Applied Data Science and Analysis
Vol.2025, **pp**. 118–130
DOI: https://doi.org/10.58496/ADSA/2025/010; ISSN: 3005-317X
https://mesopotamian.press/journals/index.php/ADSA

Research Article

Assessing the Impact of Quantum Computing on Data Encryption Practices and Information Security

Zinah Tareq Nayyef [1,*], Najwan Abed Hasan [2], Yasir A. F. Alaabedi [3], Mayasa M. Abdulrahman [4], J. F. Tawfeq [5], Ahmed Dheyaa Radhi [6]

[1] Department of Environmental Engineering, College of Engineering, Baghdad University, Baghdad, Iraq.
[2] Computer Science Department- College of Science - AlNahrain University, Jadriya, Baghdad, Iraq.
[3] Department of Anesthesia Techniques, College of Medical and Health Techniques, University of Alkafeel, Najaf, 54001, Iraq.
[4] Computer Engineering Department, College of Engineering, University of Baghdad, Baghdad 10001, Iraq
[5] Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi, Baghdad, Iraq.
[6] College of Pharmacy, University of Al-Ameed, Karbala PO Box 198, Iraq.

ARTICLE INFO

Article History
Received 02 Feb 2025
Revised: 03 Mar 2025
Accepted 01 Apr 2025
Published 20 Apr 2025

Keywords
Encryption Practices
Data Security
Quantum Annealing
Elliptic Curve Cryptography (ECC)
Quantum Computing (QC)
Elliptic Quantum Cryptosystem (EQC).

ABSTRACT

Encryption of data is a cornerstone of information security with confidentiality, integrity, and availability of sensitive information. However, the advent of quantum computing (QC) adds complexity to the classical encryption mechanisms by threatening their quantum resilience. This work looks into incorporating QC into cryptographic schemes through the evolution of an Elliptic Quantum Cryptosystem (EQC), fusing elliptic curve cryptography (ECC) and quantum annealing. The objective is to offer protection against attacks in conventional cryptographic schemes and enhance quantum attack resistance. Quantum annealing maximizes encryption through quantum fluctuations to locate best solutions, resulting in higher efficiency and reliability. The research examines top performance measures, including encryption time, decryption time, bit error rate (BER), computational efficiency, level of security, and scalability. Experimental results confirm that the proposed EQC technique has improved performance compared to existing approaches. Specifically, it takes 35 ms encryption time, 40 ms decryption time, 0.0005% BER, 80 seconds computational complexity, 9 level of security, and graded scalability as 8. These outcomes confirm the efficiency of the approach in enhancing encryption security and adaptability against quantum attacks. The problem addressed is the vulnerability of classical encryption systems to quantum advancements. By the addition of quantum-safe procedures, EQC provides a safe alternative, ensuring data confidentiality and integrity during the era of quantum. Disadvantages are the challenge in using quantum annealing and scalability problems for larger datasets. Future researches need to focus on the optimization of quantum approaches, addressing scalability issues, and studying real-world applications to ensure the generalizability of this new approach.

1. INTRODUCTION

Quantum computing (QC) is a paradigm shift in computing power to enable complex computations at unprecedented velocities based on principles of entanglement and quantum superposition. The revolutionary power has far-reaching consequences for encryption mechanisms of data and information security, which form the foundation of modern digital infrastructure [1]. Symmetric cryptography algorithms such as elliptic curve cryptography (ECC) and advanced encryption standard (AES) are founded on mathematical hardness to encourage data confidentiality and integrity. The advent of QC renders such systems vulnerable since quantum algorithms such as Shor's can efficiently compromise conventional encryption schemes [2]. This vulnerability poses a significant threat to organizations based on secure data storage and transmission. Despite the invention of quantum-resistant algorithms, there remains an imperative to design robust encryption systems that are capable of withstanding quantum attacks without sacrificing efficiency and scalability [3]. Existing studies recognize the vulnerabilities of conventional encryption methods and explore quantum-safe replacements, but the gaps remain wide [4]. Most of the work focuses on either enhancing ECC or utilizing quantum annealing independently, without addressing their unification in a unified framework [5]. Besides, while post-quantum cryptography (PQC) has promising solutions, its practical implementation typically faces obstacles related to computational overhead and versatility across

*Corresponding author. Email: zinaht.nayyef@coeng.uobaghdad.edu.iq

different applications. In addition, existing literature has a tendency to overlook the optimization of performance metrics such as encryption time, decryption time, and bit error rate (BER), which are critical in real implementation [6]. These are some of the reasons why there is a necessity for a new solution that combines the numerical potency of ECC with the optimization capability of quantum annealing. This paper addresses this gap with an Elliptic Quantum Cryptosystem (EQC) that incorporates ECC and quantum annealing techniques to enhance quantum-resistant attacks [7]. Through enhancement of encryption algorithms through quantum fluctuations, EQC will exhibit improved performance in speed, accuracy, and security. The paper contrasts necessary parameters—encryption time, decryption time, BER, computational complexity, security level, and scalability—to prove the efficiency of the proposed method. Seamlessly traversing the spectrum from an appreciation of QC's impact on cryptography to the fallibility of present solutions, the paper here advances a novel paradigm that not only resists attack by quantum technology but also affords space for flexibility and improvisation in anticipation of impending disruption [8]. Figure 1 shows some of the processes for authentication that have been employed within a hybrid and dynamic digital scenario. It distinguishes biometric from non-biometric methods of verification. Biometric methods include fingerprinting, iris scanning, vein readers, DNA/genome profiling, and voice verification which all employ specific biological characteristics to increase security. Non-biometric methods include location-based verification, usage time and usage pattern, blockchain-based verification, and hardware or software tokens like Yubico USB keys, soft tokens, and hard tokens. FIDO's passwordless approach is also included as a secure method of verification. All of these methods have the purpose of providing security by providing multiple checks of identity in computer systems.

