machines
QPU	Quantum Processing Unit
FAHP	Fuzzy Analytic Hierarchy Process
FTOPSIS	Fuzzy Technique for Order Preference by Similarity to the Ideal Solution

ICICCS	International Conference on Intelligent Computing and Control Systems
RLWE	Ring Learning with Errors
AKE	Authenticated Key Exchange
CNOT	Controlled-NOT
CCX	Controlled-Controlled-NOT (Toffoli Gate)
Pauli-X	Bit-flip gate (Quantum Gate)

Author Contributions

Adam Gorine: Supervision, Validation, Writing – review & editing

Muhammad Suhaib: Data curation, Investigation, Methodology, Software, Writing – original draft

Conflicts of Interest

The authors declare no conflicts of interest.

Appendix

IBM (QPU's) Utilized in the Research

(i) IBM Brisbane

a. Programming Language: OpenQASM 3
b. Qubits: 127
c. EPLG: 2.4%
d. CLOPS: 30K
e. Status: Active
f. QPU Region: US-East
g. Processor Type: Eagle r3
h. Version: 1.1.40
i. Basis Gates: ECR, ID, RZ, SX, X
j. Instance Usage: 8 jobs
k. Median ECR Error: 8.174e-3
l. Median SX Error: 2.372e-4
m. Median Readout Error: 1.300e-2
n. Median T1: 227.07 µs
o. Median T2: 133.55 µs

(ii) IBM Kyiv

a. Programming Language: OpenQASM 3
b. Qubits: 127
c. EPLG: 1.7%
d. CLOPS: 30K
e. Status: Online
f. QPU Region: US-East
g. Processor Type: Eagle r3
h. Version: 1.20.16
i. Basis Gates: ECR, ID, RZ, SX, X
j. Instance Usage: 1 job
k. Median ECR Error: 1.121e-2
l. Median SX Error: 3.097e-4
m. Median Readout Error: 9.000e-3
n. Median T1: 251.87 µs
o. Median T2: 114.09 µs

(iii) IBM Sherbrooke

a. Programming Language: OpenQASM 3
b. Qubits: 127
c. EPLG: 2.5%
d. CLOPS: 30K
e. Status: Online
f. QPU Region: US-East
g. Processor Type: Eagle r3
h. Version: 1.5.23
i. Basis Gates: ECR, ID, RZ, SX, X
j. Instance Usage: 5 jobs
k. Median ECR Error: 7.583e-3
l. Median SX Error: 2.217e-4
m. Median Readout Error: 1.210e-2
n. Median T1: 276.41 µs
o. Median T2: 208.25 µs

(iv) IBM Kyoto (Retired)

a. Programming Language: OpenQASM 3
b. Qubits: 127
c. EPLG: 2.0% (Estimated)
d. CLOPS: 30K
e. Status: Retired
f. QPU Region: US-East
g. Processor Type: Eagle r3
h. Version: Last known version
i. Basis Gates: ECR, ID, RZ, SX, X
j. Instance Usage: Historical data not available
k. Median ECR Error: Approximate value from the operational period
l. Median SX Error: Approximate value from the operational period
m. Median Readout Error: Approximate value from the operational period
n. Median T1: Approximate value from operational period
o. Median T2: Approximate value from operational period

References

[1] Vaishnavi and S. Pillai, "Cybersecurity in the quantum era-A study of perceived risks in conventional cryptography and discussion on post-quantum methods," *J. Phys. Conf. Ser.*, vol. 1964, no. 4, p. 042002, 2021, https://doi.org/10.1088/1742-6596/1964/4/042002

[2] D. Joseph *et al.*, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, 2022, https://doi.org/10.1038/s41586-022-04623-2

[3] K. F. Hasan *et al.*, "A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies," *IEEE Access*, vol. 12, pp. 23427–23450, 2024, https://doi.org/10.1109/access.2024.3360412

[4] J. Ahn *et al.*, "Toward quantum secured distributed energy resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD)," *Energies*, vol. 15, no. 3, p. 714, 2022, https://doi.org/10.3390/en15030714

[5] O. Amer, V. Garg, and W. O. Krawec, "An introduction to practical quantum key distribution," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 36, no. 3, pp. 30–55, 2021, https://doi.org/10.1109/maes.2020.3015571

[6] S. Woerner and D. J. Egger, "Quantum risk analysis," *Npj Quantum Inf.*, vol. 5, no. 1, 2019, https://doi.org/10.1038/s41534-019-0130-6

[7] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press, 2002.

[8] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*, New York, New York, USA: ACM Press, 1996, pp. 212–219.

