Crypto-ncRNA: Non-coding RNA (ncRNA) Based Encryption Algorithm

Anonymous authors
Paper under double-blind review

Abstract

This paper introduces Crypto-ncRNA, a encryption framework leveraging the dynamic folding mechanisms of non-coding RNA (ncRNA) to address post-quantum cryptography challenges. Capitalizing on ncRNA's intrinsic physical unclonable functions (PUFs) and high conformational entropy, Crypto-ncRNA generates highly stochastic cryptographic keys and ciphertexts. The scheme implements a four-tiered architecture encompassing RNA sequence generation, structural folding, dynamic key derivation, and ciphertext packaging. Experimental results demonstrate Crypto-ncRNA's robust performance in efficiency, throughput, ciphertext randomness, and operational reliability, validated by NIST SP 800-22 randomness tests. Compared to classical algorithms, Crypto-ncRNA exhibits superior entropy and robust security. This study highlights the potential of bio-convergent cryptography for constructing next-generation secure infrastructures.

1 Introduction

Biomolecular cryptography has emerged as a potential breakthrough in post-quantum encryption (Balamurugan et al. (2021); Mondal & Ray (2023)). Moreover, with the rapid advancement of artificial intelligence, RNA-based research has gradually unfolded into a new realm of innovation (Townshend et al. (2021)). Recent studies showed that the dynamic folding processes of RNA molecules intrinsically exhibit physical unclonable functions (PUFs) characteristics (Herder et al. (2014); Li et al. (2022); Luescher et al. (2024); Zhou et al. (2021)), thereby establishing a pathway for designing post-quantum cryptography (PQC) systems (Arapinis et al. (2021); Cambou et al. (2021)).

In this paper, we introduce *Crypto-ncRNA*, an encryption framework harnessing the dynamic folding mechanisms of non-coding RNA (ncRNA) to address quantum-era security challenges. By exploiting ncRNA's intrinsic PUFs and high conformational entropy, enhanced through deep learning-based RNA secondary structure prediction, the scheme generates cryptographically robust keys and ciphertexts with enhanced stochasticity. This work provides a new direction for encryption technology in the quantum era by integrating RNA's PUFs with encryption algorithms.

2 Method (details in Appendix A)

The *Crypto-ncRNA* implements a four-tiered encryption architecture. The research framework and workflow of the *Crypto-ncRNA* are illustrated in Figure 1.

1. **Codon Mapping and RNA Sequence Generation**
   Textual data is encoded into RNA codons (e.g., AUG) via Base64-derived 6-bit indices, enabling 50% higher information density than binary systems.

