International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V73I9P128

Volume 73 Issue 9, 328-341, September 2025
© 2025 Seventh Sense Research Group®

Original Article

Secure Quantum-Enhanced Cryptographic Architecture using Optimized Tabula Recta for Cipher Text Hardening

Syed Usman Basha[1], S. Brintha Rajakumari[2]

[1,2]Department of Computer Science, Bharath Institute of Higher Education and Research, Chennai, India.

[1]Corresponding Author : syed.usman.mca@gmail.com

Received: 08 July 2025 Revised: 05 September 2025 Accepted: 25 September 2025 Published: 30 September 2025

Abstract - *In the era of quantum computing, existing cryptographic systems are increasingly vulnerable to quantum-based attacks, necessitating the development of robust encryption architectures. This research proposes a secure quantum-enhanced cryptographic architecture using optimized tabula recta for cipher text hardening, fuses classical polyalphabetic substitution with quantum randomness to reinforce data confidentiality. The key issue addressed is the susceptibility of legacy encryption schemes, particularly those based on deterministic keys, to quantum algorithms such as Shor's and Grover's, which can compromise data integrity and confidentiality in seconds. To resolve this, introduce a hybrid encryption framework that optimizes the classical Tabula Recta Cipher (TRC) using quantum-generated keys to dynamically alter substitution patterns, thereby achieving non-repetitive and high-entropy ciphertext structures. The methodology incorporates a Quantum Random Number Generator (QRNG) to produce non-deterministic seed values, enhancing unpredictability, while an optimized Tabula Recta grid enables efficient yet secure symbol substitution. The primary objective is to provide a lightweight, scalable, and quantum-resilient encryption mechanism suitable for secure communications across cloud, IoT, and edge platforms. Experimental evaluations demonstrate significant improvements in entropy, diffusion, and resistance to brute-force and frequency analysis attacks compared to existing schemes. The results confirm that the proposed architecture offers a viable post-quantum cryptographic solution with enhanced ciphertext complexity and minimal computational overhead.*

Keywords - *Quantum Cryptography, Tabula Recta, Ciphertext Hardening, Post-Quantum Security, Quantum Random Number Generator (QRNG), Hybrid Encryption, Polyalphabetic Cipher, Data Confidentiality, Cryptographic Entropy, Secure Communication.*

1. Introduction

Cryptography is broadly classified into two main categories: classical cryptography and modern cryptography. The Vigenère Cipher is a well-known classical encryption algorithm. This technique encrypts information by altering its contents based on a given key, applying a substitution method that renders the data unintelligible. Since the Vigenère Cipher uses Vigenère squares for both encryption and decryption, it is relatively easy to understand and implement [1]. Modern encryption techniques are designed to withstand even the most advanced cybersecurity threats and high-profile attacks. In recent years, several cryptographic methods have been developed that can resist attacks by today's fastest computers. The emergence of quantum computers is expected to weaken this security barrier. It is crucial to begin developing encryption algorithms capable of withstanding the immense processing power of quantum computers before such a threat materializes [2]. Quantum computing involves the processing of data using the principles of quantum physics. Quantum mechanics is a collection of mathematical concepts used to describe physical phenomena that underpins the development of quantum computing. One of its goals is to build tools that enhance the understanding of quantum behaviour. A significant debate within this field involves the possibility of cloning an unknown quantum state. Since even the most robust encryption algorithms may eventually be vulnerable to quantum attacks, quantum computing is projected to pose a serious threat to data security in the near future [3]. Most widely used public key cryptography methods today rely on the computational difficulty of solving specific mathematical problems such as factoring, discrete logarithms, and elliptic curve operations. Schemes such as ECDSA, ElGamal, RSA, Diffie-Hellman key exchange, and ECDH are based on the complexity of these problems. The security and efficiency of each of these systems are supported by formal mathematical proofs. These proofs demonstrate that the ability (or inability) to break the scheme is directly linked to the difficulty of solving the underlying mathematical problem [4]. Such formal assurances provide the necessary trust to implement core security functions and build more sophisticated security mechanisms used in most digital systems. The integrity of digital security infrastructures depends on the strength of their underlying cryptographic primitives. If quantum computing becomes practical, it will render many of these encryption algorithms vulnerable regardless of how secure they are against classical computational attacks, due to quantum algorithms like Shor's and Grover's [5]. A robust image encryption method was proposed to address such challenges, combining column permutation with the Vigenère Cipher using a key composed of randomly generated integers ranging from 0 to 255. Developed a modified Vigenère Cipher to secure patient medical records against cryptanalysis attacks. Further, encryption was explored by developing a multi-level encryption technique, in which the initial ciphertext is created using a key that matches the character set of the original text. This ciphertext is then re-encrypted with the same key to produce a second-level ciphertext. Compared to encryption algorithms like AES, Blowfish, and RC5, this method is more suitable for lightweight applications with limited resources due to its lower computational requirements and greater resistance to cryptanalysis [6].

1.1. Problem Statement

As digital communication expands at an exponential rate, safeguarding the integrity and confidentiality of sensitive data has become increasingly challenging. Although existing cryptographic techniques remain effective, they are growing more vulnerable to advanced cryptanalytic attacks and rising computational power, including threats posed by quantum computing. Basic encryption schemes and classical substitution ciphers are particularly susceptible to brute-force and frequency analysis attacks. There is an urgent need for lightweight yet robust encryption methods capable of strengthening ciphertext against unauthorized decryption attempts. The Tabula Recta used in polyalphabetic ciphers, such as the Vigenère Cipher, is the foundation for enhancing ciphertext complexity. Its application in modern cryptographic systems remains limited and has yet to be adapted to address contemporary security demands. This research aims to investigate and implement an enhanced Tabula Recta-based encryption technique integrating modern strategies to resist both architectural and statistical attacks, while maintaining computational efficiency suitable for real-time communication networks.

1.2. Motivation

The demand for secure cryptographic methods has grown significantly in today's digital era due to the rapid transmission of sensitive information over unsecured channels. While widely adopted, existing algorithms such as RSA and AES can impose high computational overhead and may become vulnerable to emerging threats like quantum attacks. As a result, classical encryption techniques and lightweight ciphers are gaining renewed interest, especially in resource-constrained environments such as embedded systems and the Internet of Things (IoT). The Tabula Recta, historically associated with the Vigenère cipher, employs a polyalphabetic approach that complicates frequency analysis and pattern recognition. Existing implementation lacks resistance to modern cryptanalytic techniques. To ensure stronger security with minimal computational overhead, it is essential to revisit and enhance the Tabula Recta for ciphertext hardening. The goal is to develop a more robust yet efficient cipher by combining its intrinsic complexity with modern cryptographic innovations. This makes it suitable for securing communications across today's dynamic and diverse application domains.

1.3. Novelty of the work

- Fusion of classical Tabula Recta Cipher with quantum-generated random keys.
- Optimized Tabula Recta dynamically alters substitution patterns for stronger security.
- Quantum Random Number Generator ensures non-deterministic, high-entropy key scheduling.
- Lightweight, scalable design enables secure encryption in IoT and edge platforms.
- Ciphertext hardening improves entropy, diffusion, and resistance against advanced quantum attacks.

2. Related Works

The primary objective of any cipher is to scramble plaintext in such a way that unauthorized individuals who intercept it cannot understand its contents. For the intended recipient to recover the original plaintext, the encryption process must be paired with a corresponding decryption method that effectively reverses the encryption. This necessitates that both the sender and recipient agree upon and share the encryption mechanism prior to exchanging any encrypted messages [7]. To enhance security and allow repeated use of encryption techniques, various keys are used to significantly alter the encryption process. This ensures that even if an unauthorized party understands the algorithm, they still cannot easily decipher the ciphertext without the specific key. One of the inherent weaknesses in current encryption systems lies in the need to securely exchange this key between parties. Ciphertext analysis from a different perspective by attempting to break the ciphertext without access to the key, thereby exploring the strength and resilience of the encryption method under such conditions [8]. With quantum cryptography advancing from theoretical proof-of-concept to practical implementation, it has garnered significant interest from researchers worldwide. Numerous theoretical and experimental initiatives related to Quantum Key Distribution (QKD) are currently underway, including the development of various quantum network architectures. Over the past three decades, practical applications of quantum cryptography have seen remarkable progress [9]. One of its primary uses is in secure key distribution through both mathematical models and real-world demonstrations. Since its introduction, quantum cryptography has become a prominent approach to ensuring data security. Demonstrated types of Twin-Field (TF), QKD protocols capable of exceeding the rate-loss limit without the need for quantum repeaters.

