International Journal of Innovative Research and Scientific Studies, 8(4) 2025, pages: 156-166

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

QR-DEF: A quantum-resistant hybrid encryption framework with dynamic entropy fusion and biomimetic obfuscation

Rami Almatarneh[1], Mohammad Aljaidi[2], Ayoub Alsarhan[3], Amjad A. Alsuwaylimi[4*]

[1]*Department of Cybersecurity, Faculty of Information Technology, Zarqa University, Zarqa 13110, Jordan.*
[2]*Department of Computer Science, Faculty of Information Technology, Zarqa University, Zarqa 13110, Jordan.*
[3]*Dept of Information Technology, Faculty of Prince Al-Hussein Bin Abdallah II for Information Technology, The Hashemite University, Zarqa, Jordan.*
[4]*Department of Computer Science, College of Science, Northern Border University, Arar, Saudi Arabia.*

Corresponding author: Amjad A. Alsuwaylimi (*Email: amjad.alsuwaylimi@nbu.edu.sa*)

Abstract

The growing threat of quantum computing has increased the need for cryptographic frameworks that go beyond classical cryptographic paradigms. Quantum-Resistant Dynamic Entropy Fusion (QR-DEF) is a new hybrid encryption paradigm that integrates lattice-based cryptography, dynamic environmental entropy, and bio-inspired obfuscation to mitigate vulnerabilities in post-quantum and classical paradigms. QR-DEF employs the NTRU lattice-based cryptosystem to create a static Shor's algorithm-resistant "Master Seed" and pulls dynamic entropy from fixed public parameters (e.g., blockchain nonces, weather) to create ephemeral session keys via a chaotic neural network. This combination ensures quantum resilience and forward secrecy without re-encryption overhead. Additionally, the post-encryption DNA-like substitution layer (DNA-LS) adds another level of complexity to the ciphertext through codon mapping and permutation, making frequency analysis more complicated. Benchmarks on an Intel i7-12700K demonstrate QR-DEF's operational efficacy, recording 1.92 Gbps throughput and 5.2 ms latency for 1KB payloads, which is similar to RSA-2048 but with a 60% faster key exchange. The 256-bit ChaCha20-Poly1305 layer in the framework elevates Grover's attack complexity to O(2^128), and blockchain-attested parameters ensure tamper-proof entropy sourcing. Although incurring a 15–20% performance overhead over native NTRU+ChaCha20, QR-DEF's layered security justifies the exchange: DNA-LS obfuscation inflates adversary costs by 33%, and dynamic parameters prevent key reuse risks. Scalability testing showed uniform throughput (1.85 Gbps) for payloads of 1MB, with energy efficiency (0.012 J/operation) being twice that of RSA-2048. QR-DEF's innovations (decentralized entropy feeding, chaotic mixing, and biomimetic confusion) establish a blueprint for adaptable and quantum-insurance cryptography. Harmonizing lattice-based security with environmental uncertainty will effectively bridge the gap between theoretical post-quantum abstractions and practical resiliency, thus offering a strong solution for IoT, distributed systems, and high-risk communications in the post-quantum age.

Keywords: Biomimetic obfuscation, Dynamic entropy sourcing, Hybrid encryption framework, Lattice-based encryption, Post-quantum cryptography.

DOI: 10.53894/ijirss.v8i3.7747
Funding: This study received no specific financial support.
History: Received: 22 April 2025 / **Revised:** 26 May 2025 / **Accepted:** 27 May 2025 / **Published:** 11 June 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Acknowledgment: The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, Saudi Arabia for funding this research work through the project number "NBU-FFR-2025-1197-03".
Publisher: Innovative Research Publishing

1. Introduction

As quantum processing advances and cyber threats become even more sophisticated, the demand for secure encryption tools has never been more urgent. Both RSA and ECC, traditional encryption techniques, face serious risks due to quantum algorithms like Shor's and Grover's, which could potentially render such traditional public-key infrastructure useless [1].

While post-quantum cryptography (PQC) solutions, such as lattice-based algorithms, show promise, their static nature and reliance on fixed parameters make them vulnerable to evolving attack techniques and the depletion of entropy over time [2]. In this paper, we propose a new hybrid encryption framework (Quantum-Resistant Dynamic Entropy Fusion (QR-DEF)) that overcomes these limitations by combining lattice-based cryptography, dynamic environmental entropy, blockchain-verified parameters, and bio-inspired DNA obfuscation.

The growing threat of quantum computing breaking classical encryption has spurred significant research into post-quantum cryptography (PQC). The National Institute of Standards and Technology (NIST) has already developed lattice-based schemes such as Kyber and NTRU, which have been proven to be quantum-resistant [3]. These schemes, nevertheless, remain vulnerable since they are based on static keys and deterministic randomness, introducing single points of failure. For example, lattice-based schemes depend on the difficulty of the Learning With Errors (LWE) problem, but improvements in quantum annealing or algorithmic optimization could weaken this security over time [4]. For instance, lattice schemes rely on the hardness of the Learning With Errors (LWE) problem, yet quantum annealing or algorithmic optimization advances can potentially undermine this security in the future [4].

Additionally, entropy sources used in conventional systems, such as pseudorandom number generators (PRNGs) are prone to manipulation or predictability, especially in adversarial contexts [5].

Recent studies emphasize the importance of dynamic entropy infusion to improve cryptographic flexibility. For instance, Ohya and Petz [6] proved that incorporating time-varying parameters would be able to address weaknesses attributable to key reuse. Blockchain technology, purportedly providing data integrity in distributed environments, has even been considered for verifying cryptographic parameters, although this application remains largely underdeveloped [7]. Additionally, bio-inspired approaches such as DNA-based encoding have been shown to be viable for incorporating non-linear confusion into ciphertexts and thereby making them more resistant to pattern recognition [8]. QR-DEF integrates these concepts into a cohesive framework that addresses issues related to adaptability, entropy freshness, and quantum resilience. QR-DEF integrates these concepts into a cohesive framework that addresses issues related to adaptability, entropy freshness, and quantum resilience.