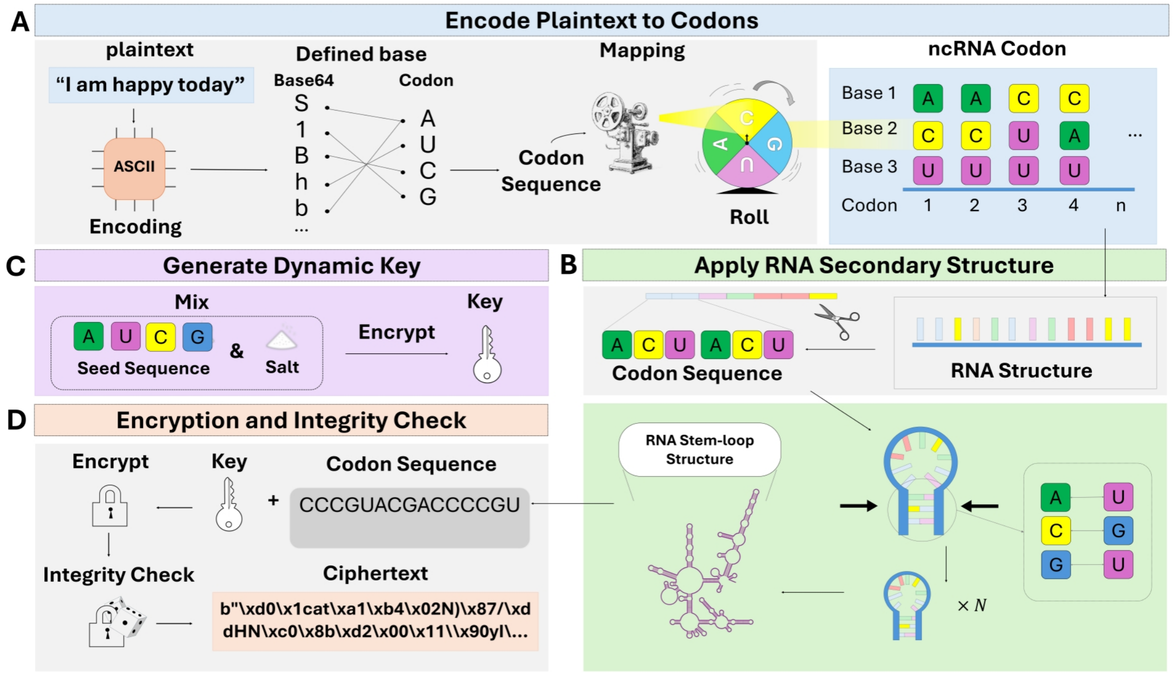

Figure 1: The Framework of Crypto-ncRNA Algorithm

2. **RNA Secondary Structure Folding**
   RNA codons are partitioned into Watson-Crick-paired stem regions and unpaired loops using LinearFold-predicted MFE structures. Dynamic codon permutation within structural constraints generates combinatorial complexity:4^N configurations, where N : dynamic positions
3. **Dynamic Key Generation**
   Quantum-resistant keys are synthesized using PBKDF2-HMAC-SHA256, leveraging RNA quaternary fingerprints (A/U/G/C positional entropy) and 256-bit cryptographic salts.
4. **Ciphertext Packaging and Integrity Verification**
   ChaCha20 encrypts payloads using dynamic RNA keys. SHA-256 hashing and enzyme markers ensure ciphertext integrity and physical binding.

At the same time, we also enhanced PUFs by combining T7-engineered RNA with restriction enzyme sites. Structural diversity and chemical fingerprints are secured through stochastic folding pathways. The process emphasizes sequence-dependent structural transformations and environmental noise integration to ensure cryptographic security and hardware-bound key uniqueness.

3 Results (details in Appendix C)

Crypto-ncRNA demonstrates robust performance across heterogeneous computing environments, validated through comprehensive benchmarking against classical algorithms (RSA, AES). The following visualizations (Figures 2) highlight its efficiency, reliability, and adaptability under varying workloads.