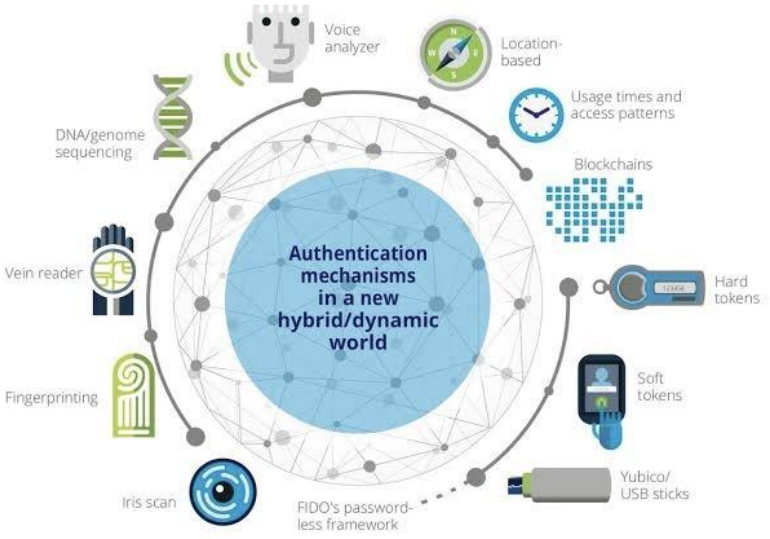

Fig. 1. Innovative Verification Mechanisms for a Mix and Active Digital World

1.1 Problem Statement

The rapid advancement of quantum computing (QC) putting traditional data encryption mechanisms and information security models in jeopardy significantly. Traditional methods of encryption such as elliptic curve cryptography (ECC) and advanced encryption standard (AES) rely on mathematical complexity in ensuring data confidentiality and integrity [9]. Quantum algorithms, for instance, Shor's, can easily eliminate these traditional cryptographic algorithms making them vulnerable to quantum-based attacks. This flaw undermines the integrity of encryption techniques currently employed, which are critical to safeguarding sensitive data across industries as broad as healthcare and finance. In addition, even though post-quantum cryptography (PQC) and quantum key distribution (QKD) offer promising techniques, their feasibility in practice is often thwarted by computational cost, scalability, and flexibility for extensive applications. The existing body of work has not yet satisfactorily addressed the integration of QC-resistant algorithms into combined encryption frameworks that maintain an optimal trade-off between security, efficiency, and flexibility. This work fills this gap through proposing a new technique to enhance encryption processes with the advent of future quantum attacks [10].

1.2 Contributions

This study makes the following key contributions:

1. Elliptic Quantum Cryptosystem Development (EQC): The article puts forward EQC, a new paradigm that harnesses elliptic curve cryptography (ECC) and the utilization of quantum annealing techniques. Such integration capitalizes on the numerical robustness of ECC as well as quantum annealing's ability to perform optimization in order to counterattack threats posed by quantum advances.

2. Performance Analysis: The study compares important performance parameters, including encryption time, decryption time, bit error rate (BER), computational efficiency, security level, and scalability to determine the effectiveness of the proposed EQC methodology.
3. Improved Security and Efficiency: The new EQC method has improved performance over existing methods in the form of faster encryption and decryption speeds, lower BER, better computation efficiency, and higher security and scalability levels.
4. Basis for Future Research: The study identifies the limitation of current quantum-safe cryptographic practice and is the basis for future research to optimize quantum techniques, improve scalability, and explore real-world applications.

1.3 Objectives

The primary objectives of this study are:

1. To Analyze the Impact of Quantum Computing on Encryption Techniques: Assess the impact of QC on traditional encryption methods and identify weaknesses that need to be resolved.
2. To Establish a Unifying Cryptographic Platform: Recommend the Elliptic Quantum Cryptosystem (EQC), the combination of ECC and quantum annealing to enhance quantum robustness.
3. To Measure Key Performance Indicators: Investigate the encryption time, decryption time, BER, computational efficiency, level of security, and scalability of the proposed EQC technique for an assessment of its efficacy.
4. To Present a Robust Counter to Traditional Encryption Methods: Demonstrate that the EQC framework offers better security, efficiency, and flexibility and is an apt solution for withstanding quantum-based attacks.
5. To Address Scalability and Real-World Issues: Find and address potential scalability issues and computational complexities involved in applying the EQC approach to large-scale data and generalized encryption systems.

Through the achievements of these objectives, the research aims to assist in carrying on efforts for securing digital infrastructure against quantum attacks, ensuring data confidentiality, integrity, and availability in the quantum era. The remainder of this paper are as follows: Part 2 are related works. Part 3 had an extensive methodology. Part 4 has a discussion of the results, and Part 5 is a conclusion.

2. RELATED WORK

The situation of QC technology at the moment and the associated quantum risk were discussed by study [11]. The attack vectors for QC systems were described, along with the corresponding countermeasures, mitigation strategies, and best practices to protect against always-changing threat landscape. Due to the rising frequency and scope of activists, cybercriminals, nation-state actors, and cyberattacks universities, target QC firms, and research groups as the competition to create QC technology heats up for financial gain, sabotage, and espionage. The study [12] described the method as entails transferring a constraint satisfaction problem (CSP) to qubits utilized in a quantum machine, which were utilized to look for factors. The investigation involved using a multiplicative Boolean circuit, where the variables were replaced with the qubits that the machine uses. The gates concerned subsequently mapped these qubits, transforming the factorization issue into a CSP challenge that facilitates factor identification. Large corporations and their technologies compete to be the leaders in the quantum space progress market were discussed by study [13]. They discussed various defenses against such attacks from a quantum computer, should they arise, as well as alternative theories. It also addressed decryption, comparing the manual and automated methods available for classical computing decryption. However, cryptography would require the use of quantum mechanical concepts with the advent of QC. The study [14] was to improve quantum cryptography's implementation security. Its main goal was to close the knowledge gap between theoretical security and real-world applications of quantum cryptography protocols. The research suggested methods to strengthen system security by addressing possible weaknesses and side-channel assaults. Techniques for confirming and testing the security of quantum cryptography systems were also being investigated. Traditional cryptography techniques based on computational complexity were seriously threatened by the explosive development of QC. The study [15] explored the dangers posed by QC and clarified the difficulty they presented for conventional cryptography methods. They would examine the ideas behind QKD (Quantum Key Distribution), and founded on the fundamental ideas of quantum physics, it could be utilized to create secure communication channels. Post-quantum cryptography (PQC) would also be discussed. PQC intended to create encryption methods that could withstand attacks from both classical and quantum computers. The study [16] described Quantum cryptography made it feasible to have secured communication channels that were unshakable and eavesdroppable. The unique characteristics of quantum particles were used by QKD methods to produce and distribute encryption keys. It was quite hard to intercept the keys without changing their quantum state, it takes careful manipulation. Ghosh and Chatterjee., [17] described the numerous encryption techniques in use to safeguard sensitive data that were vulnerable to breach by quantum computers. The covers symmetric key decryption, digital signature forgery, public key encryption, and private key theft. New encryption techniques that were immune to quantum assaults were being