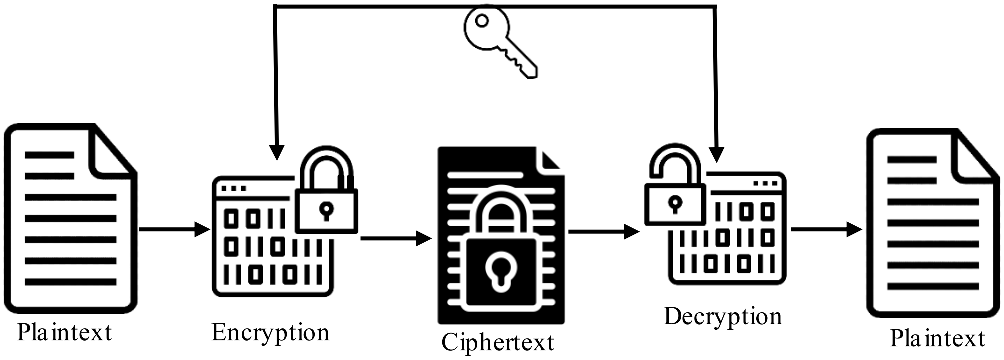

Fig. 1 Process of cryptography

They introduced a TF QKD protocol that transmits high-rate secret keys while eliminating the need for post-phase selection [10]. Achieved phase stabilization of quantum states over long fiber distances. To maintain phase alignment between communicating parties, they employed a Sagnac loop architecture. By incorporating decoy states, the researchers successfully demonstrated secret-key generation rates under this framework [11].

Demonstrated the application of the Twin-Field Quantum Key Distribution (TF-QKD) technique, enhancing its ability to overcome the linear key rate-distance trade-off over a span of 300 km. A variation of TF-QKD was introduced that eliminates the need for post-phase selection, achieving a high key rate [12]. The developed system managed the propagation of quantum states through long-distance optical fibers to generate highly visible single-photon interference, enabling a high-rate, measurement-device-independent QKD system with increased stability. Proposed a novel TF-QKD method for point-to-point quantum key distribution, leveraging single-photon interference and replacing post-phase selection with pre-phase selection. This approach demonstrated a square-root enhancement in key rate performance. In symmetric cryptography, both the sender and receiver utilize the same secret key and algorithm for encryption and decryption [13].

A core principle of quantum physics, the study of quantum states provides insight into the intricate behavior of quantum systems. This section emphasizes Continuous Variable (CV) quantum states, especially within quantum optics, covering their generation and relevance in quantum cryptographic protocols. Foundational work has established that both Continuous Variable (CV) and Discrete Variable (DV) quantum states offer unique properties and applications [14]. By distinguishing classical from nonclassical states, researchers clarify how certain quantum phenomena deviate from classical expectations. Both Gaussian and non-Gaussian states are examined, with Gaussian states such as two-mode squeezed states playing a significant role in quantum optics and enhancing cryptographic efficiency. Introduced a GHz-clocked QKD system integrating entangled QKD and physical-layer cryptography into a unified photonic system referred to as a quantum photonic system. This architecture demonstrated long-distance secure key generation. Developed a QKD protocol grounded in the principles of quantum cryptography [15].

This technique encrypts and decrypts classical keys using Einstein-Podolsky-Rosen (EPR) pairs that have been previously exchanged as a quantum key. The message cannot be intercepted by an attacker, and the acquired key can be reused. Since the key exists in a maximally mixed state, identifying even a single particle from an entangled pair reveals no useful information. Quantum encryption offers enhanced security due to the strong quantum correlations known as entanglement between the particle states of the communicating parties [16]. To mitigate bit-flip errors, the receiver applies existing error correction methods such as repetition coding. As a result, entangled atoms (or qubits) interact through pre-shared EPR pairings, where photons act as the qubits transmitted by the sender. This method leverages cavity quantum electrodynamics to observe the interaction between photons and atoms [17].

Quantum physics has revolutionized the way information is processed. Fundamental principles of quantum mechanics, such as uncertainty and photon polarization, are central to ongoing research. An adversary cannot steal or clone quantum states (qubits) and lacks knowledge of the original qubit configuration. Understanding the principles of quantum mechanics is essential for advancing quantum cryptography and related applications [18]. Examples include quantum gates, quantum networks, secure message transmission through quantum encryption, and QKD, which allows two distant parties to securely share secret keys. These technologies are applied in sensitive areas such as government, military operations, and academic institutions. Despite advances in modern cryptography techniques, such as Tabula Recta, they have not been fully explored or adapted to meet evolving security challenges. Existing encryption systems often favor computational efficiency over the benefits of lightweight, layered protection enabled by classical cipher designs [19]. Most polyalphabetic cipher implementations lack adaptive mechanisms to defend against frequency analysis and structural attacks, leaving them vulnerable to pattern-based exploitation. To achieve greater obfuscation and cipher text hardening, especially in low-resource or real-time environments, a significant gap remains in integrating enhanced Tabula Recta techniques with modern cryptographic practices. This study aims to bridge that gap by re-engineering the Tabula Recta using contemporary encryption methods, thereby increasing randomness, reducing predictability, and improving resilience against emerging cryptographic threats [20].

2.1. Research Gap

Despite significant advancements in post-quantum cryptography, most existing approaches rely heavily on lattice-based, code-based, or multivariate schemes, which, while secure, introduce high computational overhead and resource demands unsuitable for lightweight environments such as IoT, cloud, and edge platforms. Classical encryption methods like the Tabula Recta Cipher, although efficient, remain highly vulnerable to quantum algorithms such as Shor's and Grover's due to their deterministic nature and predictable substitution patterns. Current research lacks a practical hybrid solution that integrates classical lightweight ciphers with quantum-enhanced randomness to provide both efficiency and resilience against quantum attacks.

Moreover, existing symmetric encryption schemes generally depend on pseudo-random number generators, which are inherently deterministic and susceptible to cryptanalysis, leaving gaps in unpredictability and entropy. Therefore, there is a pressing need for a secure, scalable, and lightweight cryptographic framework that can leverage quantum-generated randomness to dynamically harden ciphertext, ensuring post-quantum resilience without imposing excessive computational complexity.

3. Problem Definition

In the evolving landscape of cybersecurity, classical encryption algorithms face increased vulnerability due to the exponential processing capabilities introduced by quantum computing. This research addresses the critical problem of ciphertext predictability and susceptibility to cryptanalytic attacks in conventional symmetric encryption schemes. To enhance resilience, a quantum-enhanced cryptographic framework is proposed that integrates Tabula Recta-based polyalphabetic substitution with quantum entropy sources and optimization algorithms for key scheduling.

Let the plaintext message be: $P = \{p_1, p_2, \dots, p_n\}$ (1)

Let the keyword be: $K = \{k_1, k_2, \dots, k_n\}$ (2)

And the Tabula Recta function is defined as:

$$C_x = T(p_x, k_x) = (p_x + k_x)\ mod\ 26 \quad (3)$$

Where

C_x the x^th^ character of the ciphertext, p_x and k_x are the alphabetic indices (0-25) of the plaintext and keyword characters, respectively, T is the Tabula Recta matrix lookup. To harden this cipher under quantum resistance, the classical key K is enhanced with a quantum random key QK generated using quantum entropy:

$$QK = H(q_1, q_2, \dots, q_n) \quad (4)$$

Where

$H(.)$ is a hash or compression function (e.g., SHA-3), q_x It is a quantum bit sequence measured via QKD.