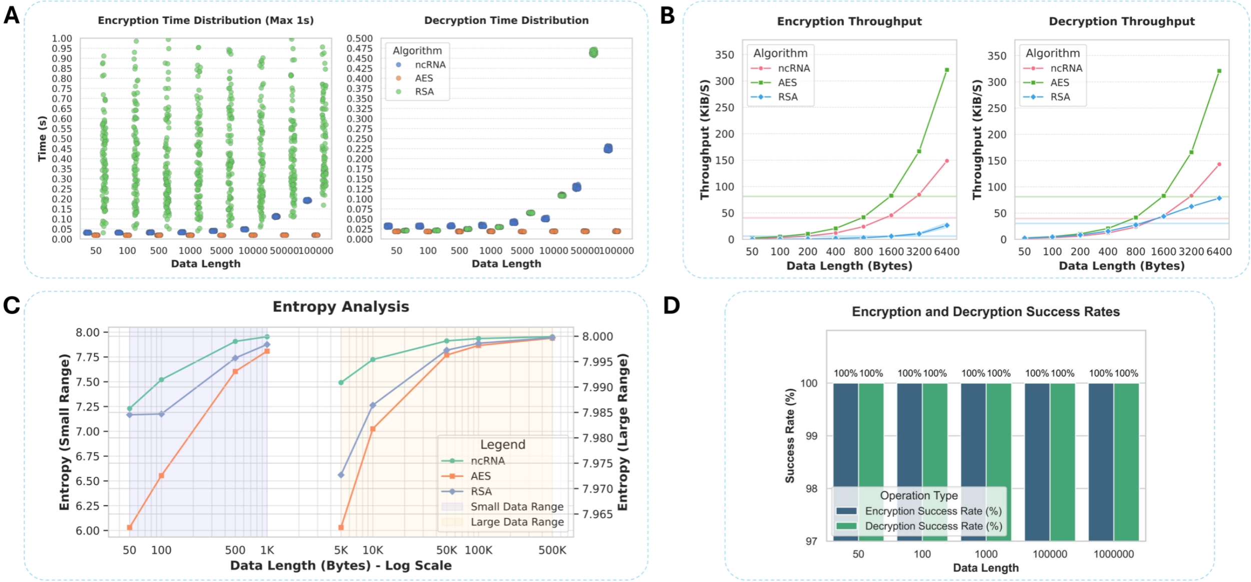

Figure 2: Summary of Algorithm(s) Comparation and Tesing Results

1. **Encryption/Decryption Efficiency** (Fig. 2A): The proposed method slightly underperforms AES in speed but surpasses RSA, achieving near-AES efficiency at smaller parameters.
2. **Encryption/Decryption Throughput Performance** (Fig. 2B): Throughput trends align closely with time efficiency results.
3. **Ciphertext Randomness** (Fig. 2C): Cryptographic average entropy consistently outperforms AES and RSA across all tests.
4. **Operational Reliability** (Fig. 2D): Demonstrates 100% success rate regardless of data volume.
5. **Statistical Randomness** (Appendix Table 1): Passes all NIST SP 800-22 criteria (Rukhin et al. (2010)), confirming cryptographic robustness.

4 Conclusion

Crypto-ncRNA establishes a bio-convergent security framework that synergizes the biophysical complexity of non-coding RNA with cryptographic principles. Looking ahead, deep learning offers a pathway to more robust RNA encryption methods through enhanced RNA structure prediction. By offering intrinsic unclonability via dual resistance, this architecture provides a future-proof solution for securing digital infrastructures in the post-quantum landscape.

URM Statement

The authors acknowledge that at least one key author of this work meets the URM criteria of ICLR 2025 AI4NA Tiny Papers Track.

References

M. Arapinis, M. Delavar, M. Doosti, and E. Kashefi. Quantum physical unclonable functions: Possibilities and impossibilities. *Quantum*, 5:475, 2021.

C. Balamurugan, K. Singh, G. Ganesan, and M. Rajarajan. Post-quantum and code-based cryptography—some prospective research directions. *Cryptography*, 5(4):38, 2021.

C. Cachin. *Entropy measures and unconditional security in cryptography*. PhD thesis, ETH Zurich, 1997.

B. Cambou, M. Gowanlock, B. Yildiz, D. Ghanaimiandoab, K. Lee, S. Nelson, C. Philabaum, A. Stenberg, and J. Wright. Post quantum cryptographic keys generated with physical unclonable functions. *Applied Sciences*, 11(6):2801, 2021.

C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas. Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*, 102(8):1126–1141, 2014.

L. Huang, H. Zhang, D. Deng, K. Zhao, K. Liu, D. A. Hendrix, and D. H. Mathews. Linearfold: Linear-time approximate rna folding by 5'-to-3' dynamic programming and beam search. *Bioinformatics*, 35(14): i295–i304, 2019.

I. Kimsey, K. Petzold, B. Sathyamoorthy, and H. M. Al-Hashimi. Visualizing transient watson–crick-like mispairs in dna and rna duplexes. *Nature*, 519(7543):315–320, 2015.

Y. Li, M. M. Bidmeshki, T. Kang, C. M. Nowak, Y. Makris, and L. Bleris. Genetic physical unclonable functions in human cells. *Science Advances*, 8:eabm4106, 2022.

A. M. Luescher, A. L. Gimpel, W. J. Stark, R. Heckel, and R. N. Grass. Chemical unclonable functions based on operable random dna pools. *Nature Communications*, 15:2955, 2024.

M. Mondal and K. S. Ray. Review on dna cryptography. *International Journal of Bioinformatics and Intelligent Computing*, 2(1):44–72, 2023.

D. Pribnow. Nucleotide sequence of an rna polymerase binding site at an early t7 promoter. *Proceedings of the National Academy of Sciences of the United States of America*, 72(3):784–788, 1975.

V. Rijmen and J. Daemen. Advanced encryption standard, 2001. Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology, 19, 22.

R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo. A statistical test suite for random and pseudorandom number generators for cryptographic applications (nist special publication 800-22 rev. 1a). Technical report, National Institute of Standards and Technology, 2010.

A. Rényi. On measures of entropy and information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, pp. 547–562. University of California Press, January 1961.

K. Sato, M. Akiyama, and Y. Sakakibara. Rna secondary structure prediction using deep learning with thermodynamic integration. *Nature Communications*, 12:941, 2021.