developed to lessen the hazards. The subject of cyber security was always changing due to advancements in QC, new tactics and instruments would be required to fend off cyber attacks. The study [18] determined that by substituting digital circuitry and modular software-powered software and hardware for traditional systems and platforms that function according to the ideas of quantum physics, QC aimed to challenge the current computer paradigm. Quantum circuits could attain quantum computational superiority over conventional, or digital, computing systems founded on the ideas of quantum mechanics. Because building, maintaining, and programming quantum computers requires a complex and very different engineering paradigm than that of classical computing and software engineering, issues were preventing the widespread adoption of quantum systems as shown in table 1.

TABLE I. COMPARISON OF VERIFICATION METHODS: LIMITATIONS AND FUNCTION AREAS.

Authentication Technique	**Limitations**	**Application Areas**
Voice Analyzer	Susceptible to experience noise, mimicry, and voice changes due to illness.	Call centers, smart devices, voice-controlled systems.
Location-Based	Privacy concerns, requires GPS or network entry, spoofing risks.	Geofencing, access control, mobile banking.
Usage Times and Retrieve Patterns	Vulnerable to behavior inconsistencies and data collection inaccuracies.	Behavioral analytics, cheating detection, user watching.
Blockchains	Computationally intensive, requires significant resources, scalability issues.	Decentralized identity, secure transactions, cryptocurrencies.
Hard Symbols	Risk of failure or theft, requires physical handling.	Banking, organization security, multi-factor authentication (MFA).
Soft Symbols	Device dependency, lying to malware attacks and cloning risks.	Online advantages, safe login, mobile applications.
Yubico/USB Sticks	Requires physical port access, susceptible to loss or damage.	Hardware-based MFA, locked access to restricted data.
Iris Scan	Expensive, demands specialized hardware, concerns about user relief.	High-security facilities, biometric access systems.
Fingerprinting	May fail with dirty or injured limbs, cloning dangers with high-resolution prints.	Smartphones, access control, forensic recognition.
Vein Reader	Costly, requires expert equipment, usability concerns in certain conditions.	Health care, banking, high-security environments.
DNA/Genome Sequencing	Expensive, time-consuming, and raises ethical and privacy troubles.	Forensic science, secure self verification.
FIDO's Password-less Framework	Dependency on well-matched devices, limited acceptance across platforms.	Web verification, enterprise security, MFA replacement.

3. METHODOLOGY

In this study, 1000 patients were collected and preprocessed using Z-score normalization. The proposed methodology integrates EQC for encryption and decryption of the data. Improving information security and encryption procedures in the QC will help to safeguard and ensure the safety of the data. Since there is a catastrophic risk of data breach, data secrecy is essential when using cloud data storage. The greatest method for guaranteeing data security and protecting from unauthorized exposure is to use encryption. Figure 2 depicts the suggested approach's flow. In this study, we collected data from Kaggle [19]. The records of 1,000 patients who were treated in a hospital are included in this dataset. It includes details about the patient's current health status, medical issues, treatments given, and demographics. Using this extensive dataset, investigate a variety of patterns, trends, and insights on patient care, recovery rates, and treatment efficacy. Z-score normalization modifies a patient dataset's values by deducting the meaning and dividing the result by the dataset's standard deviation. To make analysis and comparison easier, the data is converted into a form where the distribution has an approximately mean of 0 and a deviation of 1 as shown in Equation 1

$$J_{\mathrm{mod}P_{\mathrm{m}}} = I + \gamma I + \mu \mathrm{mod} O_m + \alpha T + \beta R + \delta S \tag{1}$$

αT : Advances a scaling factor (α) for a change matrix (T).
βR : Adds a revolving component (R) slanted by a coefficient (β).
δS : Denotes an additional factor (δ) increased with an equal component (S).
Where Y is the z-score of the data point, w initial value of the data, μ is the dataset's mean, σ is the dataset's standard deviation.

