

Crypto-ncRNA: a bio-inspired post-quantum cryptographic primitive exploiting RNA folding complexity

Xu Wang^{*2}, Yiquan Wang^{*1,3}, Tin-Yeh Huang^{*4}, Zhaorui Jiang⁵, Kai Wei^{†1}

¹*Xinjiang Key Laboratory of Biological Resources and Genetic Engineering, College of Life Science and Technology, Xinjiang University, Urumqi, Xinjiang, China*

²*Tsinghua University-Peking University Joint Center for Life Sciences, Tsinghua University, Beijing, China*

³*College of Mathematics and System Science, Xinjiang University, Urumqi, Xinjiang, China*

⁴*Department of Industrial and Systems Engineering, Faculty of Engineering, The Hong Kong Polytechnic University, Hong Kong SAR, China*

⁵*School of Environment and Energy, Shenzhen Graduate School, Peking University, Shenzhen, China*

Abstract

The imminent realization of fault-tolerant quantum computing precipitates a systemic collapse of classical public-key infrastructure and necessitates an urgent transition to post-quantum cryptography. However, current standardization efforts predominantly rely on structured mathematical problems that may remain vulnerable to unforeseen algorithmic breakthroughs, highlighting a critical need for fundamentally orthogonal security paradigms. Here, we introduce *Crypto-ncRNA* as a biophysically inspired cryptographic primitive that exploits the thermodynamic complexity of non-coding RNA folding as a computational work-factor amplifier. By leveraging the rugged energy landscape inherent to RNA secondary structure prediction, a problem intractable to rapid inversion, we establish a security foundation independent of conventional number-theoretic assumptions. We validate this approach by mapping the folding problem to a Quadratic Unconstrained Binary Optimization model and demonstrate theoretical resilience against quantum optimization attacks including the Quantum Approximate Optimization Algorithm. Functioning as a symmetric key encapsulation and derivation primitive dependent on pre-shared seeds, *Crypto-ncRNA* achieves throughputs competitive with software-based Advanced Encryption Standard implementations. By utilizing the generated high-entropy keys within a standard stream cipher framework, it exhibits ciphertext entropy that satisfies rigorous NIST SP 800-22 statistical standards. These findings not only articulate a novel bio-computational pathway for cryptographic defense but also provide a rigorous algorithmic blueprint for future physical realization, demonstrating that the thermodynamic complexity of biological systems offers a robust and physically grounded frontier for securing digital infrastructure in the post-quantum era.

Keywords: Post-Quantum Cryptography; Bio-inspired Security; Physical Unclonable Functions (PUF); RNA Folding

1 Introduction

The imminent realization of fault-tolerant quantum computing precipitates a systemic collapse of classical public-key infrastructure and necessitates an urgent transition to post-quantum cryptography. The security of ubiquitous protocols relies predominantly on the computational difficulty of integer factorization, a problem that becomes efficiently solvable via Shor's algorithm [1]. This systemic vulnerability has catalyzed global standardization efforts to identify cryptographic solutions capable of resisting quantum adversaries [2–7]. The urgency of this transition is further amplified by the prospective threat wherein adversaries stockpile encrypted data for future decryption [8, 9]. While current standardization initiatives focus on mathematical constructions such as lattice-based and code-based cryptography [10–12], these approaches typically rely on structured algebraic hardness assumptions. To hedge against unforeseen algorithmic breakthroughs that might compromise these mathematical foundations, there is a critical imperative to explore fundamentally orthogonal security paradigms that derive their robustness from physical rather than purely number-theoretic complexities.

The intersection of molecular biology and computational theory provides a fertile ground for such alternative paradigms. Since the seminal demonstration of molecular computation for solving combinatorial problems [13], biomolecules have been recognized not merely as genetic storage media but as physical substrates capable of massive parallel processing. Among these biological processes, the folding of ribonucleic acid represents a problem of profound computational intricacy. Unlike the idealized folding funnels often observed in protein dynamics which guide the molecule efficiently toward a native state [14–17], RNA folding landscapes are frequently characterized by severe ruggedness and deep kinetic traps [18]. The prediction of the Minimum Free Energy secondary structure for an RNA sequence involves navigating this complex thermodynamic terrain. While dynamic programming algorithms have been established to solve standard folding problems [19, 20], the in-

^{*}These authors contributed equally to this work.