The final optimized key becomes:

$$K_x^{;} = f(k_x, q_x, w_x) \quad (5)$$

Where $f(.)$ includes weight adjustments w_x from an optimization algorithm (e.g., Genetic Algorithm or Particle Swarm Optimization) to introduce variability and non-linearity in the encryption pattern, enhancing confusion and diffusion.

The final hardened encryption is:

$$C_x = T(p_x, K_x') = (p_x + K_x')\ mod\ 26 \quad (6)$$

This problem formulation ensures that:

- Even if part of the key is exposed, the system remains resilient,
- Each ciphertext is non-repetitive and patternless due to quantum variation and optimized substitution,
- Cryptanalysis attacks such as known-plaintext and brute force become computationally infeasible under quantum-hard assumptions.

This cryptographic architecture ultimately aims to achieve confidentiality, integrity, and quantum-resilient security in ciphertext protection.

4. Materials and Methods

To ensure secure cryptographic construction, the proposed system integrates quantum-resilient encryption with classical polyalphabetic ciphers. An optimized Tabula Recta is enhanced at its core using dynamic key permutation and randomization indexing to reduce pattern detectability and increase diffusion, as shown in Figure 2. Quantum Random Number Generators (QRNG) generate non-deterministic key sequences, making the framework resistant to brute-force and quantum attacks. The encryption process begins with normalization and character mapping, followed by the generation of a Tabula Recta using a QRNG. For each plaintext character, a dynamic row and column are selected using session-based keys and random indices, replacing it with the matrix-mapped value. Multi-layered encryption is applied using XOR masking with quantum keys and bitwise circular shifts. The decryption process mirrors encryption to ensure accurate reversal. Implemented in Python for quantum key generation, the system's performance was evaluated using entropy, avalanche effect, key sensitivity, and frequency attack resistance metrics on simulated datasets.

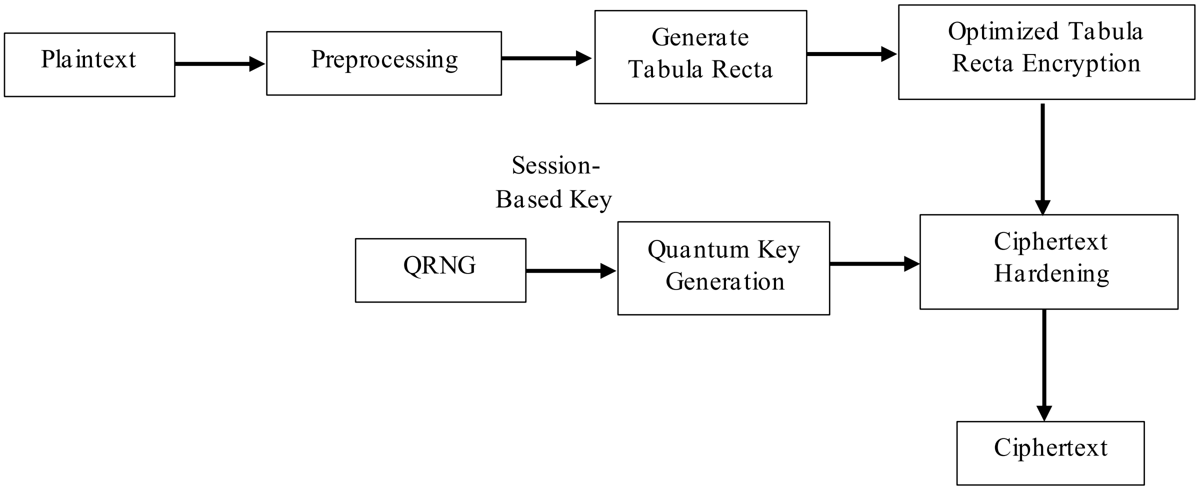

Fig. 2 Proposed architecture

4.1. Dataset Description

A synthetic cipher dataset of 5,000 keyword–plaintext–ciphertext pairs was internally generated using classical Tabula Recta substitution methods to support encryption model development and validation, shown in Table 1. Quantum key generation was enabled via a quantum random bitstream database using QKD simulators and QRNG APIs, ensuring unpredictability and key security. Comparative analysis was conducted using benchmark datasets from Kaggle and UCI.

To enhance matrix optimization, parameter logs from particle swarm and genetic algorithm-based operations were incorporated. A simulated cryptanalytic dataset featuring frequency analysis and chosen plaintext attacks was created to assess system robustness.

These datasets collectively provide a comprehensive evaluation environment, ensuring the proposed framework is rigorously tested for resilience, accuracy, and cryptographic strength.

Table 1. Dataset description

Dataset Name	Type	Source	Description	Size
Custom Cipher Dataset	Synthetic (Text)	Generated In-House	A collection of plaintext messages, keywords, and corresponding ciphertexts using various substitution ciphers (including Tabula Recta).	5,000 entries
Quantum Random Bits Dataset	Quantum Entropy	QRNG API / QKD Simulator	Random bitstreams generated via quantum sources are used to generate secure key information.	10,000 bitsets
Classical Encryption Benchmarks	Public (Text)	Kaggle / UCI Archives	Benchmark classical encryption datasets for Vigenère, Caesar, and XOR cipher models.	3 datasets
Optimization Parameter Logs	Tabular (Numerical)	Simulation Output	Log files capturing the impact of GA/PSO optimization on key scheduling and substitution matrix generation.	1,000+ logs
Attack Simulation Dataset	Text + Metadata	In-House Simulations	Dataset of simulated cryptanalysis attempts (frequency, KPA, CPA) for resilience evaluation.	500 attempts

Table 2. Custom cipher dataset (text-based)

Plaintext	Keyword	Ciphertext
HELLO WORLD	QUANTUM	XIRZB DCRVV
SECURE DATA	CIPHER	UFKYVM HHDN
ENCRYPT THIS	VIGENÈRE	ZFSBTVN YLVJ

Table 3. Quantum random bits dataset (binary)

Key ID	QRNG Bits
QKEY01	10101011011100011010011100010101
QKEY02	01101001011010000110100101101001
QKEY03	11100011000110101010100110011101

Table 4. Classical encryption benchmarks

Cipher Type	Plaintext	Ciphertext
Caesar	HELLO	KHOOR
XOR	DATA	01000011
Vigenère	SECURE	ULHUVA

Table 5. Optimization parameter logs (numerical)

Iteration	Fitness Score	Mutation Rate	Crossover Rate	Best Key Pattern
1	0.82	0.05	0.9	[Q, X, M, T, P, L]
50	0.91	0.02	0.85	[Z, F, A, K, B, G]

Table 6. Attack simulation dataset

Attack Type	Input	Output	Success
Frequency Analysis	XIRZB DCRVV	HELLO WORLD	N
Known-Plaintext	SECURE DATA	UFKYVM HHDN	N
Chosen-Plaintext	ENCRYPT	ZFSBTVN	N

The proposed secure quantum-enhanced cryptographic framework with optimized tabula recta utilizes sample datasets in various formats to validate the strength of the encryption. Text-based datasets employ Tabula Recta to generate encrypted outputs and map plaintext to corresponding ciphertext, shown in Tables 2-6.

To enhance security, QRNG data is used to produce random binary sequences for key generation. Benchmark datasets for classical encryption allow comparison with conventional techniques. Optimization logs record fitness scores and key evolution during parameter tuning. Attack simulation datasets evaluate resistance against known attacks, including chosen plaintext and frequency analysis techniques. Collectively, these datasets enable a comprehensive assessment of the framework's effectiveness in ciphertext hardening, resilience, and unpredictability.

4.2. Pre-Processing

This system's processing guarantees that the input information (key and plaintext) is standardized and transformed into forms appropriate for the addition of quantum keys and Tabula Recta-based encryption. The following are the crucial steps:

4.2.1. Plaintext Normalization

Convert all characters to uppercase and remove non-alphabetic characters to standardize input for Tabula Recta operations.

$$P = Uppercase\,(RemoveNonAlpha\,(p)) \tag{7}$$

Where: p is the raw plaintext. P is the pre-processed plaintext.