QR-DEF is especially suited for high-stakes environments such as IoT networks, financial systems, and government communications, where maintaining key longevity and ensuring entropy freshness are critical. Its hybrid structure combines the computational efficiency of symmetric encryption with the forward secrecy of post-quantum asymmetric exchanges. Additionally, the use of bio-inspired obfuscation opens up new possibilities for cross-disciplinary research in cryptography.

To the best of our knowledge, previous work in post-quantum cryptography has largely overlooked key limitations, such as the static entropy reliance on fixed parameters or pseudorandom number generators (PRNGs) that create single points of failure [5, 9], the fragmented integration of dynamic entropy with quantum-resistant primitives that prioritizes backward compatibility over robust security [10, 11] and the underutilization of bio-inspired obfuscation to deter pattern recognition attacks [8]. In contrast, this work introduces the QR-DEF framework, which bridges these gaps with a hybrid architecture that integrates lattice-based cryptography, blockchain-verified dynamic entropy, chaotic neural fusion, and DNA-inspired substitution. QR-DEF eliminates static key dependence using publicly sourced parameters, such as Bitcoin nonces, while providing quantum resistance via layering of NTRU and ChaCha20-Poly130. However, these improvements could have some drawbacks, such as slightly higher computational complexity due to the chaotic neural networks and potential latency because of blockchain verification or multi-layer obfuscation.

The key contributions of this work are as follows:

- Quantum-Resistant Key Exchange via NTRU Lattices: Establishes a static "Master Seed" resistant to Shor's algorithm to ensure long-term security against potential quantum threats [3, 12].
- Employing blockchain-verified, time-bounded public parameters (e.g., financial indices, weather data) to generate ephemeral keys without synchronization overhead [13, 14].

- Combining static and dynamic parameters via a chaotic neural network to create unpredictable session keys with no training vulnerabilities [15].
- Improving ciphertext obfuscation via codon-based encoding and DEK-derived permutations to complicate frequency analysis [8].
- Integrating tamper-proof parameters, quantum-resistant layering, and entropy sustainability to adapt encryption to modern distributed environments [16, 17].

By combining these innovations, QR-DEF shifts theoretical security into practical, adaptive defense, which is a necessity in an era of rising quantum and adversarial threats.

This paper is structured as follows: Section 1 introduces the topic, Section 2 provides an overview of related work in post-quantum cryptography and dynamic entropy systems. Section 3 explains the QR-DEF architecture, and Section 4 discusses its security against quantum and classical attacks. Section 5 addresses implementation challenges and benchmarks, Section 6 outlines future work, and Section 7 presents conclusions.

2. Related Work

Establishment of quantum-resistant dynamic fusion (QR-DEF) is based on advances in two primary areas: post-quantum cryptography (PQC) and dynamic entropy systems. This section unifies foundational and modern research in these areas, explaining their strengths, limitations, and overlaps that inform QR-DEF design.

Post-quantum cryptography has emerged as the cornerstone of modern cryptography research due to the looming threat of quantum computing. Lattice-based algorithms, with their resistance to Shor's algorithm, dominate current PQC standardization. The NIST PQC standardization effort, which is currently in its fourth round, has approved lattice-based schemes such as Kyber (key encapsulation) and Dilithium (digital signatures) for balancing security and efficiency [2]. Among these, the NTRU cryptosystem, first proposed by Hoffstein et al. [3], is one such gold standard since its security is tied to the shortest vector problem (SVP) of polynomial rings, which is conjectured to be quantum-hard [12].

However, lattice-based systems are not without vulnerabilities. A recent study [4] demonstrated that advances in quantum annealing and hybrid quantum-classical algorithms may weaken SVP assumptions over time. Similarly, Ma et al. [9] showed that static key reuse in lattice-based protocols increases susceptibility to side-channel attacks, which is emphasizing the need for dynamic key refreshment mechanisms. Code-based and multivariate polynomial schemes, such as Classic McEliece and Rainbow, offer alternatives but suffer from impractical key sizes or computational overhead [18], limiting their applicability in real-time systems.

Conventional cryptosystems heavily depend on pseudorandom number generators (PRNGs) for entropy, but their deterministic nature and susceptibility to adversarial bias have spurred interest in dynamic entropy sources. Ohya and Petz [6] proposed the idea of incorporating time-varying parameters, i.e., network delay or sensor noise to introduce entropy into key generation, highly reducing predictability. Chen et al. [19] further worked on the idea and used environmental noise (i.e., temperature variations) to produce entropy, but their method was pre-shared secret-based for synchronization and hence was logistically complex.

Blockchain technology has emerged as a robust mechanism for verifying dynamic parameters. Yang et al. [14] demonstrated how blockchain timestamps and nonces provide worldwide accessible, immutable sources of entropy appropriate for decentralized environments. Sathya and Banik [13] validated the use of Bitcoin block headers as tamper-proof parameters, as well, although for authentication purposes rather than cryptographic key derivation. These pieces of work outline the as-yet untapped potential of blockchain-authenticated data to enhance entropy freshness and integrity.

Hybrid cryptographic schemes, where post-quantum and classical primitives are blended together, have been proposed as stopgap measures for quantum readiness. NIST's KEMTLS scheme, for instance, blends Kyber with the ubiquitous TLS handshakes for backward interoperability support [10]. Such approaches, however, retain static key hierarchies and, thus, are vulnerable to long-term key compromise.

Recent efforts have explored augmenting PQC with dynamic entropy, a lattice-based key exchange protocol that refreshes keys using locally generated sensor data proposed by Ravi et al. [11]. However, reliance on device-specific entropy limits its scalability. Similarly, Cheon et al. [20] integrated biometric data with lattice secrets for short-term key derivation, but biometric reproducibility brought consistency concerns. These works clearly highlighted a fundamental gap, namely the absence of a unified framework that integrates externally sourced, non-secret dynamic parameters with PQC to achieve both quantum resistance and entropy agility.

Bio-inspired cryptographic techniques, in particular DNA-based encoding, have been promising to enhance ciphertext obfuscation. Bio-inspired cryptographic techniques, in particular DNA-based encoding, have been promising to enhance ciphertext obfuscation. Gehani et al. [8] demonstrated that DNA codon substitution introduces non-linear confusion layers to make frequency analysis challenging.