[†]Corresponding author: kaiwei@xju.edu.cn

clusion of complex topological features such as pseudoknots dramatically escalates the computational demand, rendering general structure prediction and its inverse problem mathematically intractable [21–23].

Here, we introduce *Crypto-ncRNA*, a biophysically inspired cryptographic primitive that utilizes thermodynamic complexity as a computational work-factor amplifier. Distinct from lattice-based or code-based constructs, which rest upon structured algebraic hardness that remains theoretically vulnerable to hidden symmetries or algorithmic inversion, the security of *Crypto-ncRNA* is predicated on the stochastic and chaotic nature of high-dimensional energy landscapes. This introduces a source of entropy that is fundamentally orthogonal to traditional number-theoretic assumptions, thereby providing an irreplaceable layer of defense against mathematical cryptanalysis. By incorporating structural dependencies into the encryption schema, we transform the decryption process into a validation task that necessitates traversing the rugged energy landscape of a simulated RNA molecule. This design effectively treats the biophysical simulation as a computational barrier analogous to a one-way function [24]. To verify a potential key, an adversary is forced to execute a computationally expensive simulation, imposing an $O(N^3)$ complexity penalty characteristic of algorithms like LinearFold [25]. We validate this approach by mapping the folding problem to a Quadratic Unconstrained Binary Optimization model. Our analysis demonstrates that the dense and frustrated nature of the resultant landscape presents a formidable barrier to quantum optimization strategies, including the Quantum Approximate Optimization Algorithm, which typically struggle to locate global minima in glass-like systems [26].

To comprehensively validate the viability of this bio-computational paradigm, this study proceeds by first articulating the algorithmic architecture that transforms digital information into codon sequences and subsequently maps them onto secondary structures. We then rigorously evaluate the statistical quality of the generated ciphertext using the NIST SP 800-22 test suite to ensure indistinguishability from random noise. Following the statistical verification, we assess the quantum resistance of the primitive by simulating a Grover-based search and QAOA attacks on a coherent photonic quantum computer, quantifying the attack success probability against the dense QUBO formulation. Finally, we benchmark the computational throughput of the algorithm against industry standards such as AES and RSA to demonstrate its suitability for high-bandwidth applications [27]. By reconciling the thermodynamic complexity of RNA folding with algorithmic efficiency, this work establishes the conceptual and operational validity of bio-inspired cryptography as a scalable defense mechanism for the post-quantum era.

2 Results

Crypto-ncRNA demonstrates consistent performance across heterogeneous computing environments. This has been validated through benchmarking against classical algorithms, namely RSA-2048 and AES-256 [28–30]. The subsequent

sections and visualizations (Figures 1, 2, 3, and 4) detail its efficiency, throughput, ciphertext randomness, operational reliability, and the characteristics of the underlying key generation module. (Detailed metrics, methodologies, and raw data tables are presented in Appendix).

2.1 Biophysical complexity and structural avalanche effects

To establish the biophysical foundation of our security model, we quantified the entropy introduced by the transformation from digital bits to biological complexity. As visualized in Figure 4, the encryption pipeline integrates a baseline confusion layer, derived from a third-order Cartesian product of nucleotide bases, with a structural permutation layer that exploits the topology of RNA secondary structures. Our sensitivity analysis reveals that this architecture creates a critical error intolerance; minimal deviations in structural label prediction—simulating a corrupted key or approximate folding—trigger widespread index reordering. This phenomenon, effectively a biophysical avalanche effect, enforces a rigorous decryption condition where adversaries are prevented from utilizing approximate structures to derive partial permutation keys. Furthermore, cumulative randomness verification confirms that the synergistic application of codon mapping and structural permutation allows the ciphertext to converge rapidly to an ideal Hamming distance of approximately 0.5, yielding output that is statistically indistinguishable from random noise.

2.2 Statistical validation of ciphertext entropy

The statistical integrity of the generated ciphertext was rigorously verified against the full NIST SP 800-22 test suite (Table 1), confirming that the biophysical encryption process yields cryptographic-quality output. Crucially, the system passed Maurer’s Universal Test (P -value = 0.85), a metric that evaluates the compressibility of the sequence. This result signifies that the output effectively behaves as a high-entropy source free from discernible patterns or algorithmic bias. By satisfying these stringent statistical standards, *Crypto-ncRNA* demonstrates that the chaotic nature of the simulated RNA folding landscape is successfully translated into a random bit-stream capable of resisting statistical cryptanalysis.