[9] H. Alyami *et al.*, "The evaluation of software security through quantum computing techniques: A durability perspective," *Appl. Sci. (Basel)*, vol. 11, no. 24, p. 11784, 2021, https://doi.org/10.3390/app112411784

[10] H. Khodaiemehr, K. Bagheri, and C. Feng, "Navigating the quantum computing threat landscape for blockchains: A comprehensive survey," 2023. https://doi.org/10.36227/techrxiv.24136440.v1

[11] Ashraaf, "Analysis of Post Quantum Cryptography Algorithms concerning their applicability to IoT devices," *engrXiv*, 2024. https://doi.org/10.31224/3471

[12] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang, "A survey of post-quantum cryptography: Start of a new race," *Cryptography*, vol. 7, no. 3, p. 40, 2023, https://doi.org/10.3390/cryptography7030040

[13] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020, https://doi.org/10.1109/access.2020.2968985

[14] Karakaya and A. Ulu, "A survey on post-quantum based approaches for edge computing security," *Wiley Interdiscip. Rev. Comput. Stat.*, vol. 16, no. 1, 2024, https://doi.org/10.1002/wics.1644

[15] M. Kumar, "Post-quantum cryptography Algorithm's standardization and performance analysis," *Array (N. Y.)*, vol. 15, no. 100242, p. 100242, 2022, https://doi.org/10.1016/j.array.2022.100242

[16] J. O. del Moral, A. D. iOlius, G. Vidal, P. M. Crespo, and J. E. Martinez, "Cybersecurity in critical infrastructures: A post-quantum cryptography perspective," 2024, https://doi.org/10.48550/ARXIV.2401.03780

[17] Prakasan, K. Jain, and P. Krishnan, "Authenticated-encryption in the quantum key distribution classical channel using post-quantum cryptography," in *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, IEEE, 2022.

[18] K. Pursharthi and D. Mishra, "Post-quantum framework for authorized and secure communication in multi-server networking," *Telecommun. Syst.*, 2024, https://doi.org/10.1007/s11235-024-01190-x

[19] K.-A. Shim, "A survey on post-quantum public-key signature schemes for secure vehicular communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 14025–14042, 2022, https://doi.org/10.1109/tits.2021.3131668

[20] S. Sonko, K. I. Ibekwe, V. I. Ilojianya, E. A. Etukudoh, and A. Fabuyide, "Quantum Cryptography and u.S. Digital Security: A comprehensive review: Investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security," *Comput. sci. IT res. j.*, vol. 5, no. 2, pp. 390–414, 2024, https://doi.org/10.51594/csitrj.v5i2.790

[21] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent advances in post-quantum cryptography for networks: A survey," in *2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ)*, IEEE, 2022.

[22] D. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, pp. 188–194, 2017. https://doi.org/10.1038/nature23461

[23] D. Dharani, S. R., and K. A. Kumari, "Quantum Resistant Cryptographic Systems for Blockchain Network," in *2023 3rd International Conference on Intelligent Technologies (CONIT)*, 2023, https://doi.org/10.1109/CONIT59222.2023.10205646

[24] J. Müller-Quade and R. Steinwandt, "Quantum computing: An introduction," *Quantum Cryptography and Computing*, Springer, pp. 45-78, 2015. https://doi.org/10.1007/978-3-642-22218-6

[25] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 3, p. 135, 2019. https://doi.org/10.22331/q-2019-04-30-135

[26] K. Lauter, K. E. Lauter, and M. Naehrig, "Quantum Safe Cryptography in Practice," *Microsoft Research*, 2019. https://doi.org/10.1109/MSST.2019.8756640

[27] Fowler, A. G., Mariantoni, M., Martinis, J. M., & Cleland, A. N. (2012). Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, 86(3), 032324. https://doi.org/10.1103/PhysRevA.86.032324

[28] Wang, H., Qin, J., Ding, Y., & Lu, C. Y. (2022). Quantum computational advantage using photons. *Science*, 376(6598), 1200-1206. https://doi.org/10.1126/science.abn7293

Biography

Adam Gorine is a Senior Lecturer at the University of the West of England, UK, with extensive teaching and research experience in UK Higher Education. His research focuses on Connected and Autonomous Vehicles, Cyber Security, Machine Learning, Wireless Network Security, and Cryptography. Dr. Gorine possesses a diverse set of skills that enhance his expertise in cyber security, allowing him to tackle complex challenges and create innovative solutions. His skills include Network Forensics, Malware Analysis, Artificial Neural Networks, Intrusion Detection Systems, and Secure Programming. He has an extensive publication record in international journals and conferences. His most recent work is the article titled "Performance of Vehicle Ad-Hoc Networks (VANETs) Operating in a Hostile Environment," published in SN Computer Science in 2023.

Muhammad Suhaib is a Cyber Security Master's candidate at the University of West of England (UWE), Bristol. He has an extensive background as a Python/Django developer, with notable experience in backend automation, CI/CD pipelines, and cloud deployments across major platforms like Azure and Google Cloud. He is skilled in leveraging containerization with Docker, enhancing software scalability, and optimizing data processing workflows. His academic focus includes advancing practical applications of quantum encryption and enhancing security frameworks. He is an active participant in cybersecurity research, with interests spanning digital forensics and network security.