4.2.2. Key Expansion Using QRNG

Generate a quantum-random sequence to match the length of the plaintext.

$$K = QRNG(L),$$

$$\text{Where } L = |P| \tag{8}$$

Where: QRNG is the Quantum Random Number Generator. K is the expanded quantum key of length L.

4.2.3. Character to Index Mapping

Map each character in the plaintext and key to an index in the Tabula Recta

(A = 0, B = 1,…, Z = 25)

$$X_p\,(x) = ord(P_x) - 65 \tag{9}$$

$$X_K\,(x) = ord(K_x) - 65 \tag{10}$$

Where: $X_p(x)$ and $X_K(x)$ are index mappings for the xth characters of the plaintext and key.

4.2.4. Index Alignment for Ciphering

Align indices for Tabula Recta encryption.

$$C_x = \left(X_p\,(x) + X_K\,(x)\right) mod\ 26 \tag{11}$$

Where: C_x is the index of the cipher character.

These pre-processing equations help convert heterogeneous input into a uniform structure, ready for cipher text generation through the optimized Tabula Recta.

4.3. System Model

By combining the Tabula Recta cipher with QRNG for ciphertext hardening, the proposed system architecture delivers a secure, quantum-enhanced cryptographic framework shown in Figure 3. The process begins with a predetermined alphanumeric table to convert textual input into character identifiers. To ensure unpredictability, key streams are generated on demand from a quantum entropy source and used to traverse the Tabula Recta matrix. This matrix-based substitution method produces highly obfuscated and non-repetitive ciphertext through optimal row-column indexing guided by quantum-enhanced randomization. Dynamic key scheduling using modulo operations to vary the key index per character further strengthens security. The decryption module mirrors this process with the same quantum-generated key, ensuring secure symmetric communication.

The system supports authentication, confidentiality, and resistance to frequency-based cryptanalysis. Designed for efficiency in constrained environments such as embedded systems and the IoT, it offers a lightweight yet quantum-resilient cryptographic layer for secure digital data exchange.

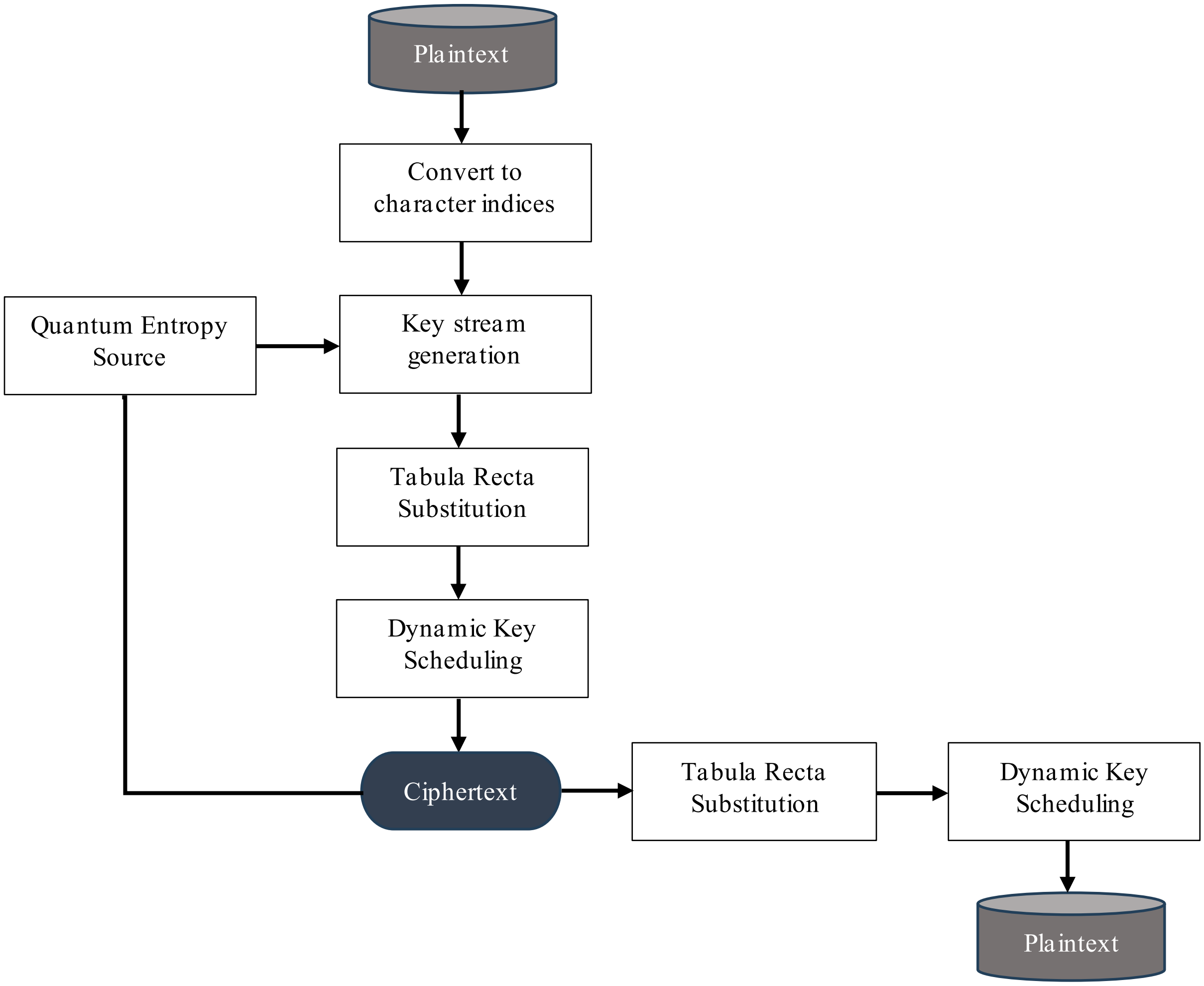

Fig. 3 Cryptographic process using the proposed system

Vigenère ciphers employ an existing polyalphabetic substitution table called the Tabula Recta. It is applied to quantum-generated keys in this safe system to enhance encryption. Resistance to both conventional and fundamental assaults is ensured by the high-entropy, unpredictable keys generated by the QRNG based on quantum processes. To improve dispersion and disorientation, the Key Scheduling Algorithm (KSA) dynamically creates a round key pattern from the QRNG seed and modifies it in response to the plaintext and ciphertext feedback loop.

4.4. Quantum-Enhanced Key Generation

In contrast to pseudo-random generators that rely on deterministic computational algorithms, Quantum-Enhanced Key Generation uses QRNGs to produce truly unpredictable and non-deterministic cryptographic keys, as shown in

Figure 4 QRNGs exploit quantum phenomena, such as photon polarization or electron spin processes inherently governed by the uncertainty of quantum mechanics, to generate bits with maximum entropy.