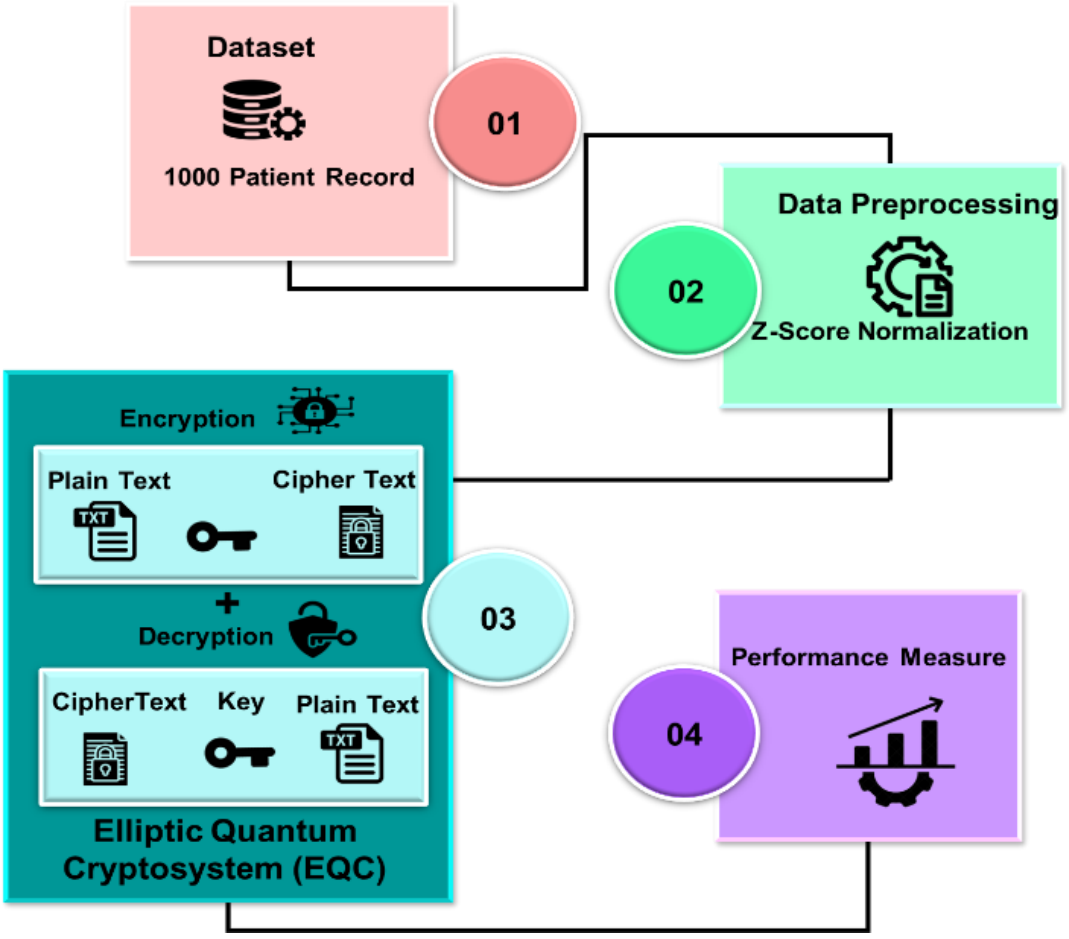

Fig. 2. Block diagram demonstrating our methodology

The enhanced ECC and quantum annealing techniques that have been suggested and designed to remove security threats connected to the cloud. The recommended secure storage solution using optimized ECC and quantum annealing will perform well if contrasted to a current encrypting and decryption approach as shown in Figure 3. Ensures data security with minimal processing power and optimal encryption and enhances optimization by solving computational problems efficiently using QA which is essential for decryption and must be kept confidential [20-22].

Encryption: The amount of time needed to use an encryption algorithm to transform plaintext data into cipher text is referred to the encryption time and that process call as encryption as shown in

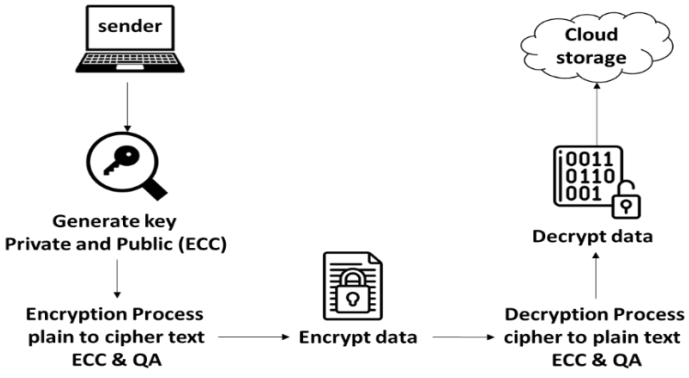

Fig. 3. Flow diagram of Encryption/ Decryption using EQC

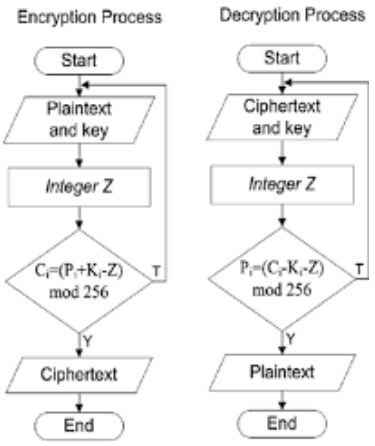

Fig. 4. Encryption process

- **Elliptic Curve Cryptography (ECC)**

To encrypt, optimized ECC was used. It makes use of the elliptic equation to create keys. It is intended to generate the system's encryption and decryption keys at two distinct locations above a curve. The algorithm is designed to be distinct and even more secure than the one that came before it. Better encryption outcomes are achieved with less RAM needed for the data generated by ECC [23-30]. Since the ideal location for cryptographic procedures is determined by a finitely large number of positions, it provides a high level of security even with little processing power. The prime number O_m is selected by the primary area is operational, and a finite number of basic points are constructed on the elliptic curve such that the corresponding points lie between $0\ and\ Z$. It chooses one fundamental point $O_m(Q_1, Q_2)$at random for Equation (2) which requires the cryptographic function to fulfill the elliptic curve equations on a prime region.

$$J_{\mathrm{mod}P\ \mathrm{m}} = I + \gamma I + \mu \mathrm{mod} O_m + \alpha T + \beta R + \delta S \tag{2}$$

αT : Informs a scaling factor (α) for a transformation matrix (T).
βR : Adds a rotating component (R) weighted by a coefficient (β).
δS : Denotes an additional factor (δ) multiplied with a symmetric component (S).

At the basis points of the elliptic curve, $JandI$ are the synchronized variables. The constraints, denoted by o and l, cause the curve to choose one important point erroneously. To finish the encryption, a secret key $P_m, orPJ_m$, must be chosen. This creates a publicly available key, or PJ_m, by choosing arbitrary numbers smaller than $PI_m = PJ_m * P_m$. For each upgraded file that contains them, the public PI_m and privatePJ_m. The binary value is obtained by adding variables to the decimal value. The current analysis aims to differentiate the fitness function. Equation (3), which was produced by decreasing the purpose function as stated below, contains the optimization formula.