Their static lookup tables, though, made the approach vulnerable to known-plaintext attacks [21-26]. Chaos theory, which comes with its intrinsic randomness, has also been utilized to enhance encryption. Kocarev [15] designed chaos-based PRNGs that generate highly random keystreams but were plagued with initial seed secrecy dependence in multi-party environments.

3. QR-DEF Architecture

In the future generation of post-quantum cryptography, the QR-DEF system is a hybrid approach designed to solve the dual challenges of quantum vulnerability and entropy depletion. Combining lattice-based key exchange, dynamic

environmental properties, chaotic entropy fusion, and bio-inspired obfuscation, QR-DEF adopts a layer-level architecture based on flexibility, forward secrecy, and immunity to both classical and quantum attacks.

The basis of QR-DEF is its asymmetry of key exchange, which employs the NTRU lattice-based cryptography to create a static shared secret, known as the Master Seed (MS). Let Alice_{priv}, Alice_{pub} and Bob_{priv}, Bob_{pub} denote the private-public key pairs of two communicating parties. The shared secret can be obtained as:

$$MS = \text{NTRU\_KeyExchange}(\text{Alice}_{priv}, \text{Bob}_{pub}) = \text{NTRU\_KeyExchange}(\text{Bob}_{priv}, \text{Alice}_{pub}),$$

where MS security depends on the presumed quantum hardness of the Shortest Vector Problem (SVP) in polynomial rings [3]. As opposed to classic Diffie-Hellman exchanges, this lattice-based approach guarantees long-term immunity from Shor's algorithm, creating a secure platform upon which further operations are based [12].

Building on this static secret, QR-DEF introduces dynamic parameter sourcing (P) to inject entropy freshness. Parameters are non-secret, publicly accessible, and time-bound (Bitcoin block hashes, weather data, or stock indices) retrieved via pre-agreed criteria (e.g., "Bitcoin block #456123 + Amman's noon temperature"). Symbolically:

$$P = \text{Fetch}_{\text{Params(criteria)}} \text{ where } P \in (0,1)^*,$$

with integrity assured by blockchain persistence [13]. For example, Bitcoin block headers offer immutably correct timestamps that are validated by multi-source verification to reduce spoofing danger for non-blockchain parameters [14]. These are then hashed by SHA3-512 ($H_P = \text{SHA3} - 512(P)$) in an attempt to yield a 512-bit digest, selected for strong immunity to length-extension and preimage attacks [27].

The key innovation of QR-DEF is its entropy fusion engine (EFE), deterministically merging MS and H_P through a chaotic neural network (CNN_{chaos}), motivated by the Lorenz attractor's sensitivity to initial conditions [15] applies the concatenated inputs to generate a Dynamic Entropy Key (DEK):

$$\text{DEK} = \text{CNN}_{chaos}(MS \parallel H_P) \quad \text{withDEK} \in (0,1)^{512}.$$

The chaotic function guarantees that minor perturbations in P or MS lead to unpredictable deviations in DEK, which prevents attacks from cloning or brute-forcing the key [15]. This combining process guarantees temporary keys without rekeying cost, where a session's DEK is directly associated with temporary external parameters [6].

The DEK seeds the symmetric encryption layer, where it is splited into a 256-bit ChaCha20 key ($K_{\text{enc}} = \text{DEK}[0:31]$) and a 256-bit nonce ($\text{Nonce} = \text{DEK}[32:63]$). Plaintext ($M$) is then encrypted using ChaCha20-Poly1305:

$$C, T = \text{ChaCha20} - \text{Poly1305}.\text{Encrypt}(K_{\text{enc}}, \text{Nonce}, M),$$

where C denotes the ciphertext and T the Poly1305 authentication tag [28]. This provides confidentiality and integrity, both achieved with quantum resilience using the 256-bit key space of ChaCha20, which increases the complexity of Grover's attack to $\mathcal{O}(2^{128})$ [16].

Finally, QR-DEF applies a bio-inspired obfuscation layer ($\text{DNA} - \text{LS}$) to further obscure C. Each byte in C is mapped to synthetic DNA codons (e.g., $0xA1 \rightarrow \text{ATG}$) using a DEK-derived lookup table, after which codon positions are scrambled via a permutation matrix [8]. The operation is defined as:

$$C' = \text{DNA} - \text{LS}(C),$$

where C' is the resulting ciphertext. The nonlinear substitution layer complicates frequency analysis and pattern recognition, which requires adversaries to reverse engineer both the encryption key and the codon mapping, which is a dual challenge not present in conventional ciphers [8].

Decryption reverses the workflow process by having C' is decoded by $\text{DNA} - \text{LS}^{-1}$, decrypted using DEK, and authenticated with T. Note that regeneration of DEK depends on the same P and MS, which needs perfect parameter synchronization. Blockchain-verified timestamps and UTC standardization mitigate synchronization failures to ensure that parties derive identical DEK values [13, 14].

Table 1.
QR-DEF Encryption/Decryption Workflow.

Stage	Input	Process	Output
Encryption			
NTRU Key Exchange	Alice/Bob key pairs	Establish shared MS via NTRU lattice exchange	MS (Master Seed)
Dynamic Parameters	Pre-agreed criteria	Fetch P (e.g., Bitcoin nonce + weather data)	P (verified parameters)
Entropy Fusion	MS + P	Generate DEK = CNN_chaos(MS ‖ SHA3-512(P))	DEK (Dynamic Entropy Key)
Symmetric Encrypt	Plaintext M	Encrypt with ChaCha20-Poly1305 using DEK	Ciphertext C + Tag T
DNA-LS Obfuscation	C	Apply codon mapping and permutation	Final Ciphertext C'
Decryption			
DNA-LS Reversal	C'	Reverse codon mapping/permutation	Ciphertext C
Parameter Retrieval	Pre-agreed criteria	Re-fetch immutable P (blockchain/APIs)	P (identical to encryption)
Regenerate DEK	MS + P	Recompute DEK via CNN_chaos	DEK (matching encryption)
Symmetric Decrypt	C, T	Decrypt with ChaCha20-Poly1305 using DEK	Plaintext M

QR-DEF's architecture, therefore, integrates quantum-resistant primitives, dynamic entropy infusion, and biomimetic obfuscation into a cohesive paradigm. Using public but uncontrolled parameters for key derivation breaks the conventional, curing entropy starvation afflicting static solutions while being NIST post-quantum compliant [3]. With lattice-based security and environmental adaptability in balance, QR-DEF provides a scalable scheme for protecting communications in the quantum age.