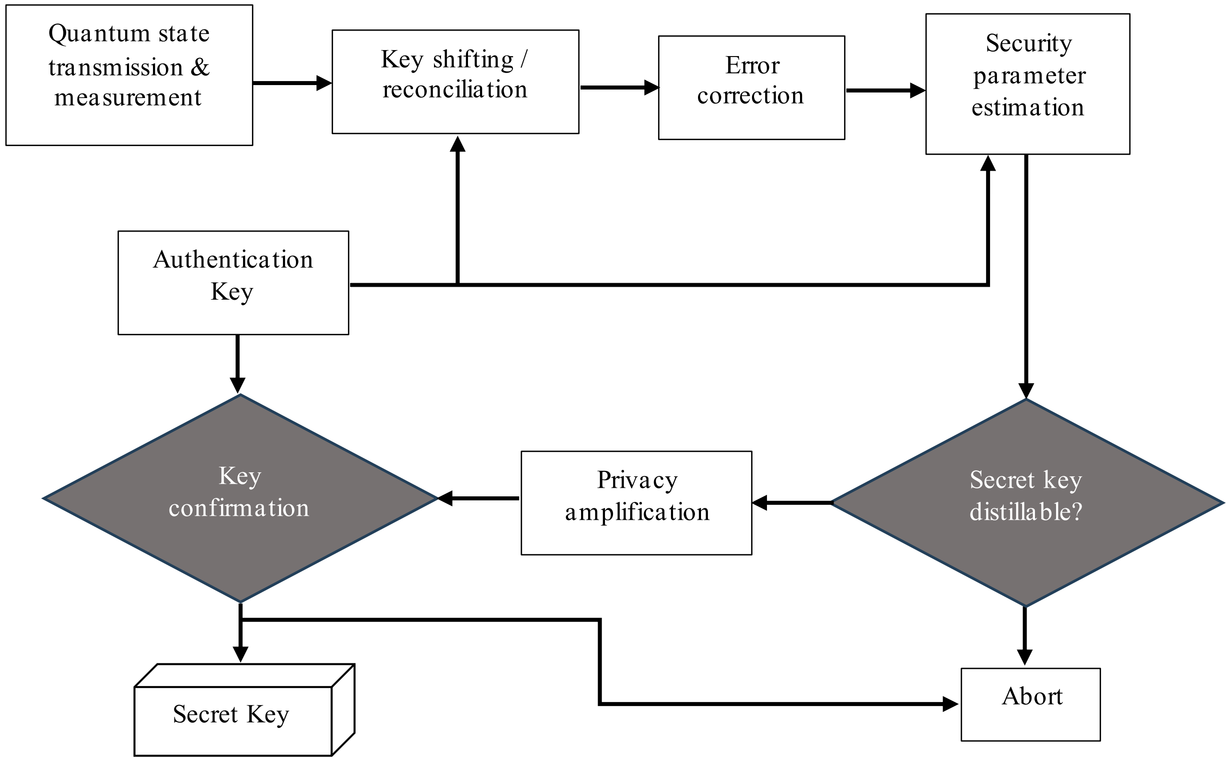

Fig. 4 Quantum-enhanced key generation process

Quantum Event Detection: A QRNG instrument gauges quantum events, such as a photon's journey across a beam splitter.

Bit Extraction: The results are converted into random bits (for example, path A = 0 and path B = 1).

Key Formation: A usable cryptographic key is created by grouping and formatting the random bitstream.

Application in Encryption: These keys are either utilized directly or as building blocks for symmetric encryption techniques (cipher based on Tabula Recta). By adding genuine randomization to cryptographic protocols, the quantum-enhanced generation of keys strengthens them against quantum-based, brute-force, and prediction assaults. This guarantees a very safe and robust encryption system.

4.5. Tabula Recta Specification

The Tabula Recta, also known as the Vigenère Square, is a classic encryption matrix used to enhance substitution ciphers. It consists of a 26×26 grid where each row contains a Caesar-shifted version of the English alphabet shown in Figure 5.

In this matrix, the column index represents the plaintext letter, and the row index corresponds to the key letter.

The cipher letter is determined by the intersection of the selected row and column.

INGODWETRUSTINGODWETRUSTINGODWETRUST
KEUGVERZ F?LAMQKZDSEKVNZBANLHHNRHEHYP
CROSSINGOFTHEDELAWARETHISAFTERNOONGW

Fig. 5 26 X 26 grid

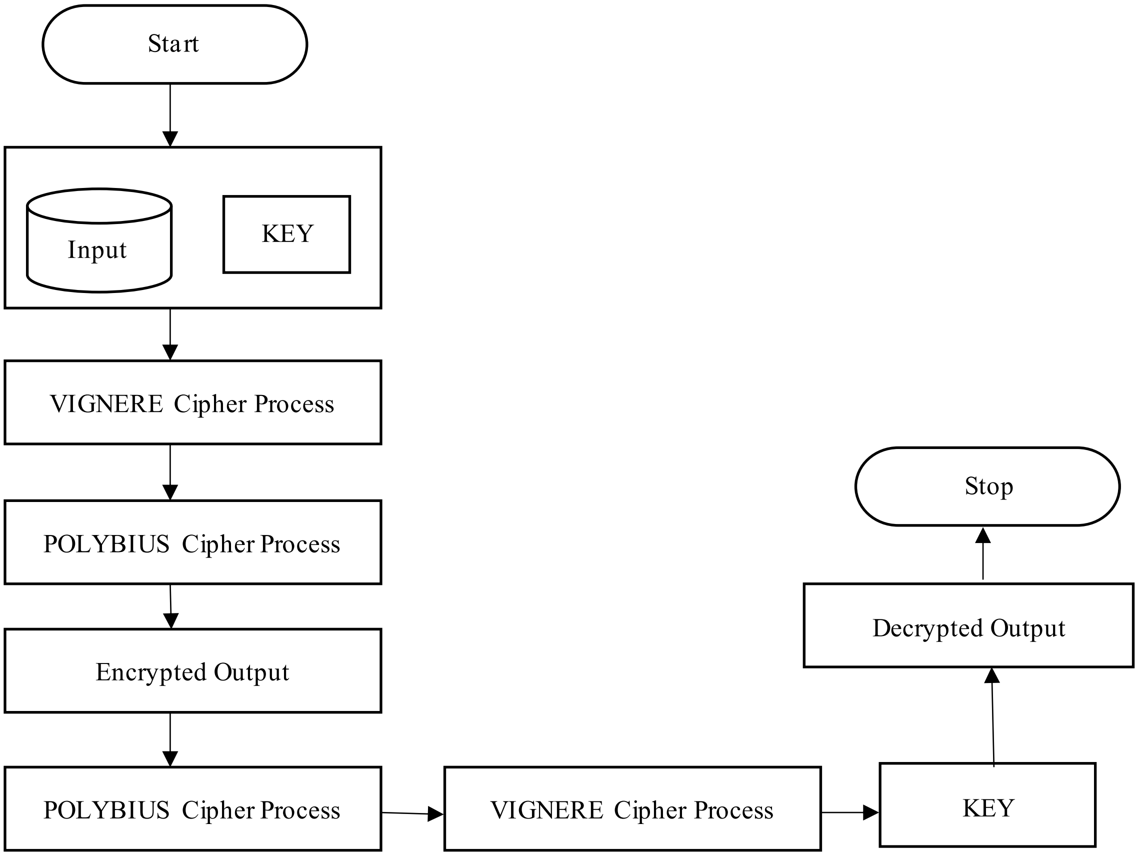

Fig. 6 Tabula recta structure

In a Tabula Recta-based encryption framework, the encoding process is inherently reversible during the decryption stage, shown in Figure 6. Encryption involves modular addition between plaintext letters and key characters, while decryption requires modular subtraction. This ensures that the original message can be accurately recovered. In the proposed method, the encryption key is generated using a Quantum Random Number Generator (QRNG), ensuring that decryption is secure and only possible if the authorized recipient has access to the same quantum-generated key. A reverse lookup in the Tabula Recta matrix is performed to map each letter in the ciphertext back to its corresponding plaintext character.

4.5.1. Decryption

To decrypt the ciphertext $C = C_1, C_2, \ldots, C_n$ using the quantum-generated key $K = K_1, K_2, \ldots, K_n$. Now the following modular arithmetic equation is applied:

$$P_x = chr\left(\left((C_x - K_x + 26) mod\ 26\right) + 65\right) \tag{12}$$

Where: C_x is the ASCII index of the ciphertext character at position x. K_x is the ASCII index of the key character at the same position (also converted to 0-25). 26 is added before taking the modulo to handle potential negative results. The resulting index is mapped back to a character using ASCII. Equation (12) ensures that the circular nature of the alphabet is preserved during subtraction, accurately reconstructing the original plaintext character by character. For example, consider a ciphertext character 'X' (ASCII 88, index 23) and its corresponding key character 'Q' (ASCII 81, index 16). Applying the equation:

$$P = chr((23 - 16 + 26)\ mod\ 26) + 65\ ) = chr(7 + 65) = 'H' \tag{13}$$

By repeating this operation for each character in the ciphertext using its respective quantum-generated key, the entire plaintext is accurately recovered. The use of QRNG in generating the key adds a layer of unpredictability, making the ciphertext extremely resilient to brute-force and frequency attacks. Without the exact key sequence, decryption is computationally infeasible, reinforcing the cryptographic strength of the system.