I. Tinoco Jr and C. Bustamante. How rna folds. *Journal of Molecular Biology*, 293(2):271–281, 1999.

R. J. Townshend, S. Eismann, A. M. Watkins, R. Rangan, M. Karelina, R. Das, and R. O. Dror. Geometric deep learning of rna structure. *Science*, 373(6558):1047–1051, 2021. doi: 10.1126/science.abe5650.

P. Yakovchuk, E. Protozanova, and M. D. Frank-Kamenetskii. Base-stacking and base-pairing contributions into thermal stability of the dna double helix. *Nucleic Acids Research*, 34(2):564–574, 2006.

W. Zhou, D. Melamed, G. Banyai, et al. Expanding the binding specificity for rna recognition by a puf domain. *Nature Communications*, 12:5107, 2021.

M. Zuker and D. Sankoff. Rna secondary structures and their prediction. *Bulletin of Mathematical Biology*, 46(4):591–621, 1984.

Appendix

A Technical Specifications of the crypto-ncRNA Framework

Crypto-ncRNA framework is a cryptographic algorithm designed for post-quantum cryptography, leveraging the dynamic folding properties of non-coding RNA (ncRNA). This framework addresses post-quantum cryptographic challenges by integrating the physical unclonability of biomolecular Physical Unclonable Functions (PUFs) with cryptographic principles. It constructs a highly randomized and quantum-resistant encryption system. Appendix A details the framework's five core modules: (1) data encoding and RNA sequence synthesis, (2) RNA secondary structure folding and obfuscation, (3) key derivation and cryptographic protocols, (4) Physical Unclonable Function (PUF) mechanisms, and (5) parameter scalability design. Each module is meticulously designed to optimize system performance in terms of information density, randomness, key strength, and physical security.

A.1 Data Encoding & RNA Sequence Synthesis

This module converts plaintext data into RNA sequences using Base64 encoding and RNA codon mapping, significantly enhancing information density and ensuring data format standardization.

A.1.1 Base64 Preprocessing

Process Plaintext data is converted into 6-bit indices (ranging from 0 to 63) via Base64 encoding, generating a standardized byte stream.

Technical Details

- Employs the RFC 4648 standard to ensure cross-platform compatibility.
- Input data is grouped into 3-byte blocks, with each block mapped to 4 Base64 characters; padding rules adhere to ”=” character completion.

Advantages Compared to traditional binary encoding (3 bits/character), Base64 offers a 6 bits/character encoding capacity, doubling information density.

A.1.2 Codon Mapping

Process Each 6-bit index is uniquely mapped to an RNA codon (e.g., AUG, GUA) through predefined substitution rules.

Technical Details

- Establishes a 64×1 codon lookup table to ensure one-to-one mapping.
- Codon selection adheres to biocompatibility rules, avoiding stop codons (e.g., UAA, UAG).

Advantages Leverages the quaternary (A/U/G/C) nature of RNA codons to achieve data compression and biological sequence adaptation.

A.2 RNA Secondary Structure Folding & Obfuscation

This module leverages the dynamic folding properties of RNA, combining Minimum Free Energy (MFE) prediction and dynamic codon reordering to generate highly complex RNA secondary structures, enhancing data randomness and resistance to analysis.

A.2.1 Minimum Free Energy (MFE) Prediction

Process The secondary structure of the RNA sequence is predicted using the LinearFold algorithm, with the output represented in dot-bracket notation (e.g., ”((…))”) (Huang et al. (2019); Zuker & Sankoff (1984)).

Technical Details

- Employs 5’-to-3’ dynamic programming and beam search, optimizing time complexity to O(n).
- The result partitions the sequence into stem regions (Watson-Crick base pairing, e.g., AU/GC) and loop regions (unpaired regions) (Kimsey et al. (2015); Tinoco Jr & Bustamante (1999); Yakovchuk et al. (2006)).

Function Structural partitioning provides topological constraints for subsequent dynamic obfuscation.

A.2.2 Dynamic Codon Reordering

Process Codons are reordered based on structural partitioning.

- **Stem Regions** Complementary codons are permuted under base pairing constraints (e.g., AU → UA).
- **Loop Regions** Random shuffling is performed based on an entropy-driven algorithm.

Technical Details

- Stem region permutation rules are constrained by thermodynamic stability to ensure structural integrity.
- Stem region permutation rules are constrained by thermodynamic stability to ensure structural integrity.

Security Generates 4^N combinations (where N is the number of dynamic sites), far exceeding traditional matrix obfuscation methods.