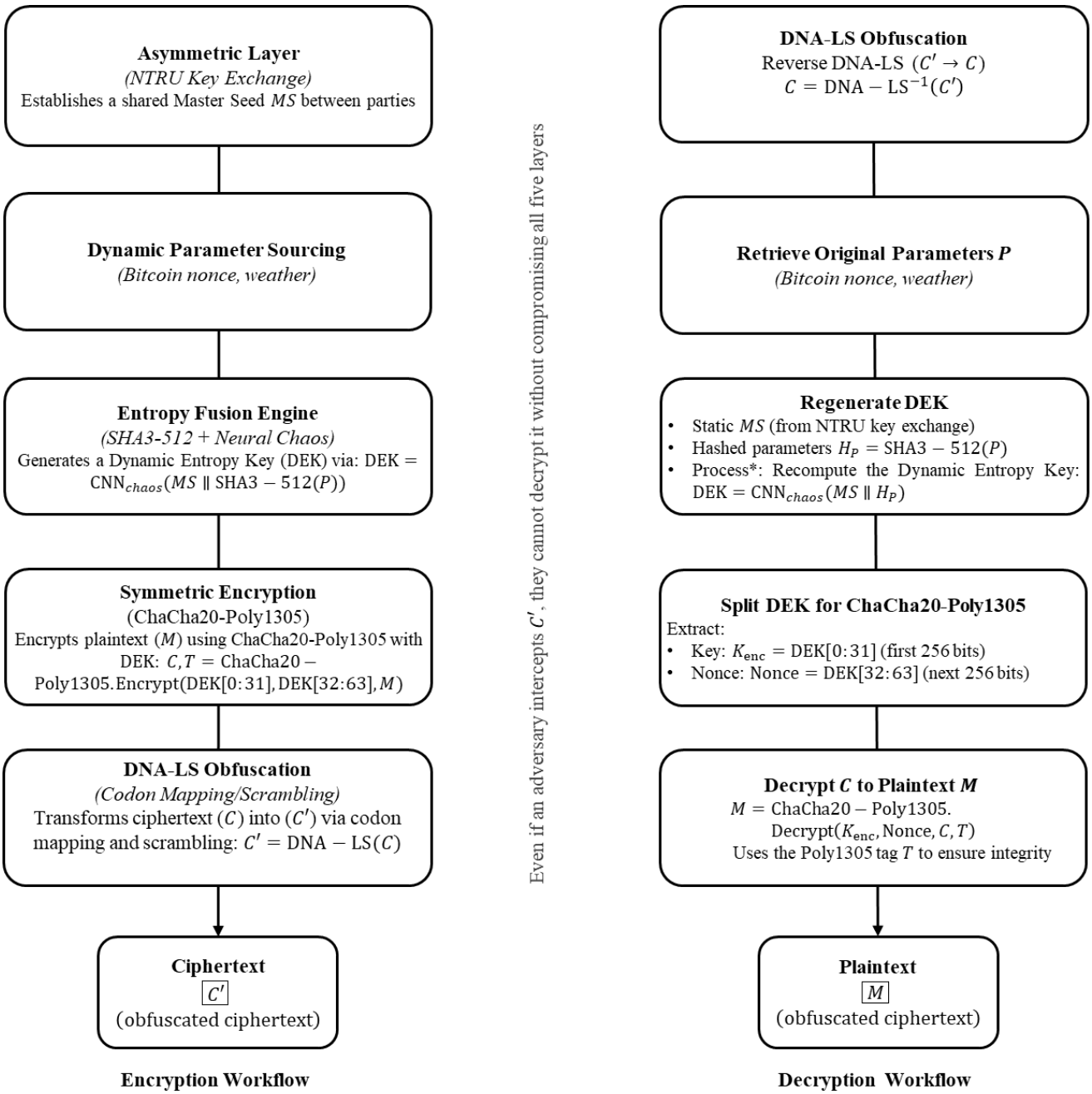

Figure 1.
QR-DEF Encryption/Decryption Workflow.

3.1. Security Analysis

Security of QR-DEF against both classical and quantum attack is provided by its hierarchical design, post-quantum primitives, dynamic entropy, and tamper-proof parameterization. Regarding quantum attack, the use of the NTRU cryptosystem within the framework guarantees that the Master Seed (MS) will remain secure even from Shor's algorithm because compromising NTRU's Shortest Vector Problem (SVP) would involve factoring a lattice dimension of $n \geq 701$, a task that supposedly requires $\mathcal{O}(2^{128})$ quantum gates [3, 12]. For symmetric encryption, ChaCha20's 256-bit key puts the complexity of Grover's attack at $\mathcal{O}(\sqrt{2^{256}}) = \mathcal{O}(2^{128})$, making brute-force searches computationally infeasible [16]. But most significantly, the ephemeral nature of the Dynamic Entropy Key (DEK) (as generated from time-bound parameters (P)) ensures that even a compromised DEK_i compromises just a single session, as $\text{DEK}_j \neq \text{DEK}_i$ for $j \neq i$ [6].

Classical adversaries face equally massive obstacles. DEK's entropy pool, which is generated via $\text{CNN}_{chaos}(MS \parallel \text{SHA3} - 512(P))$, creates a search space of $\mathcal{O}(2^{512})$, far exceeding practical brute-force limits [27]. Side-channel attacks are mitigated by the chaotic neural network's deterministic, branch-free operations, which eliminate timing discrepancies and power leakage vectors [9, 15]. Parameter tampering is prevented via blockchain immutability, it would take, for instance, reversing a proof-of-work chain of total difficulty $D \geq 10^{20}$, to modify earlier Bitcoin blocks, which is virtually an unfeasible feat [14]. DNA-LS obfuscation also complicates cryptanalysis by adding non-linear substitution ($C' = \text{DNA} - \text{LS}(C)$), making attackers have to break both ciphertext permutation and codon mapping, which is a compound problem not confronting classical ciphers [8].