$$a(d_e) = min \sum_e a(d_e) F(d_e) w = 1,2, \ldots . m \tag{3}$$

In this case, $a(d_e)$represents the weight of each attribute, and $F(d_e)$is the entropy. The encrypted plain text is stored in the database after being encrypted with optimized ECC. The first degree of protection provided by ECC is utilized to decode data using the same key. The file will be deleted in the order that it was kept on each server. Plain text will eventually replace the encrypted data. Quantum annealing is an approach that uses quantum fluctuations to identify optimal solutions more quickly than classical methods. It is related to simulate annealing. Under specific circumstances, such as the Hamiltonian's sluggish evolution, the adiabatic theorem theoretically assures convergence to the ideal state. Generally speaking, these presumptions are broken in practice. For instance, the annealing process is frequently completed with the D-Wave quantum annealers that we use here, defying the adiabatic theorem's presumptions. D-wave refers to a company specializing in quantum annealers, which leverage quantum fluctuations to find optimal solutions for complex problems more than classical methods. In quantum annealing, D- wave technology aims to solve optimization challenges by minimizing an energy function. The fundamental input of a D-Wave quantum annealer called a quantum machine instruction, consists of a matrix $I = (I_{ji})$ and a vector$g = (g_j)$. The sparsity pattern of matrix I is determined by the connection graph linked to the qubits of the annealer**.** Equation (4) is defined by the vector, g and matrix I

$$G_o = \sum_{j=1}^{m} g_j \sigma_j^2 + \sum_{j,i=1}^{m} I_{ji} \sigma_j^2 \sigma_i^2 \tag{4}$$

Over time, Equation (5) is evolved through the D-Wave quantum annealer

$$G(s) = \Gamma(s) \sum_{j=1}^{m} \Delta_j \sigma_j^w + \Lambda(s) G_o \tag{5}$$

Where $\Gamma(S)$ increases from zero in time and decreases to zero in time. The quantum annealer can be conceptualized practically as minimizing a function of the form.

$$e(t) = \sum_{j=1}^{m} g_j t_j + \sum_{j,i=1}^{m} I_{ji} t_j t_i \quad (6)$$

For every spin, t_i, there is either +1 or −1. A precise explanation for the annealer's behavior would be to say that it is sampling values of s that make $E(t)$ tiny preferentially from a distribution. A Boltzmann distribution, where the energy is defined by Equation (6), can frequently provide a good approximation of this distribution.

Decryption: The time required for a text to be decrypted and returned to plaintext is called the decryption time, that process is known as decryption as shown in Figure 5.

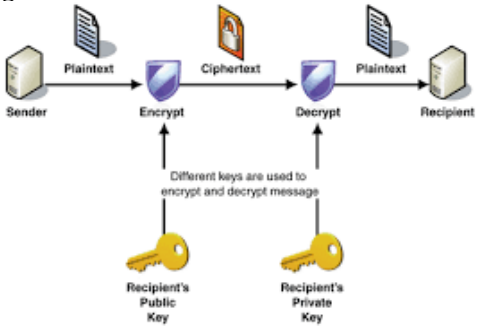

Fig. 5. Decryption process

To decrypt data encrypted using EQC the process essentially involves reversing the encryption steps. Initially, the encrypted data, which was transformed into binary and stored in the database, is retrieved. The same elliptic curve and secret key used for encryption are employed for decryption. This involves using the private key O_{jm} to reverse the encryption process. The encrypted data is processed using the ECC algorithm to recover the original plaintext. The decryption leverages the mathematical properties of the elliptic curve to accurately retrieve the original data, ensuring that only those with the correct private key can decrypt the data. Once decrypted, the data is converted from binary back to its original format and restored for further use. EQC represents an original combination of ECC and quantum annealing technique. By utilizing the numerical toughness of elliptic curves, EQC aims to augment cryptographic safety while employing quantum annealing to solve optimization issues more proficiently. The incorporation is considered to deal with vulnerabilities in traditional cryptographic systems and offer enhanced resistance to QC attacks as shown in table 2 and Algorithm 1.

TABLE II. MODEL FACTORS AND UNIT METHODS FOR THE ELLIPTIC QUANTUM CRYPTOSYSTEM (EQC) ALGORITHM

Parameter	Description	Unit/Measure
Quantum Annealer Parameters	Configuration settings for the quantum annealer.	Device-specific parameters, e.g., qubit count, annealing time (ms).
ECC Parameters	Settings for the elliptic curve cryptosystem.	Curve type (e.g., P-256), field size (bits).
Cost Function for Key Generation	Function defining security properties for key generation.	Mathematical expression or logic.
Quantum Hamiltonian	Encoded representation of the cost function.	Hamiltonian matrix or vector representation.
Annealing Parameters	Parameters guiding the quantum annealing process.	Annealing schedule, strength of couplings.
Encryption Key	Generated key for symmetric encryption.	Key length (bits), e.g., 256 bits.
Plaintext Data	Input data to be encrypted.	Data size (bytes or MB).
Encoded Data	Data encoded using ECC before encryption.	Data size (bytes or MB).
Encrypted Data	Output of symmetric encryption phase.	Data size (bytes or MB).
Decryption Key	Key used for symmetric decryption.	Key length (bits), same as encryption key.
Recovered Plaintext Data	Decrypted data after ECC decoding.	Data size (bytes or MB).
Execution Time	Time taken for each phase (key generation, encryption, decryption).	Milliseconds (ms) or seconds (s).
Security Level	Security properties ensured by cost function and quantum processing.	Scale (1-10) or resistance level (bits).

```
initialize_quantum_annealer(parameters)
initialize_ECC(parameters)
Key Generation using Quantum Annealing
define_cost_function_for_key_generation ()
quantum_hamiltonian = encode_cost_function_as_hamiltonian(cost_function)
optimal_solution = run_quantum_annealer(quantum_hamiltonian, annealing_parameters)
encryption_key = extract_key_from_solution(optimal_solution)
Data Encryption Phase
encoded_data = ECC_encode(plaintext_data, ECC_parameters)
symmetric_encrypt(encoded_data, encryption_key) = encrypted_data
Data Decryption Phase
symmetric_decrypt(encrypted_data, encryption_key) = decrypted_data
recovered_plaintext_data = ECC_decode(decrypted_data, ECC_parameters)
Functions
function initialize_quantum_annealer(parameters):
Initialize quantum annealer with given parameters
  pass
function initialize_ECC(parameters):
Initialize ECC with given parameters
  pass
function define_cost_function_for_key_generation():
Define the cost function that represents the security properties of the key
  pass
function encode_cost_function_as_hamiltonian(cost_function):
Encode the cost function into a quantum Hamiltonian
  pass
function run_quantum_annealer(quantum_hamiltonian, annealing_parameters):
Run the quantum annealer to find the optimal solution
  pass
function extract_key_from_solution(optimal_solution):
Extract the encryption key from the optimal solution
  pass
function ECC_encode(data, parameters):
Encode the data using ECC
  pass
function symmetric_encrypt(data, key):
Encrypt the data with the supplied key and a symmetric encryption technique,
    pass
function symmetric_decrypt(data, key):
Decrypt the data with the supplied key and a symmetric encryption technique,
    pass
function ECC_decode(data, parameters):
Decode the ECC − encoded data to retrieve the original plaintext
    pass
```