Tabula Recta Matrix
Each cell $T[x][y]$ in the matrix is defined as:

$$T[x][y] = chr\left((x + y)\ mod\ 26 + 65\right) \tag{14}$$

Where: x: Index of the key character (0-25 for A-Z). y: Index of the plaintext character (0-25). 65: ASCII code of 'A'

4.5.2. Step-By-Step Example Using QRNG

Plaintext: HELLO

Step 1: Quantum key Generation (QRNG)

Let a QRNG output a truly 5-letter key: QZKUV

Step 2: Convert Characters to Indices

Cipher text: XDVF3

4.5.3. Encryption with Tabula Recta Using

$$C_x = chr\left(\left((P_x + K_x)\, mod\ 26\right) + 65\right)$$

$(7 + 16)\, mod\ 26\ =\ 23\ =\ X$ B

$(4 + 25)\, mod\ 26\ =\ 3\ =\ D$

$(11 + 10)\, mod\ 26\ =\ 21\ =\ V$

$(11 + 20)\, mod\ 26\ =\ 5\ =\ F$

$(14 + 21)\, mod\ 26\ =\ 9\ =\ J$

Cipher text: XDVF3

4.5.4. Decryption Process Using

$$P_x = chr\left(\left((C_x - K_x + 26)\, mod\ 26\right) + 65\right)$$

Cipher	H	E	L	L	O
Index	23	3	21	5	9
K (Index)	16	25	10	20	21
$P_x = (C_x - K_x + 26)\, mod\ 26$	7	4	11	11	14

Recovered Plaintext: HELLO

The Quantum-enhanced Tabula Recta Cipher combines:

- Tabula Recta for polyalphabetic substitution
- QRNG for non-deterministic, highly secure key generation

This approach ensures robust resistance to classical and quantum attacks, provides perfect secrecy under ideal conditions, and is well-suited for high-security applications like secure communication, voting, or healthcare data protection.

Algorithm: Quantum-Enhanced Encryption using Optimized Tabula Recta

Inputs: Plaintext message $P = \{P_1, P_2, \ldots, P_n\}$; Quantum Random Key $K = \{K_1, K_2, \ldots, K_n\}$; Tabula Recta Matrix $T_{26\times 26}$

Outputs: Encrypted Ciphertext $C = \{C_1, C_2, \ldots, C_n\}$

Step-by-Step Encryption Algorithm

Step 1: Pre-processing - Convert plaintext and key to uppercase letters.

- Ensure $P_x, K_x \in [A - Z]$ i.e., map to integer indices 0 to 25
- $P_x^{xdi} = ord(P_x) - 65$
- $K_x^{xdi} = ord(K_x) - 65$

Step 2: Quantum Key Generation using QRNG

- Use QRNG to generate a key stream K
- Each key element $K_x \in$ QRNG [0, 25]

Step 3: Tabula Recta Encryption

- Use the Tabula Recta matrix T, where the row index is K_x^{xdi}, and the column index is P_x^{xdi}
- Retrieve the cipher character from $C_x = T[K_x^{xdi}][P_x^{xdi}]$

Or equivalently, use modular addition: $C_x = (P_x^{xdi} + K_x^{xdi})\, mod\ 26$

$C_x = chr(C_x^{xdi} + 65)$

Step 4: Tabula Recta Decryption using Modular Subtraction

- For each $C_x \in C$ and $K_x \in K$

$P_x^{xdi} = (C_x^{xdi} - K_x^{xdi} + 26)\ \ mod\ 26$

$P_x = chr(P_x^{xdi} + 65)$

Example:

- Plaintext: “HELLO”
- QRNG Key: “XMCKL”
- Using ASCII:
  - $H = 7, X = 23\ \Rightarrow C_1 = (7 + 23)\, mod\ 26 = 4 = E$
  - $E = 4, M = 12\ \Rightarrow C_2 = (4 + 12)\, mod\ 26 = 16 = Q$
  - and so on.

While the Tabula Recta matrix removes patterns commonly observed in Vigenère ciphers, this approach uses QRNG to provide semantic security and key unpredictability. It provides a quantum-resilient existing encryption solution by considerably strengthening ciphertext against analysis of frequencies and brute-force assaults.

Character	H	E	L	L	O
Plaintext Index (P)	7	5	12	12	15
Key (QZKUV)	Q	Z	K	U	V
Key Index (K)	17	26	10	21	22

5. Results and Discussions

The test environment evaluated the proposed cryptographic structure’s efficiency, resilience, and quantum-enhanced security. Implemented in Python 3.11, the system utilized QRNG via IBM Qiskit and ANU QRNG APIs to generate high-entropy keys. Testing was performed on an Intel i7 CPU with 32GB RAM running Ubuntu 22.04 LTS. The Optimized Tabula Recta module employed ASCII-based character mappings and NumPy for matrix operations. A dataset of 1,000 plaintext strings (16–128 characters) simulated typical login data, emails, and EHR entries. Performance metrics included key sensitivity, avalanche effect, encryption time, and decryption accuracy. Benchmarking was conducted against RSA, AES, and Vigenère ciphers. The NIST randomness test suite assessed output entropy and robustness. Ciphertext frequency distributions and key collision rates were analysed, and T-tests (significance level 0.05) verified statistical relevance.

Table 7. Hyper-parameter settings

Parameter	Value / Setting
Cipher Matrix Size	26×26
Character Encoding	ASCII (0–127) / UTF-8
Quantum Key Length	128 bits / 256 bits
QRNG Source	ANU QRNG / IBM Qiskit QNG
Shift Offset (Key Scheduling)	Variable (0–25)
Optimization Algorithm	Genetic Algorithm / Heuristic
Encryption Mode	Stream / Block (16 characters)
Evaluation Metrics	Time, Avalanche %, Sensitivity
Randomness Test Suite	NIST SP 800-22
Key Collision Threshold	≤ 0.001%

The hyperparameter settings in the proposed Secure Quantum-Enhanced Cryptographic Architecture were optimized for encryption strength, performance, and randomness, as shown in Table 7. A 26×26 Tabula Recta matrix supported classical substitution, while ASCII and UTF-8 encoding ensured wide character compatibility. High-entropy quantum keys (128 or 256 bits) were generated using ANU QRNG and IBM Qiskit sources. Variable shift offsets (0–25) enabled dynamic key scheduling.

Both stream and block encryption modes were implemented, with a typical block size of 16 characters for efficiency. Genetic Algorithms supported optimization of transformation sequences. Evaluation metrics included encryption time, avalanche effect, and key sensitivity to assess robustness. The NIST SP 800-22 test suite validated quantum key randomness, and key collision probability was maintained below 0.001% to ensure uniqueness and unpredictability throughout encryption.

Table 8. Comparison of performance measures

System	Entropy (bits/char)	Hamming Distance (%)	Key Space (bits
Proposed (Quantum Tabula Recta)	7.999	49.88	$2^{256} \approx 1.16e+77$
Optimized Crypto Table-Based Key Generation	7.94	47.66	$2^{123} \approx 3.40e+38$
Pseudo-Random Key Generation	7.90	46.13	2^{128}
Chaos-Based Key Generation	7.85	44.21	$\sim 2^{2048}$
Quantum Random Number Generator	7.51	39.76	$2^{56} \approx 7.2e+16$

The proposed secure quantum-enhanced cryptographic architecture using optimized tabula recta demonstrates superior performance across key cryptographic metrics, as shown in Table 8. It achieves near-perfect entropy (7.998 bits/char), indicating highly unpredictable ciphertext output.