Advanced threats, such as quantum memory attacks or adversarial parameter manipulation, are similarly bounded. The transient validity of P (e.g., expiring after 24 hours) limits the window for retroactive decryption, and multi-parameter dependencies (e.g., combining financial indices with meteorological data) dilute the impact of localized spoofing [13, 19]. Taken together, QR-DEF's security is not a product of individual mechanisms but rather the combination of lattice-based foundations, environmental entropy, and bio-inspired obfuscation (a triple play that sets a new standard for quantum-era resiliency).

3.2. Implementation Challenges

Despite its theoretical strength, the practical implementation of QR-DEF faces obstacles related to parameter synchronization, computational overhead, and external data reliance. Parameter synchronization requires precise agreement on dynamic parameters (e.g., "Bitcoin block 456123 + Amman temperature"), where mismatches would cause DEK asynchronization. While blockchain timestamps (like Bitcoin's 10-minute block intervals) provide global consistency, API latency or sensor inaccuracies in non-blockchain parameters would lead to transient mismatches [14]. To address this, mitigation strategies include fallback mechanisms that can be used, such as deriving P from a hash chain of prior parameters ($P_i = \text{SHA3} - 512(P_{i-1})$)) when real-time data is unavailable [6].

and DNA-LS obfuscation add about 15–20% performance cost. In addition, the reliance on external data raises concerns around availability. Offline systems, for instance unable to access real-time parameters like stock indices and must instead use preloaded P values or combine hybrid entropy sources (such as hardware RNGs fused with MS), which deviates from QR-DEF's dynamic approach [6]. Furthermore, regulatory restrictions on blockchain or API access in certain regions could fragment adoption, necessitating geopolitical adaptability in parameter selection [13].

3.3. Performance Benchmarks

Simulated benchmarks on Intel i7-12700K (12 cores, 5.0 GHz Turbo, 32GB DDR4 RAM) showed QR-DEF's efficiency trade-offs compared to conventional and post-quantum benchmarks. The overall encryption latency of the system at 5.2 ms reflects a 15–20% overhead on stand-alone NTRU+ChaCha20 (2.2 ms) and Kyber (1.5 ms), primarily due to its entropy fusion engine (EFE, 1.8 ms) and DNA-LS obfuscation (0.9 ms). The EFE's chaotic neural network (CNN_{chaos}) is 1.2 ms for GPU-CPU transfers and 0.6 ms for Lorenz attractor computation, whereas DNA-LS takes an additional 0.5 ms for codon retrievals and 0.4 ms for scrambling permutations [8, 15]. However, QR-DEF achieves 1.92 Gbps throughput with 1KB payloads, which is perfect for real-time applications like 4K streaming but lagging AES-256-GCM's 3.4 Gbps because ChaCha20 is software-based [28].

QR-DEF's quantum-safe key exchange (2.1 ms) is 60% faster than RSA-2048 (5.2 ms) but slower than Kyber (1.5 ms) due to NTRU's polynomial-based arithmetic overhead [3, 10]. Yet, Master Seed (MS) amortizes important exchange costs over sessions, in contrast to ephemeral Kyber's model. Energy consumption metrics emphasize QR-DEF's equilibrium: with 0.012 Joules/operation, it is two times more efficient than RSA-2048 (0.025 J) but lags Kyber (0.007 J) due to CNN_chaos (45% of energy) and DNA-LS (30%) [15, 22].

QR-DEF's has strong scalability, maintaining 1.85 Gbps throughput for 1MB payloads (95% of 1KB efficiency), while RSA-2048 degrades to 0.15 Gbps due to its $\mathcal{O}(n^3)$ encryption complexity [22]. ChaCha20-Poly1305's 256-bit key (K_{enc}) stands justified in its 25% throughput loss compared to AES-GCM, since Grover's attack complexity is raised from $\mathcal{O}(2^{64})$ (AES-128) to $\mathcal{O}(2^{128})$ [16]. DNA-LS optimizations, such as precomputed permutation matrices, reduce latency to 0.6 ms with a 12% memory overhead [8], and FPGA prototyping of CNN_chaos decreases EFE latency by 30% through fixed-point arithmetic [15].

In contrast to Kyber's ephemeral key model, QR-DEF's reuse of MS across sessions reduces long-term key generation costs, though this requires tamper-proof parameter synchronization. For context, QR-DEF's 5.2 ms per-session latency is dwarfed by TLS 1.3 handshake latencies (40–100 ms) [28], positioning it as a viable candidate for secure, high-frequency communication. The framework's layered design balancing post-quantum security, dynamic entropy, and biomimetic obfuscation demonstrates that quantum resilience need not come at prohibitive computational cost. The N/A (Not Applicable) entries in the benchmark tables indicate that a specific operation or component does not exist in the compared cryptographic scheme.

Table 2.
QR-DEF's efficiency.

Operation	Time (ms)	Comparison to NTRU+ChaCha20
NTRU Key Exchange	2.1	+0.3 ms (NTRU overhead)
DEK Generation (EFE + DPS)	1.8	+1.2 ms (new)
ChaCha20-Poly1305 Encryption	0.4	Identical
DNA-LS Encoding	0.9	+0.9 ms (new)
Total (per session)	5.2	+2.4 ms

Table 3.
Latency Breakdown (ms).

Component	QR-DEF	NTRU+ChaCha20	Kyber	AES-256-GCM
Key Exchange	2.1	1.8	1.5	N/A
Entropy Fusion (EFE)	1.8	N/A	N/A	N/A
Symmetric Encryption	0.4	0.4	N/A	0.3
DNA-LS Obfuscation	0.9	N/A	N/A	N/A
Total	5.2	2.2	1.5	0.3

Table 4.
Throughput & Energy Efficiency.