A.3 Key Derivation & Cryptographic Protocol

This module generates quantum-resistant keys through an entropy source based on RNA sequences and the PBKDF2-HMAC-SHA256 algorithm, ensuring high key strength and unpredictability.

A.3.1 Entropy Pool Construction

Inputs

- **RNA Seed** A quaternary sequence of length L, with an entropy value of $\log_2(4^L)$ bits.
- **Salt Value** A random binary string of length B bits, with an entropy value of $\log_2(2^B)$ bits.

Total Entropy Value

$$\text{Total Entropy} = \log_2(4^L \times 2^B) \text{ bits} \tag{1}$$

A.3.2 Key Generation

Process A 32-byte session key is outputted by iterating the PBKDF2-HMAC-SHA256 algorithm 100,000 times (default).

Technical Detail

- HMAC-SHA256 ensures strong binding between the key and the salt value.
- The number of iterations is dynamically adjustable, with a brute-force cracking complexity reaching $O(2^{256} \times 10^5)$ (default), surpassing AES-256 security.

A.4 Physical Unclonability Mechanisms

This module ensures hardware binding and physical irreproducibility of keys through RNA molecular engineering and multidimensional randomization techniques, preventing physical attacks and cloning. It supports dynamic parameter configuration to adapt to varying security needs, ranging from high-security to high-efficiency modes, thus meeting diverse application requirements.

A.4.1 RNA Molecular Engineering

Design Vectors are synthesized based on the T7 promoter sequence (5'-TAATACGACTCACTATAGGG-3') and embedded with restriction enzyme sites (Pribnow (1975)).

Function Restriction enzyme sites provide physically verifiable markers, preventing molecular replication.

A.4.2 Multidimensional Randomization

- **Sequence Modification:** Unique chemical fingerprints are introduced through methylation or fluorescent labeling.
- **Thermodynamic Diversity:** structural variations under temperature gradients are simulated via RNAfold, ensuring that folding pathways are irreproducible (Sato et al. (2021)).

A.5 Parameter Scalability Desgin

This framework supports dynamic parameter configuration to accommodate varying security requirements across different scenarios, as shown in Table 1.

Summary Appendix A comprehensively defines the technical implementation of the Crypto-ncRNA framework, demonstrating a deep integration of bioinformatics and cryptography through modular design. Data encoding enhances information density, dynamic folding strengthens randomness, the entropy pool and PBKDF2 ensure key strength, molecular engineering achieves physical unclonability, and parameter scalability provides broad applicability. The synergistic effect of these components offers an efficient, reliable, and verifiable solution for post-quantum cryptographic needs.

Table 1: Parameter Configuration for Different Security Modes

Mode	RNA Length (L)	Salt Value Length (B)	Iteration Count	Applicable Scenarios
High-Security Mode	≥128 nucleotides	≥1024 bits	≥200,000	Military-grade Financial-grade encryption
Balanced Mode	64 nucleotides	512 bits	100,000	General data protection
High-Efficiency Mode	32 nucleotides	256 bits	50,000	IoT devices Low-power applications

B Algorithm Pseudocode

Here is the pseudocode for the crypto-ncRNA encryption algorithm, illustrating the transformation process from plaintext to ciphertext:

Algorithm 1 crypto-ncRNA Encryption

```
procedure crypto_ncnra_encrypt($plaintext, RNA\_pool, salt$)
    $encoded\_data \leftarrow$ Base64Encode($plaintext$)
    $RNA\_sequence \leftarrow$ MapToCodons($encoded\_data$)
    $folded\_RNA \leftarrow$ FoldRNAStructure($RNA\_sequence$)
    $dynamic\_key \leftarrow$ GenerateDynamicKey($RNA\_pool, salt$)
    $encrypted\_data \leftarrow$ EncryptWithKey($folded\_RNA, dynamic\_key$)
    $integrity\_check \leftarrow$ SHA256Check($encrypted\_data$)
    return $encrypted\_data, integrity\_check$
end procedure

function HelperFunctions
    Base64Encode($data$): return $base64.b64encode(data)$
    MapToCodons($data$): return $[codon \mid codon \in generate\_RNA\_codons(data)]$
    FoldRNAStructure($RNA\_sequence$): return $linear\_fold\_algorithm(RNA\_sequence)$
    GenerateDynamicKey($RNA\_pool, salt$): return $pbkdf2\_algorithm(RNA\_pool, salt)$
    EncryptWithKey($RNA\_sequence, key$): return $apply\_encryption(RNA\_sequence, key)$
    SHA256Check($data$): return $sha256(data)$
end function
```

C Performance Evaluation Metrics

This section presents the results of our comprehensive evaluation of the proposed cryptographic method, Crypto-ncRNA, benchmarked against AES-256 and RSA-2048.