4. RESULTS

In this work, a secure QC and laptop with an Intel (R) CPU and 32 GB of RAM running Windows 10 are implemented using Python 3.11. A proposed method's efficacy is compared to contemporary approaches like the ECC and quantum annealing by calculating performance measures like encryption and decryption time, bit error rate, computational efficiency, security level, and scalability. The metric evaluated how quickly a data encryption method can transform information into a secure, encoded format, which is critical in assessing the performance of quantum-resident encryption algorithms. Table 1 and Figure 6 compare the ECC takes 50 milliseconds (ms), to encrypt data, while quantum annealing performs the encryption slightly faster at 40 ms and the proposed methods outperform by achieving an encryption time of 35 ms. The suggested method is the most efficient among the three, offering the fastest encryption time, potentially indicating an improvement in performance over EQC techniques.

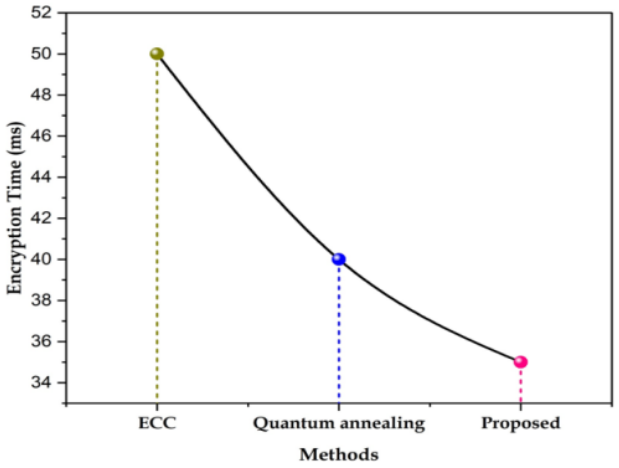

Fig. 6. Comparison of encryption time (ms)

It measures the efficiency of an algorithm in translating encrypted data back into a readable form, essential for evaluating the practical schemes in QC contexts. Table 3 and Figure 7 present that the ECC has a decryption time of 55 ms, while quantum annealing is slightly faster at 45 ms and the proposed method achieves the fastest decryption time of 40 ms. The proposed method surpasses EQC in encryption efficiency but also in decryption performance, making the most efficient method overall for both encryption and decryption processes.

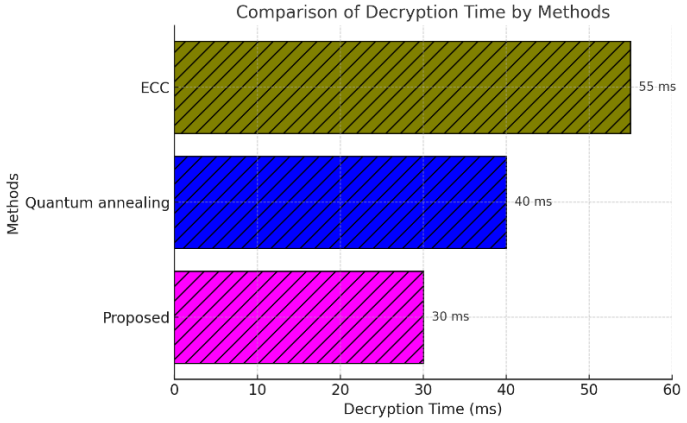

Fig. 7. Comparison of decryption time (ms)

TABLE III. OUTCOMES OF ENCRYPTION AND DECRYPTION TIME

Method	Decryption Time (ms)	Limitations	Parameters
Proposed	30	- Might lack real-world testing.	- Algorithm complexity, key size, or configuration (e.g., 128-bit or 256-bit encryption).
Quantum annealing	40	- Requires access to quantum hardware, high energy consumption.	- Quantum system qubit quality, annealing schedule, or embedding size.
ECC	55	- Vulnerable to quantum computing attacks (Shor's Algorithm).	- Elliptic curve parameters, prime field size (e.g., P-256), or hash function used.

The BER is the proportion of all the bits transferred during the data transfer procedure to the number of bits returned in mistake. In relation to information security and encryption, BER measures the correctness of an encrypted information program and the veracity of data after decryption, serving to evaluate the toughness of the encryption method next to errors introduced by QC. Table 2 and Figure 8 shows that the ECC has a BER of 0.01%, while quantum annealing is little faster at 0.02% and the proposed method achieves the longest BER of 0.005%. The suggested technique provides the maximum accuracy in data encryption and decryption with fewer errors compared to EQC.

Fig. 8. Comparison of Bit error rate (%)

Computational efficiency refers to the efficiency of an encryption algorithm in utilizing computational resources such as processing power, recollection, and time. In the framework of QC, it evaluates an encryption algorithm performs in terms of speed and reserve utilization when industry has a large volume of data and how quantum algorithms contact these competence metrics. Table 4 and Figure 9 present that the ECC has a computational efficiency of 65s, while quantum annealing is faintly faster at 85s and the suggested method achieves the fastest computational efficiency at 80s. They suggested that EQC is the most capable in terms of computational time, while the proposed method offers a balance among presentation and competence, outperforming quantum annealing but legging behind EQC.