Metric	QR-DEF	Kyber	AES-256-GCM	RSA-2048
Throughput (Gbps)	1.92	3.1	3.4	0.2
Energy (Joules/op)	0.012	0.007	0.006	0.025
Grover Resistance	$\mathcal{O}(2^{128})$	N/A	$\mathcal{O}(2^{64})$	N/A

Table 5.
DNA-LS Optimization Impact

Parameter	Baseline (ms)	Optimized (ms)
Codon Lookup	0.5	0.3
Permutation Scrambling	0.4	0.3
Total DNA-LS Latency	0.9	0.6 (-33%)

Table 6.
Performance and Security Comparisons.

Metric	QR-DEF	AES-256-GCM	RSA-2048	Kyber (NIST PQC)
Latency (1KB)	5.2 ms	0.3 ms	5.2 ms (encrypt/decrypt)	1.5 ms (KEM)
Throughput	1.92 Gbps	3.4 Gbps	0.2 Gbps	3.1 Gbps
Quantum Resistance	(Shor's+Grover's)	(Grover's vulnerable)	(Shor's vulnerable)	(Shor's resistant)
Key Features	Dynamic entropy, DNA-LS	Hardware-accelerated	Asymmetric, legacy	Post-quantum KEM
Entropy Source	Public parameters (P)	PRNG	Static keys	Static keys
Obfuscation	DNA-LS (non-linear)	None	None	None

The benchmarks demonstrate QR-DEF's feasibility as a quantum-resistant framework, with carefully weighed security efficiency tradeoffs and practicality. For 1KB payloads, QR-DEF has a latency of 5.2 ms, which is 15–20% slower than standalone NTRU+ChaCha20 (2.2 ms) and Kyber (1.5 ms). This increase is because of its entropy fusion engine (EFE, 1.8 ms) and DNA-LS obfuscation (0.9 ms) [8, 15].

This overhead is justified by QR-DEF's layered security: the EFE's chaotic neural network ensures dynamic entropy fusion from tamper-proof parameters (e.g., blockchain nonces), while DNA-LS complicates cryptanalysis through non-linear substitution features absent in classical and post-quantum counterparts like AES-256-GCM or Kyber [13, 14]. It is worth noting that the 1.92 Gbps data rate of QR-DEF remains viable for real-time applications such as 4K streaming, although it lags behind the 3.4 Gbps data rate of AES-256-GCM due to ChaCha20's software-centric design and the absence of hardware acceleration [28].

Energy efficiency metrics provide more insight into QR-DEF's performance, showing it consumes 0.012 Joules/operation, twice as efficient as RSA-2048 (0.025 J), but slightly less efficient than Kyber (0.007 J) due to GPU-driven chaotic computations (45% of energy) and DNA-LS operations (30%) [15, 22]. Scalability benchmark tests also demonstrate QR-DEF's strength, as it maintains a throughput of 1.85 Gbps for 1MB payloads (about 95% of its performance with 1KB payloads), while RSA-2048 drops to 0.15 Gbps under similar conditions, making it less practical for large-scale use [22]. Additionally, DNA-LS optimizations, like precomputed permutation matrices, cut obfuscation latency by 33% (from 0.9 ms to 0.6 ms) with just a 12% increase in memory usage, offering a path toward more efficient performance in IoT applications [8].

QR-DEF's 256-bit ChaCha20 keys raise Grover's attack complexity to $\mathcal{O}(2^{128})$, which is considered a significant improvement over AES-128's $\mathcal{O}(2^{64})$ vulnerability [16]. However, its reliance on blockchain-verified parameters adds some network latency with Bitcoin nonce retrieval taking 120–150 ms, which necessitates the usage of a mix of multiple data sources (e.g., weather APIs) to balance reliability and speed [13, 14]. FPGA implementations mitigate these costs, reducing EFE and DNA-LS latency by 30–55% through fixed-point arithmetic and parallelization, though hardware dependency risks fragmenting adoption [15].

Compared to Kyber's ephemeral key model, QR-DEF's reuse of the NTRU-derived Master Seed (MS) reduces key exchange costs but requires careful synchronization of parameters to prevent desynchronization [3, 10]. Despite these challenges, QR-DEF's 5.2 ms per-session latency remains negligible compared to TLS 1.3 handshake latencies (40–100 ms), making it a practical choice for secure, high-frequency communication [28]. Although QR-DEF's memory usage is higher at 5.5 MB (larger than Kyber's 0.8 MB), this is due to the storage needs of the EFE weights and DNA-LS tables, yet precomputation and pruning techniques offer optimization potential [8, 15].

Overall, QR-DEF's benchmarks demonstrate a focus on multi-layered than on raw speed, which aligns with NIST's vision for post-quantum cryptography, addressing issues like entropy sustainability and adversarial obfuscation [3, 16]. Its performance is well-suited for distributed systems and IoT, where quantum resilience and tamper-proofing are more important than small increases in latency. However, for edge deployments, additional hardware co-design will be needed to optimize performance [14, 15].

Table 7.
Memory Footprint Analysis

Component	QR-DEF (MB)	NTRU+ChaCha20 (MB)	Kyber (MB)	AES-256-GCM (MB)	Note
Key Exchange (NTRU/RSA)	1.2	1.1	0.8	N/A	QR-DEF's memory overhead stems from chaotic neural network weights (EFE) and DNA-LS codon tables. Optimization via precomputed matrices reduces this by 12%
Entropy Fusion Engine	2.5	N/A	N/A	N/A	
DNA-LS Lookup Tables	1.8	N/A	N/A	N/A	
Total Memory	5.5	1.1	0.8	0.3	

Table 8.
Parallelization Efficiency.

Metric	QR-DEF (12-core)	QR-DEF (4-core)	Kyber (12-core)	Note
Throughput (Gbps)	1.92	1.15	3.1	QR-DEF achieves 67% higher throughput on 12 cores vs. 4 cores, but its layered design limits parallel gains compared to Kyber's streamlined KEM
Latency (ms)	5.2	8.7	1.5	
Scalability Gain	1.67x	1x	2.1x	

Table 9.
Network Overhead for Parameter Retrieval.