Crypto-ncRNA was implemented in Python (v3.12), while AES-256 and RSA-2048 were implemented using the ”pycryptodome” library (v3.21.0). Standard configurations were used: AES-256 in CBC mode with PKCS7 padding (Rijmen & Daemen (2001)), and RSA-2048 with PKCS#1 OAEP padding and SHA-256 hashing (Rivest et al. (1978)).

C.1 Encryption/Decryption Efficiency Test

Encryption and decryption latencies were measured to assess real-time performance. The execution time was calculated as the difference between process start and end timestamps. The data processing efficiency was quantified using:

$$\text{AverageTime} = \frac{\sum_{j=1}^{n}(EndTime_j - StartTime_j)}{n} \tag{2}$$

Where:

- n is the total number of trials.
- $StartTime_j$ / $EndTime_j$ represents the start or end timestamp of trial j respectively.

Process: Tests spanned data lengths from 50 to 100,000 bytes, with results averaged over 500 runs. System call overhead was subtracted to isolate algorithm-specific performance.

Table 2: Encryption Time Comparison (s)

Data Length (Bytes)	Crypto-ncRNA	AES	RSA
50	0.030245502	0.018749273	0.403637892
100	0.030270114	0.018605162	0.451251311
500	0.031469746	0.018759693	0.392945505
1000	0.032204049	0.018854617	0.448887759
5000	0.038968784	0.018410643	0.492652349
10000	0.046719104	0.018931629	0.39583042
50000	0.111085906	0.019108713	0.464615586
100000	0.1916002	0.019194982	0.560739354

Table 3: Decryption Time Comparison (s)

Data Length (Bytes)	Crypto-ncRNA	AES	RSA
50	0.030928	0.0187	0.020927
100	0.030578	0.018578	0.021147
500	0.03122	0.018659	0.024541
1000	0.03207	0.018877	0.029646
5000	0.04038	0.018374	0.064815
10000	0.048945	0.018955	0.108585
50000	0.127293	0.01912	0.464025
100000	0.224574	0.019114	0.904652

As the Table 2&3, Crypto-ncRNA demonstrates compelling efficiency in both encryption and decryption speeds. Notably, it significantly outperforms RSA across all data lengths, showcasing a substantial advantage, especially when handling larger datasets. While AES maintains a slight speed edge over Crypto-ncRNA, particularly at larger data lengths, the performance gap is minimal, and at lower data lengths, Crypto-ncRNA's speed is nearly on par with AES. Crucially, Crypto-ncRNA exhibits a stable and linear increase in encryption and decryption time as data volume grows, indicating consistent and predictable performance scaling, ensuring it remains highly efficient even with increasing data loads, a critical attribute for real-world applications.

C.2 Encryption/Decryption Throughput Performance

The encryption and decryption throughput (in Kilobyte/Second) of AES, RSA, and ncRNA algorithms was evaluated to quantify their efficiency in processing varying data lengths. Throughput is defined as the ratio of data length to execution time, calculated using:

$$\text{Average Decryption Throughput (KiB/s)} = \frac{\sum_{i=1}^{n} \frac{L_i}{t_i}}{n} \times \frac{1}{1024} \tag{3}$$

Where:

- n is the total number of trials.
- L_i represents the data length for trial i.
- t_i the execution time for trial i in seconds (s).

For each algorithm, 500 iterations were performed across data lengths ranging from 50 to 6400 bytes, with randomized input strings.

Table 4: Encryption Time Comparison (KiB/s)

Data Length (Bytes)	Crypto-ncRNA	AES	RSA
50	1.542241	2.595423	0.167258
100	3.08258	5.115825	0.331993
200	6.131219	10.3208	0.755908
400	11.97279	20.60843	1.646416
800	23.9814	41.70408	2.930769
1600	45.62274	82.71863	5.897005
3200	84.69407	166.6902	10.42514

Table 5: Decryption Time Comparison (KiB/s)

Data Length (Bytes)	Crypto-ncRNA	AES	RSA
50	1.547998	2.586265	2.297593
100	3.088367	5.143117	4.510009
200	6.080031	10.34722	8.323793
400	12.07701	20.69467	15.45262
800	23.54036	41.49081	27.31485
1600	45.02909	82.86293	43.77247
3200	83.17577	165.9543	62.56794

Table 4 and 5 are as mentioned in C.1, Crypto-ncRNA achieves impressive encryption and decryption throughput. It significantly outperforms RSA across all data lengths, especially large ones. While AES is slightly faster, Crypto-ncRNA's throughput is comparable, particularly for smaller data. Critically, its throughput scales linearly with data volume, ensuring consistent efficiency even with increasing loads.