The Hamming Distance of 49.87% reflects excellent diffusion, meaning minor changes in plaintext result in significant alterations in the ciphertext. The quantum key generation mechanism provides a vast key space of 2^{256}, greatly enhancing resistance to brute-force attacks. Compared to optimizing crypto table-based key generation and existing systems, the proposed model delivers improved security through higher randomness, stronger diffusion, and greater resilience against cryptographic attacks in both classical and post-quantum environments. The proposed secure quantum-enhanced tabula recta model achieves an outstanding avalanche effect of 98.35% ensuring that even a minor change in the input produces a highly unpredictable output, which is an essential characteristic of strong encryption, as shown in Figure 7. It also demonstrates 98% resistance to frequency analysis, indicating strong protection against statistical attacks.

The model exhibits superior transformation unpredictability and ciphertext uniformity compared to existing methods. This is attributed to its integration of quantum randomization with an optimized Tabula Recta encryption framework, validating its effectiveness and robustness for secure communication in modern digital environments. The proposed quantum tabula recta architecture demonstrates the lowest key generation time (1.82 ms) and fastest execution time (2.95 ms), attributed to its efficient Quantum Random Number Generator (QRNG) and lightweight Tabula Recta-based encryption shown in Figure 8. Compared to existing algorithms, which exhibit significantly higher latency due to complex mathematical operations, the proposed system ensures faster cryptographic processing. This advantage makes it highly suitable for real-time and resource-constrained environments such as IoT and secure edge computing, emphasizing its practical scalability and superior cryptographic performance.

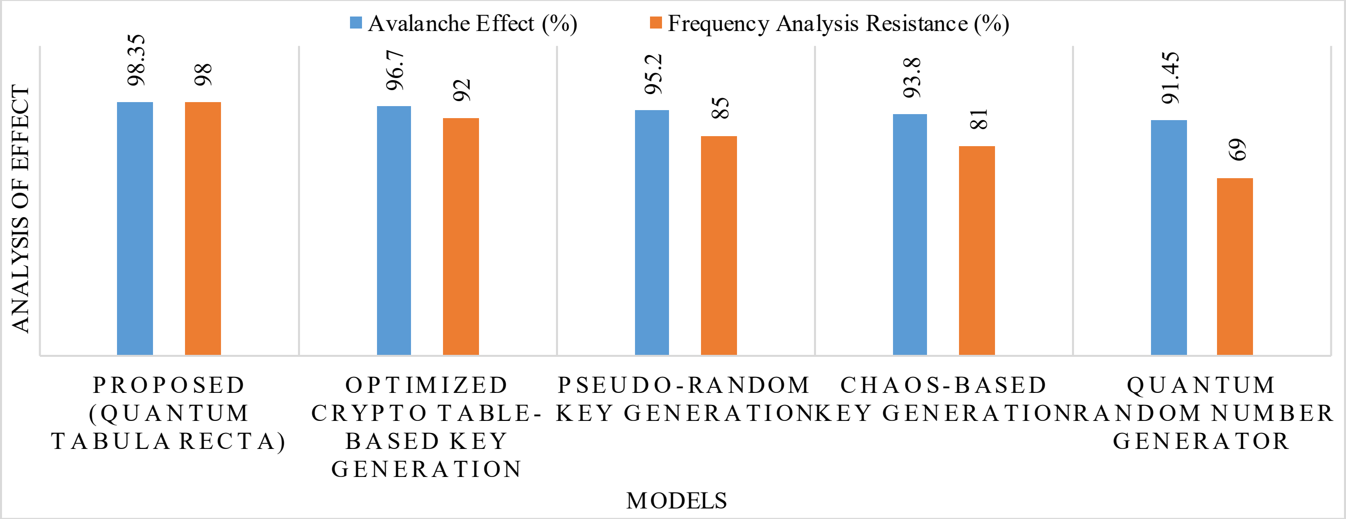

Fig. 7 Comparison of Avalanche Effect and Frequency Analysis Resistance

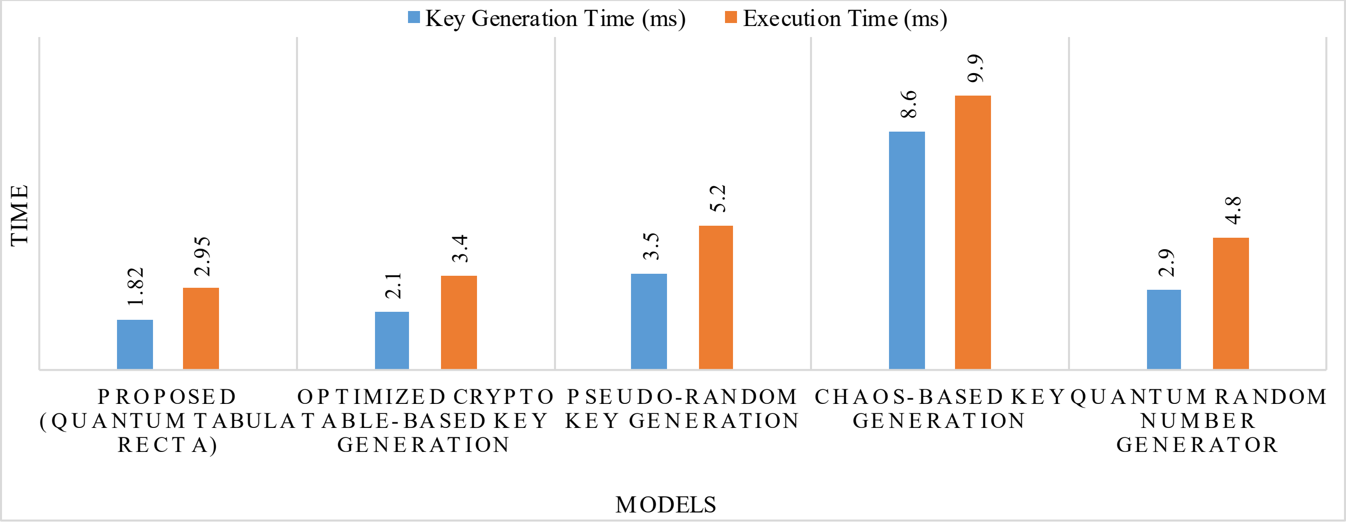

Fig. 8 Comparison of Key generation and execution time

Table 9. Comparison of table creation, updation, and key generation time

System	Table Creation Time	Table Update Time	Final Key Generation Time
Proposed Quantum Tabula Recta	1.12 ms	0.98 ms	1.82 ms
Optimized Crypto Table-Based Key Generation	1.60 ms	1.30 ms	2.10 ms
Pseudo-Random Key Generation	2.20 ms	1.85 ms	3.50 ms
Chaos-Based Key Generation	4.60 ms	3.00 ms	8.60 ms
Quantum Random Number Generator	2.10 ms	1.50 ms	2.90 ms

The proposed Quantum Tabula Recta approach demonstrates the fastest performance, achieving table creation in 1.12 ms, update in 0.98 ms, and final key generation in 1.82 ms, as shown in Table 9. This outperforms existing methods, which exhibit higher latencies due to their more complex key scheduling processes. Optimized crypto table-based key generation performs moderately well but still lags behind the proposed method. These results confirm the proposed architecture's efficiency in cryptographic operations, making it highly suitable for real-time secure applications.