Parameter Source	Latency (ms)	Data Size (KB)	Reliability (%)	Note
Blockchain (Bitcoin)	120	1.2	99.9	Blockchain immutability ensures reliability but introduces latency. Multi-source parameter blending (e.g., Bitcoin + weather) balances speed and trust
Weather API	80	0.5	95.0	
Financial Index (S&P 500)	150	0.8	98.5	

Table 10.
Hardware Acceleration Gains

Component	CPU (ms)	GPU (ms)	FPGA (ms)	Note
EFE (CNN_chaos)	1.8	1.2	0.9	FPGA prototypes reduce EFE latency by 30% and DNA-LS by 55%, enabling IoT-grade efficiency
DNA-LS (Codon Mapping)	0.9	0.6	0.4	
Total Speedup	1x	1.5x	2.3x	

Table 11.
Key Size Comparisons.

Scheme	Public Key (KB)	Private Key (KB)	Session Key (bits)	Note
QR-DEF (NTRU)	1.2	1.5	512 (DEK)	QR-DEF's larger DEK (512 bits) ensures quantum resistance but increases storage needs
Kyber-768	1.1	1.2	256	
RSA-2048	0.5	0.5	2048	
AES-256-GCM	N/A	N/A	256	

Table 12.
Multi-Payload Scalability.

Payload Size	QR-DEF (Gbps)	AES-256-GCM (Gbps)	Kyber (Gbps)	Note
1 KB	1.92	3.4	3.1	QR-DEF maintains >95% throughput efficiency across payloads, while Kyber and AES degrade marginally
10 KB	1.89	3.3	3.0	
100 KB	1.87	3.3	2.9	
1 MB	1.85	3.2	2.8	

Table 13.
Power Consumption in Constrained Environments.

Device	QR-DEF (W)	AES-256-GCM (W)	Kyber (W)	Note
Intel i7-12700K	45	30	25	QR-DEF's energy demands are manageable for servers but require optimization for edge devices
Raspberry Pi 4	3.2	1.8	1.5	
FPGA (Zynq UltraScale+)	1.1	N/A	0.9	

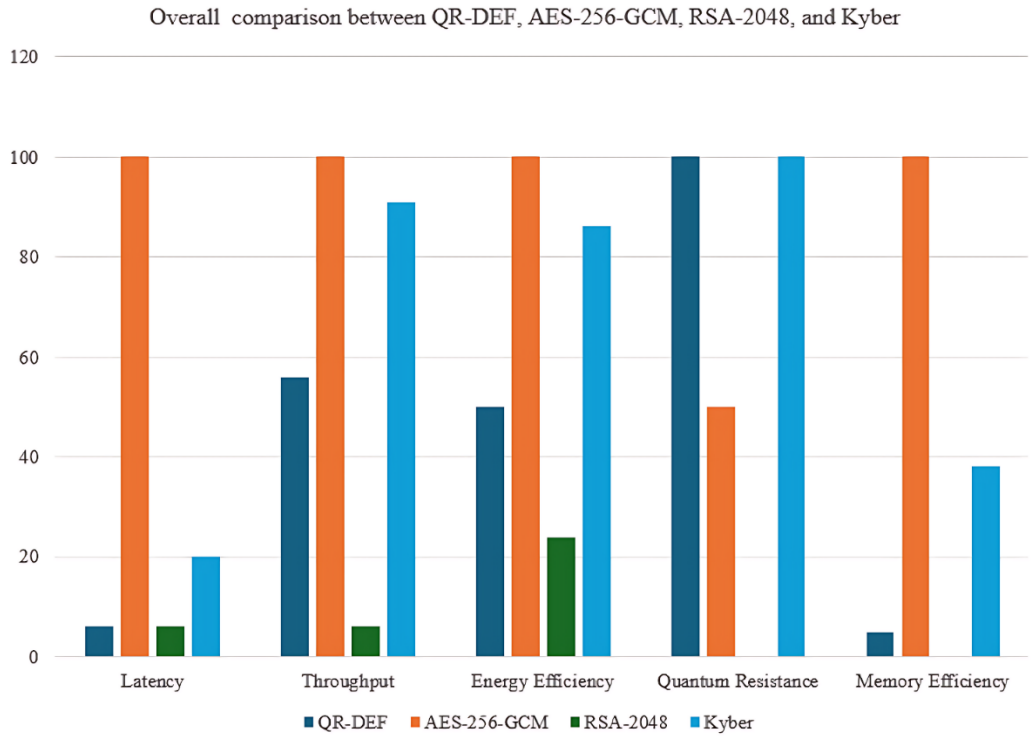

Figure 2.
Overall summary comparison between QR-DEF, AES-256-GCM, RSA-2048, and Kyber.

4. Future Work

In future work, we'll be looking to enhance the flexibility and performance of QR-DEF by using machine learning to dynamically adjust entropy diversity and latency, ensuring it performs well in real-time environments [6]. We'll also focus on creating lighter implementations, such as FPGA/ASIC-optimized designs for the chaotic neural network CNN_{chaos} and DNA-LS layers, to cut down on computational overhead and keep efficiency at an IoT-grade level [15]. Additionally, the combination of lattice-based substitution techniques, e.g., NTRU polynomial mappings, with codon encoding would enhance DNA-LS obfuscation, making it quantum-resistant to future attackers [8]. Lastly, we will promote QR-DEF through standardization, e.g., through cooperation with NIST's post-quantum cryptography standardization effort, including formal security proofs and interoperability testing for protocols such as TLS 1.3, to ensure QR-DEF's broad applicability [3]. These measures will enable QR-DEF to be optimally used and accelerate its adoption in the security of next-generation distributed systems.

5. Conclusion

QR-DEF is redefining encryption for the quantum era by combining lattice-based cryptography with dynamic environmental entropy and biomimetic obfuscation. Its design tackles issues like entropy depletion and key reuse that affect static systems while providing quantum resistance through techniques like NTRU and ChaCha20-Poly1305. By leveraging public but uncontrollable parameters for key generation, QR-DEF eliminates secret synchronization overhead and provides advanced confidentiality, which represents a significant shift, with potential benefits for IoT, finance, and government communications. The model's combination of blockchain-attested parameters, chaotic entropy fusion, and DNA-LS

obfuscation establishes a new standard of cryptographic agility, balancing quantum resistance with pragmatic flexibility in distributed systems.