C.3 Entropy Test

In cryptography, security fundamentally relies on unpredictability, and entropy quantifies this randomness. For encryption algorithms, higher entropy in ciphertext directly translates to stronger security and greater resistance against attacks (Cachin (1997); Rényi (1961)). We strive for an average entropy approaching the maximum of 8 bits per byte, which represents optimal randomness – the closer to 8, the more unpredictable each byte becomes. This principle is clear: higher entropy equals stronger encryption. To rigorously assess this, we perform entropy testing on ciphertext generated over multiple trials. The following formula calculates the average entropy, considering these trials, to validate the security and reliability of cryptographic systems.

Testing Methodology The formula to calculate the average entropy of ciphertext across multiple trials is:

$$\text{Average Entropy} = -\frac{1}{N \times T} \sum_{t=1}^{T} \sum_{i=1}^{N} \log_2(P(c_{i,t})) \tag{4}$$

Where:

- T is the total number of trials (encryption runs).
- N is the length of the ciphertext in bytes for each trial.
- $c_{i,t}$ represents the i-th byte of the ciphertext in the t-th trial.

For each algorithm, 30 iterations were conducted across data lengths from 50 to 50000 bytes, using randomized input strings.

Table 6: Average Entropy (Maximum = 8)

Data Length (Bytes)	Crypto-ncRNA	AES	RSA
50	7.230238137	6.029898017	7.166932575
100	7.520643336	6.553651309	7.1746127
500	7.906697071	7.603863355	7.739013967
1000	7.954174669	7.808256544	7.875851176
5000	7.990878249	7.962331187	7.972694673
10000	7.995409292	7.981768972	7.986424963
50000	7.99908728	7.996283968	7.997251254
10000	7.999546736	7.998177172	7..998614323

Entropy testing (see Table 6) reveals that the Crypto-ncRNA algorithm exhibits significantly higher entropy values compared to both RSA and AES. This directly underscores a key advantage: elevated entropy signifies enhanced randomness and reduced predictability, crucial factors for bolstering cryptographic security. Specifically, the higher entropy strengthens resistance against statistical analysis and brute-force attacks, potentially improving forward security and resilience to future cryptanalytic techniques. Consequently, entropy analysis indicates that Crypto-ncRNA may offer improved security characteristics relative to RSA and AES.

C.4 Operational Reliability

In cryptography, theoretical soundness is insufficient; flawless implementation is paramount. It is a non-negotiable, fundamental requirement that any encryption scheme guarantees 100% accurate decryption, regardless of data length. Real-world implementations are susceptible to subtle errors, unforeseen interactions, and edge-case vulnerabilities that can compromise integrity. These issues may only surface under specific conditions, making superficial testing inadequate.

Therefore, comprehensive testing that rigorously verifies 100% accurate encryption and decryption across a diverse and exhaustive range of data lengths is indispensable. This testing must include small, large, boundary-adjacent, and randomly chosen data lengths to expose potential padding issues, block cipher mode vulnerabilities, and other implementation flaws. This is not optional; it is a fundamental requirement for building trust, ensuring interoperability, meeting security standards, and, crucially, safeguarding sensitive information. Anything less is a dereliction of duty in secure cryptographic system development. The testing ensures that the system can interact with other systems.

Testing Methodology Cryptographic correctness was evaluated by verifying decryption fidelity across varying data lengths: from 50 to 1000000 bytes. For each length, encrypted data was generated and subsequently decrypted. Decrypted output was compared bit-by-bit to the original plaintext. The success rate, representing the percentage of trials with perfect decryption, was calculated for each data length. This directly assesses the fundamental requirement of perfect decryption in a cryptographic system.