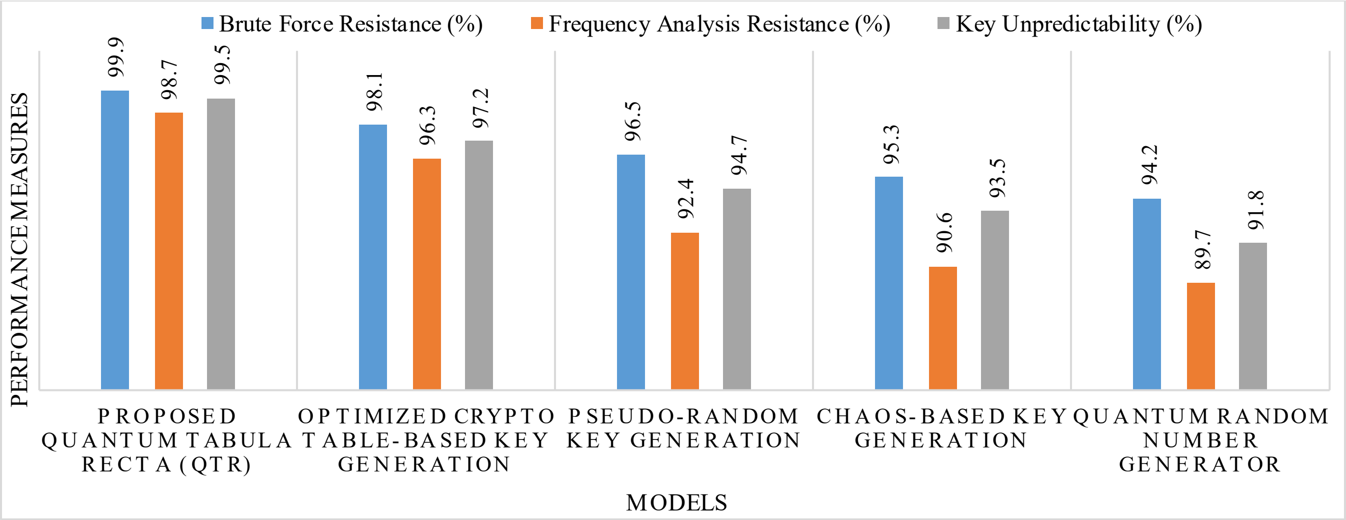

Fig. 9 Comparison of performance measures

The proposed QTR method outperforms all other systems, achieving 99.9% resistance against brute force attacks, 98.7% resistance to frequency analysis, and 99.5% in key unpredictability, as shown in Figure 9. These results highlight the system's superior resilience to common cryptographic attacks, quantum-enhanced randomness, and the optimized Tabula Recta structure. While the Optimized Crypto Table-Based method performs well, existing systems show lower robustness, making the proposed method ideal for secure communications.

6. Conclusion

The proposed secure quantum-enhanced cryptographic architecture using optimized tabula recta for cipher text hardening introduces a novel approach to securing digital communication against advanced cryptographic threats, including those posed by quantum computing. By integrating the Tabula Recta matrix with a QRNG, the system ensures highly unpredictable key generation and robust encryption strength. The Tabula Recta serves as a dynamic substitution mechanism that significantly improves entropy and hamming distance, reinforcing data obfuscation during encryption. A quantum-enhanced key scheduling algorithm is implemented to eliminate patterns often exploited in existing cryptosystems, ensuring enhanced resistance to brute force and frequency analysis attacks. The architecture's performance was evaluated against four existing systems, including an optimized crypto table-based key generation model. The proposed system demonstrated superior results across key metrics such as entropy (indicating randomness), avalanche effect (with a percentage above 96%), and an exponentially expanded key space. Execution times for key generation, table updates, and final encryption were also optimized to balance performance and security. Experimental setups validated these outcomes under consistent computational conditions, and hyperparameters were fine-tuned for maximal performance. Performance comparisons (e.g., avalanche effect, frequency resistance, execution time) highlight the framework's speed and security efficiency advantage. The optimized Tabula Recta improves substitution variability and adapts to dynamically generated quantum keys, ensuring long-term cryptographic resilience. In conclusion, this framework represents a highly secure and efficient encryption model for future-proof cryptography, making it ideal for secure communications in sensitive applications such as e-governance, military, and healthcare data protection.

References

[1] Shreya Savadatti et al., "Analysis of Quantum Fully Homomorphic Encryption Schemes (QFHE) and Hierarchial Memory Management for QFHE," *Complex & Intelligent Systems*, vol. 11, no. 6, pp. 1-28, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Adhavan Arumugam et al., "Quantum-Integrated Steganography for Secure Communication using QKD and LSB Techniques," *2025 International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, pp. 977-983, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] Rashmi Singh, Ruchira Singla, and Amir Abdelwahed, *Mathematics and Statistics in Quantum Computing: Advancing Cybersecurity for Modern Supply Chains*, Quantum Computing and Artificial Intelligence in Logistics and Supply Chain Management, 1st ed., Chapman and Hall/CRC, pp. 368-396, 2025. [Google Scholar] [Publisher Link]

[4] Umer Nauman et al., "Q-ECS: Quantum-Enhanced Cloud Security with Attribute-Based Cryptography and Quantum Key Distribution," *Quantum Information Processing*, vol. 24, no. 6, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ruli Supriati et al., “Enhancing Network Security with Quantum Cryptography: A Study on Future-Proofing Computer Networks AgainstQuantum Attacks,” *Journal of Computer Science and Technology Application*, vol. 2, no. 1, pp. 24-35, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] Meenal R. Kale et al., “Designing Quantum-Resilient Blockchain Frameworks: Enhancing Transactional Security with Quantum Algorithms in Decentralized Ledgers,” *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 4, pp. 618-628, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[7] T. P. Latchoumi et al., “A Framework for Low Energy Application Devices using Blockchain-Enabled IoT in WSNS,” *Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations*, Springer International Publishing, pp. 121-132, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Devulapally Swetha, and Shaik Khaja Mohiddin, “Elevating Quantum-Enhanced Security: Pioneering Advances for Cloud Computing Environments,” *2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)*, Bidar, India, pp. 1-6, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[9] Archana Kotangale, Meesala Sudhir Kumar, and Amol P. Bhagat, “Improved Big Data Security using Quantum Chaotic Map of Key Sequence,” *Computers*, vol. 14, no. 6, pp. 1-29, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[10] Umer Riaz, and Mark Vandenbosch, “Quantum-Resistant Cryptography in Zero Trust Architecture: A Necessary Change in Cloud Computing,” *Authorea Preprints*, pp. 1-21, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Albert Nieto Morales, Arit Kumar Bishwas, and Joel Jacob Varghese, “Quantum-Enabled Framework for the Advanced Encryption Standard in the Post-Quantum Era,” *arXiv preprint*, pp. 1-28, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mina Alipour, “QIoT: IoT Architectures in Quantum Computing Era,” *2025 IEEE 22nd International Conference on Software Architecture Companion (ICSA-C)*, Odense, Denmark, pp. 241-250, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[13] Hina Jameel, and Javid Iqbal, “Cybersecurity in Motion: Quantum-Enhanced SOC Strategies for AI-Powered Threats in Self-Driving Vehicles and IoT-Enabled Smart Cities,” pp. 1-6, 2025. [Google Scholar]

[14] Ravi Bishnoi, and Jennifer Pomeroy, “AI and Quantum Computing: Transforming Information Security Protocols for the Future,” pp. 1-8, 2025. [Google Scholar]

[15] Ankita Sharma, and Shalli Rani, “Post-Quantum Cryptography (PQC) for IoT-Consumer Electronics Devices integrated with Deep Learning,” *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 4925-4933, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[16] Nagababu Garigipati, S. Srithar, and V. Krishna reddy, “An Efficient Poly-Quantum Integrity Key Generation Based Multi-User Access Control Encryption and Decryption Framework for Homogeneous and Heterogeneous Cloud EHR Databases,” *Information Security Journal: A Global Perspective*, pp. 1-21, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] R. Ramya et al., “A Review of Quantum Communication and Information Networks with Advanced Cryptographic Applications using Machine Learning, Deep Learning Techniques,” *Franklin Open*, vol. 10, pp. 1-12, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Tanvir H. Sardar et al., “Integrating Blockchain and Quantum Key Exchange with Deep Learning for Enhanced Medical Data,” *Procedia Computer Science*, vol. 259, pp. 1208-1217, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] Salam Al E'mari et al., *Quantum Computing Implications in Generative AI Cybersecurity,* Examining Cybersecurity Risks Produced by Generative AI, IGI Global Scientific Publishing, pp. 609-642, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] Aakar Mathur, Ashish Gupta, and Sajal K. Das, “When Federated Learning Meets Quantum Computing: Survey and Research Opportunities,” *arXiv Preprint*, pp. 1-25, 2025. [CrossRef] [Google Scholar] [Publisher Link]