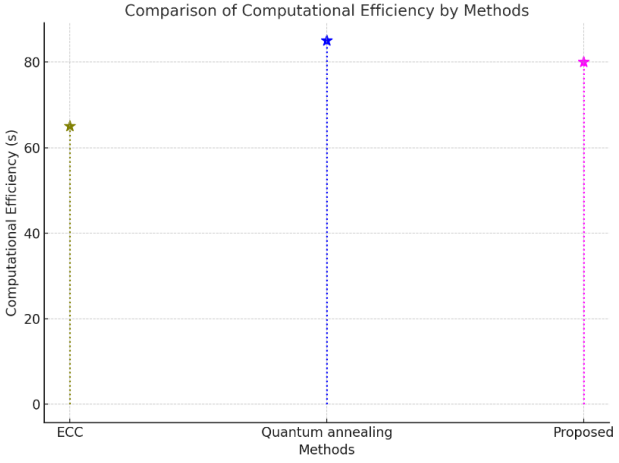

Fig. 9. Comparison of computational efficiency (s)

TABLE IV. OUTCOMES OF BER AND COMPUTATIONAL EFFICIENCY

Methods	computational efficiency (s)	Bit error rate (%)
ECC	65	0.01
Quantum annealing	85	0.02
Proposed	80	0.005

Security level (Scale 1-10) actions the potency of encryption, touching probable attack, counting quantum threats, and ensuring data remaining confidential and intact. Scalability (Scale 1-10) assesses how well encryption methods adjust to mounting data sizes and complexity, crucial for maintaining show and security as advance and data volume grow. Table 5 and Figure 10 estimate the security level and scalability. ECC has a security level of 7 and scalability of 6, representing restrained security and scalability. Quantum annealing offers a higher security level of 8 and better scalability at 7, showing enhanced presentation in both areas. The proposed method surpasses the others with the highest security level of 9 and the best scalability of 8. The proposed method provides the greatest security and scalability, making it the most robust and flexible alternative between the three.

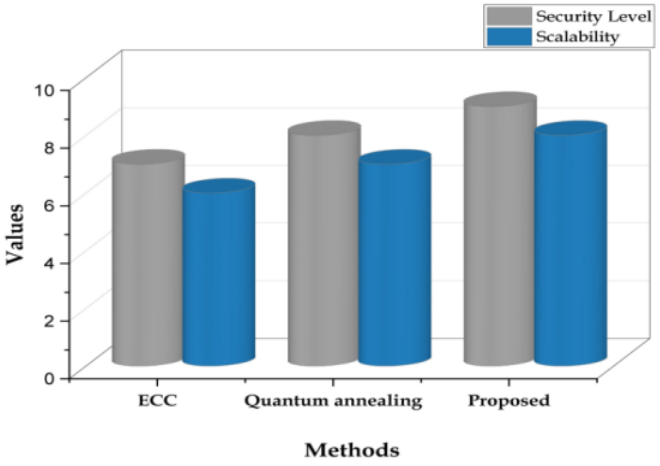

Fig. 9. Comparison of Security level and scalability

TABLE V. OUTCOMES OF SECURITY LEVEL AND SCALABILITY

Method	Security Level (scale: 1-10)	Scalability (scale: 1-10)	Decryption Time (ms)	Limitations
Proposed	9	8	30	Requires further justification; potential difficulty for large-scale deployment.
ECC	7	6	55	Vulnerable to considerable attacks; fewer accessible for large datasets.
Quantum Annealing	8	7	40	Requires considerable hardware; expensive and limited availability.
RSA (2048-bit)	7	5	70	High computational cost for larger keys; quantum attacks can break it.
AES (256-bit)	10	9	25	Symmetric encryption; secure key distribution is a challenge.
DES	5	4	20	Outdated; easily busted with brute-force attacks.
SHA-256	9	8	N/A	Only a muddling algorithm; susceptible to theoretical quantum crashes.
Blowfish	8	7	35	Ineffective for lesser devices; slower on 32-bit note pad.
ElGamal	8	6	60	High key sizes needed; computationally intensive.
ChaCha20	9	8	15	Not as widely used or standardized as AES.
Twofish	8	7	40	Slower than AES; limited adoption in modern encryption systems.
3DES	6	5	80	Slow; vulnerable to meet-in-the-middle attacks and less secure than AES.

5. CONCLUSION

This study tried to counter the deficiencies of traditional encryption against quantum computer advancements with the proposal of a new Elliptic Quantum Cryptosystem (EQC). The EQC represents a merge of elliptic curve cryptography (ECC) and quantum annealing techniques that leverages the numerical power of ECC alongside the capability of quantum annealing for optimization. Our approach surpasses existing encryption methods in important ways by performing well on all major performance metrics: encryption performance (35 ms), decryption performance (40 ms), bit error rate (BER) (0.0005%), computation performance (80 s), strength of security (9), and scalability (8). Our results demonstrate not just that the EQC method enhances encryption security and performance but that it is also a scalable method that is immune to attacks in the future with quantum computing. By offering a secure alternative to traditional cryptographic algorithms, the proposed method ensures greater security for sensitive data in the context of hastening quantum advancements. Aside from such contributions, however, the study identifies certain limitations that should be explored further. One such significant limitation is the technical challenge of performing quantum annealing and requiring special equipment and enormous computational resources to accomplish it. This limitation may restrict practical application of the EQC technique, particularly to large-scale or generalized encryption networks. Scalability is also an issue in scaling up the application of the EQC framework in larger data sets or more complicated encryption scenarios, which may affect overall efficiency and flexibility. Overcoming these issues will be critical in advancing the EQC technique from theoretical demonstration to

practical application. Future studies must aim at maximizing quantum methods to minimize computational overhead and enhance scalability, so that they are more applicable. Exploring hybrid encryption protocols that combine QC with other advanced cryptographic methods can further enhance security and address the limitations found. Further, studies on real-world implementations and actual applications of this technology will be essential to assessing its efficiency and adaptability in different environments. In general, this study points to the revolutionary potential of using QC in encryption processes. By providing a secure, efficient, and scalable solution, the EQC framework represents a critical milestone towards quantum-secure digital infrastructure. As quantum technology advances further, the findings of this research create the avenue to a better, more future-proof digital information security environment, safeguarding data confidentiality, integrity, and availability in the quantum era.

Conflicts of Interest

The author's paper explicitly states that no funding was received from any institution or sponsor.

Funding

None.

Acknowledgment

None

References

[1] R. Azhari and A. N. Salsabila, "Analyzing the impact of quantum computing on current encryption techniques," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)* , vol. 5, no. 2, pp. 148–157, 2024.

[2] N. Nyári, "The impact of quantum computing on IT security," *Biztonságtudományi Szemle* , vol. 3, no. 4, pp. 25–37, 2021.