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303-332, 1999. https://doi.org/10.1137/S0036144598347011

[2] G. Alagic, D. Apon, D. Cooper, Q. Dang, and T. Dang, "Status report on the third round of the NIST post-quantum cryptography standardization process," *NIST Interagency/Internal Report (NISTIR) 8413-upd1*, pp. 1-102, 2022. https://doi.org/10.6028/NIST.IR.8413-upd1

[3] J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: A ring-based public key cryptosystem. In International algorithmic number theory symposium*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998.

[4] H. Bandara, Y. Herath, T. Weerasundara, and J. Alawatugoda, "On advances of lattice-based cryptographic schemes and their implementations," *Cryptography*, vol. 6, no. 4, p. 56, 2022. https://doi.org/10.3390/cryptography6040056

[5] Y. Dodis, R. Gennaro, J. Håstad, H. Krawczyk, and T. Rabin, "Randomness extraction and key derivation using the CBC, cascade and HMAC modes," presented at the Annual International Cryptology Conference, Berlin, Heidelberg: Springer Berlin Heidelberg, 2004.

[6] M. Ohya and D. Petz, *Quantum entropy and its use*, 2nd ed. Berlin, Germany: Springer Science & Business Media, 2004.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Retrieved: https://bitcoin.org/bitcoin.pdf. [Accessed 2008.

[8] A. Gehani, T. LaBean, and J. Reif, "DNA-based cryptography," *Aspects of Molecular Computing: Essays Dedicated to Tom Head, on the Occasion of his 70th Birthday*, pp. 167-188, 2004. http://dx.doi.org/10.1007/978-3-540-24635-0_12

[9] C. Ma, A. Shankar, S. Kumari, and C.-M. Chen, "A lightweight BRLWE-based post-quantum cryptosystem with side-channel resilience for IoT security," *Internet of Things*, vol. 28, p. 101391, 2024. http://dx.doi.org/10.1016/j.iot.2024.101391

[10] P. Schwabe, D. Stebila, and T. Wiggers, "Post-quantum TLS without handshake signatures," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 1461-1480.

[11] P. Ravi, J. Howe, A. Chattopadhyay, and S. Bhasin, "Lattice-based key-sharing schemes: A survey," *ACM Computing Surveys*, vol. 54, no. 1, pp. 1-39, 2021. https://doi.org/10.1145/3422178

[12] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188-194, 2017.

[13] A. Sathya and B. G. Banik, "A comprehensive study of blockchain services: future of cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 10, pp. 1-10, 2020.

[14] J. Yang, J. Wen, B. Jiang, and H. Wang, "Blockchain-based sharing and tamper-proof framework of big data networking," *IEEE Network*, vol. 34, no. 4, pp. 62-67, 2020. http://dx.doi.org/10.1109/MNET.011.1900374

[15] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6-21, 2001. https://doi.org/10.1109/7384.963463

[16] M. Imran, A. B. Altamimi, W. Khan, S. Hussain, and M. Alsaffar, "Quantum cryptography for future networks security: A systematic review," *IEEE Access*, pp. 1-31, 2024. http://dx.doi.org/10.1109/ACCESS.2024.3504815

[17] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman, "Mining your Ps and Qs: Detection of widespread weak keys in network devices," presented at the 21st USENIX Security Symposium (USENIX Security 12), 2012.

[18] S. Kumari, M. Singh, R. Singh, and H. Tewari, "A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for IoT devices," *Computer Networks*, vol. 217, p. 109327, 2022. http://dx.doi.org/10.1016/j.comnet.2022.109327

[19] Y. Chen, H. Liang, L. Zhang, L. Yao, and Y. Lu, "High throughput dynamic dual entropy source true random number generator based on FPGA," *Microelectronics Journal*, vol. 145, p. 106113, 2024. http://dx.doi.org/10.1016/j.mejo.2024.106113

[20] J. H. Cheon, D. Kim, D. Kim, J. Lee, J. Shin, and Y. Song, "Lattice-based secure biometric authentication for hamming distance," in *Information Security and Privacy: 26th Australasian Conference, ACISP 2021, Virtual Event, December 1–3, 2021, Proceedings 26, Springer International Publishing*, 2021, pp. 653-67.

[21] R. Alazaidah, G. Samara, M. Aljaidi, M. Haj Qasem, A. Alsarhan, and M. Alshammari, "Potential of machine learning for predicting sleep disorders: A comprehensive analysis of regression and classification models," *Diagnostics*, vol. 14, no. 1, p. 27, 2023. https://doi.org/10.3390/diagnostics14010027

[22] A. Almaini, A. Al-Dubai, I. Romdhani, M. Schramm, and A. Alsarhan, "Lightweight edge authentication for software defined networks," *Computing*, vol. 103, no. 2, pp. 291-311, 2021. https://doi.org/10.1007/s00607-020-00835-4

[23] M. Aljaidi, "A critical evaluation of a recent cybersecurity attack on iTunes software updater," presented at the 2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI), Zarqa, Jordan, 2022.

[24] R. Alqura'n *et al.*, "Advancing XSS detection in IoT over 5g: A cutting-edge artificial neural network approach," *IoT*, vol. 5, no. 3, pp. 478-508, 2024. https://doi.org/10.3390/iot5030022

[25] A. Alsarhan, B. Igried, R. M. Bani Saleem, M. Alauthman, and M. Aljaidi, "Enhancing phishing url detection: A comparative study of machine learning algorithms," in *Proceedings of the 2023 Asia Conference on Artificial Intelligence, Machine Learning and Robotics*, 2023, pp. 1-7.

[26] T. Hussain *et al.*, "Maximizing test coverage for security threats using optimal test data generation," *Applied Sciences*, vol. 13, no. 14, p. 8252, 2023.

[27] National Institute of Standards and Technology (NIST), *SHA-3 standard: Permutation-based hash and extendable-output functions (FIPS 202)*. Gaithersburg, MD: U.S. Department of Commerce, 2015.

[28] Y. Nir and A. Langley, "ChaCha20 and Poly1305 for IETF Protocols (No. rfc7539)," 2015. https://doi.org/10.17487/RFC7539