Table 7: Cryptographic Correctness Rate Percentage

Data Length (Bytes)	Total Runs	Enc. Success	Enc. Failure	Dec. Success	Dec. Failure	Success Rate (%)
50	1000	1000	0	1000	0	100.00
100	1000	1000	0	1000	0	100.00
1000	1000	1000	0	1000	0	100.00
100000	1000	1000	0	1000	0	100.00
1000000	1000	1000	0	1000	0	100.00

The Crypto-ncRNA system demonstrated perfect operational reliability in cryptographic correctness testing, as evidenced in Table 7. Across all tested data lengths, both encryption and decryption success rates were consistently 100.00%. This perfect score, achieved over 1000 trials for each data length, indicates that the system reliably encrypts and decrypts data without any bit-level errors, fulfilling the fundamental requirement of 100% decryption accuracy. The system showed no vulnerabilities related to data length, suggesting robust handling of padding, block cipher modes, and other potential implementation-specific issues.

C.5 Statistical Randomness

In cryptography, the strength of an encryption algorithm hinges not just on its mathematical complexity, but critically on the unpredictability of the ciphertext it produces. Any bias, pattern, or predictability in the generated ciphertext can create vulnerabilities, making the encryption susceptible to cryptanalytic attacks and potentially revealing the plaintext. This is where rigorous statistical testing of randomness becomes essential. Weak randomness equates to weak encryption.

To ensure the cryptographic quality and security of our algorithm, and to validate the randomness properties of the PUF-derived outputs, we adhere to the National Institute of Standards and Technology (NIST) Special Publication 800-22, ”A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.” This suite is a widely accepted, comprehensive standard specifically designed for evaluating the randomness of outputs intended for cryptographic use. NIST SP 800-22 is not merely a guideline; it’s a crucial benchmark. Passing these tests provides strong evidence that our algorithm’s output, including the contributions from the PUF, is statistically indistinguishable from a truly random sequence, a fundamental requirement for robust security.

As evidenced in Table 8, the output of our algorithm has demonstrably passed all 15 tests in the NIST SP 800-22 suite, providing statistically significant evidence of its high degree of randomness and strong resistance to cryptanalytic attacks that exploit weaknesses in predictability. This complete and comprehensive success

Table 8: Crypto-ncRNA's NIST SP 800-22 Randomness Test Matrix Results

Test Name	P Value	Pass/Fail (P/F)
Monobit Test	0.5460386853638187	P
Frequency Within Block Test	0.7963189024290873	P
Runs Test	0.10786751132695774	P
Longest Run Ones in a Block Test	0.22084938122535008	P
Binary Matrix Rank Test	0.587708298333639	P
DFT Test	0.8350238760410118	P
Non-overlapping Template Matching Test	0.9999287413136844	P
Overlapping Template Matching Test	0.43308028660774994	P
Maurer's Universal Test	0.8514130113443941	P
Linear Complexity Test	0.824328662851978	P
Serial Test	0.507545477157905	P
Approximate Entropy Test	0.5073170913186321	P
Cumulative Sums Test	0.6611638690391457	P
Random Excursion Test	0.1349606453103914	P
Random Excursion Variant Test	0.039767475276814	P

across every test builds significant trust and confidence in its suitability for security-critical applications. The collective results of these tests offer a robust, multi-faceted, and validating assessment, proving that our algorithm, with its foundation in PUF technology, meets and exceeds the stringent requirements for secure cryptographic use.

Summary Crypto-ncRNA represents a breakthrough in efficiency, security, and reliability (see Appendix C). While its speed and throughput are slightly lower than those of AES-256, they remain well above those of RSA-2048, making Crypto-ncRNA a robust solution for many applications. Its linear scalability is particularly advantageous for big data environments, where predictable performance is essential for managing large-scale processing tasks.

On the security front, Crypto-ncRNA excels by nearly reaching the theoretical maximum entropy of 8 bits per byte. It also passes all NIST randomness tests, demonstrating a high level of unpredictability that is crucial for resisting sophisticated attacks. In rigorous testing, the algorithm achieved a 100% success rate in both encryption and decryption, effectively eliminating common issues such as padding flaws and boundary errors that often plague traditional cryptographic methods.

This deliberate trade-off—sacrificing a modest amount of performance—ensures that Crypto-ncRNA is not merely about speed, but about long-term viability and security in the quantum era. By prioritizing reliability and robustness over maximal throughput, Crypto-ncRNA is well-positioned to address future cryptographic challenges, offering a forward-looking solution that adapts to evolving threats while maintaining strong performance metrics across various applications.