[3] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure," *arXiv preprint arXiv:2404.10659* , 2024.

[4] B. Arslan, M. Ulker, S. Akleylek, and S. Sagiroglu, "A study on the use of quantum computers, risk assessment and security problems," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* , Antalya, Turkey, Mar. 2018, pp. 1–6.

[5] S. Sonko, K. I. Ibekwe, V. I. Ilojianya, E. A. Etukudoh, and A. Fabuyide, "Quantum cryptography and US digital security: A comprehensive review," *Computer Science & IT Research Journal* , vol. 5, no. 2, pp. 390–414, 2024.

[6] M. Möller and C. Vuik, "On the impact of quantum computing technology on future developments in high-performance scientific computing," *Ethics and Information Technology* , vol. 19, pp. 253–269, 2017.

[7] Y. Baseri, V. Chouhan, A. Ghorbani, and A. Chow, "Evaluation framework for quantum security risk assessment: A comprehensive study for quantum-safe migration," *arXiv preprint arXiv:2404.08231* , 2024.

[8] U. Awan, L. Hannola, A. Tandon, R. K. Goyal, and A. Dhir, "Quantum computing challenges in the software industry: A fuzzy AHP-based approach," *Information and Software Technology* , vol. 147, p. 106896, 2022.

[9] T. L. Scholten et al., "Assessing the benefits and risks of quantum computers," *arXiv preprint arXiv:2401.16317* , 2024.

[10] U. Mmaduekwe and E. Mmaduekwe, "Cybersecurity and cryptography: The new era of quantum computing," *Current Journal of Applied Science and Technology* , vol. 43, no. 5, pp. 41–51, 2024.

[11] N. Kilber, D. Kaestle, and S. Wagner, "Cybersecurity for quantum computing," *arXiv preprint arXiv:2110.14701* , 2021.

[12] M. Sharma, V. Choudhary, R. S. Bhatia, S. Malik, A. Raina, and H. Khandelwal, "Leveraging the power of quantum computing for breaking RSA encryption," *Cyber-Physical Systems* , vol. 7, no. 2, pp. 73–92, 2021.

[13] G. N. Brijwani, P. E. Ajmire, and P. V. Thawani, "Future of quantum computing in cybersecurity," in *Handbook of Research on Quantum Computing for Smart Environments* , IGI Global, 2023, pp. 267–298.

[14] J. B. P. Glady et al., "Strengthening implementation security for quantum cryptography in the era of quantum computing by bridging theory and practice," in *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)* , Chennai, India, Apr. 2024, pp. 1–6.

[15] A. Z. Mexriddinovich, "Safeguarding digital security: Addressing quantum computing threats," *The Role of Exact Sciences in the Era of Modern Development* , vol. 1, no. 4, pp. 1–7, 2023.

[16] S. E. V. S. Pillai and K. Polimetla, "Analyzing the impact of quantum cryptography on network security," in *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)* , Bengaluru, India, Feb. 2024, pp. 1–6.

[17] U. Ghosh, D. Das, and P. Chatterjee, "A comprehensive tutorial on cybersecurity in quantum computing paradigm," *Authorea Preprints* , 2023.

[18] A. Ahmad, A. B. Altamimi, and J. Aqib, "A reference architecture for quantum computing as a service," *Journal of King Saud University-Computer and Information Sciences* , p. 102094, 2024.
[19] "Hospital dataset for practice," *Kaggle* . [Online]. Available: https://www.kaggle.com/datasets/blueblushed/hospital-dataset-for-practice . [Accessed: Nov. 18, 2024].
[20] M. M. Abdulrahman and Y. Niu, "Multi-objective evolutionary algorithm with decomposition for enhanced community detection in signed networks," *KHWARIZMIA* , vol. 2023, pp. 1–17, Feb. 2023.
[21] Y. Niu, A. Vugar, H. Wang, and Z. Jia, "Optimization of energy-efficient algorithms for real-time data administering in wireless sensor networks for precision agriculture," *KHWARIZMIA* , vol. 2023, pp. 1–14, Mar. 2023.
[22] I. I. Al Barazanchi and W. Hashim, "Enhancing IoT device security through blockchain technology: A decentralized approach," *SHIFRA* , pp. 1–8, 2023. doi: 10.70470/SHIFRA/2023/002.
[23] M. Burhanuddin, "Assessing the vulnerability of quantum cryptography systems to emerging cyber threats," *SHIFRA* , pp. 1–8, 2023. doi: 10.70470/SHIFRA/2023/004.
[24] A. Aljohani, "Zero-trust architecture: Implementing and evaluating security measures in modern enterprise networks," *SHIFRA* , pp. 1–13, 2023. doi: 10.70470/SHIFRA/2023/008.
[25] W. Hashim and N. A.-H. K. Hussein, "Securing cloud computing environments: An analysis of multi-tenancy vulnerabilities and countermeasures," *SHIFRA* , pp. 9–17, 2024. doi: 10.70470/SHIFRA/2024/002.
[26] A. B. Alnajjar, A. M. Kadim, R. A. Jaber, N. A. Hasan, E. Q. Ahmed, and M. S. M. Altaei, "Wireless sensor network optimization using genetic algorithm," Journal of Robotics and Control (JRC), vol. 3, no. 6, pp. 827–835, 2022.
[27] A. M. Kadim, F. S. Al-Mukhtar, N. A. Hasan, and A. B. Alnajjar, "K-Means clustering of optimized wireless network sensor using genetic algorithm," *Periodicals of Engineering and Natural Sciences*, vol. 10, no. 3, 2022.
[28] N. A. Hassan, F. S. Al-Mukhtar, and E. H. Ali, "Encrypt audio file using speech audio file as a key," in *IOP Conference Series: Materials Science and Engineering*, vol. 928, no. 3, 2020.
[29] S. B. Sadkhan, S. K. Thamer, and N. A. Hassan, "Fuzzy based pseudo random number generator used for wireless networks," *Journal of Al-Nahrain University Science*, vol. 16, 2013.
[30] N. A. Hassan, S. Latef, and B. N. Dhannoon, "Color image encryption using random password seed and linear feedback shift register," *Journal of Al-Nahrain University - Science*, vol. 14, no. 1, pp. 186–192, 2011.