2.3 Computational throughput and operational efficiency

Beyond theoretical security, *Crypto-ncRNA* demonstrates operational efficiency suitable for high-bandwidth applications. Comparative benchmarking, as presented in Figure 1, reveals that our method achieves orders-of-magnitude higher throughput than RSA-2048 and maintains a competitive performance profile relative to AES-256. Specifically, for data blocks of 100 KB, *Crypto-ncRNA* requires approximately 0.19s compared to 0.56s for RSA, positioning it as a viable candidate for replacing legacy systems in resource-constrained environments. This balance between computational complexity—required for security—and algorithmic efficiency confirms that the overhead of the RNA folding simulation is manageable for practical deployment without sacri-

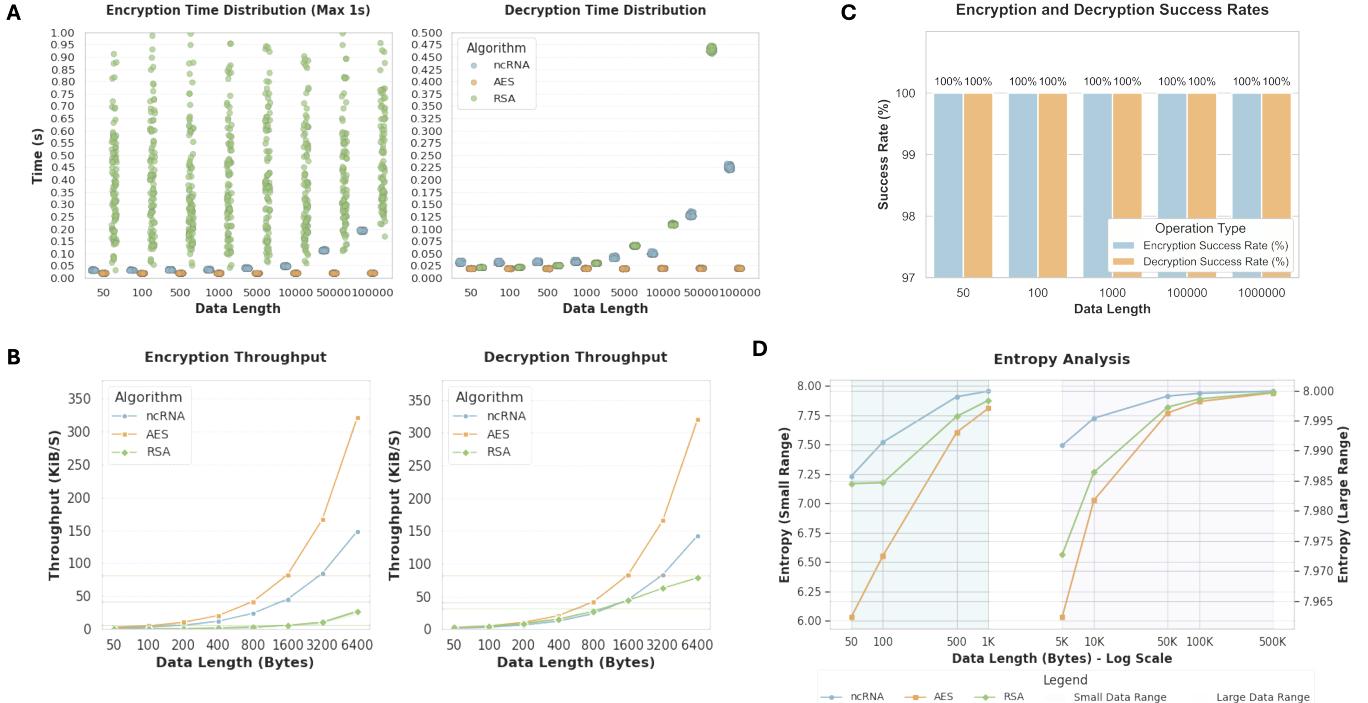


Figure 1: Summary of Algorithm Comparison and Testing Results. (A) Encryption/Decryption Efficiency. Comparison of average encryption and decryption times for Crypto-ncRNA (purple), AES-256 (green), and RSA-2048 (blue). Tests were performed on data lengths from 50 to 100,000 bytes. Time is plotted on a logarithmic scale. (B) Encryption/Decryption Throughput. Throughput in KiB/s is plotted against data length for Crypto-ncRNA, AES-256, and RSA-2048. (C) Ciphertext Randomness (Entropy). The average Shannon entropy per byte of the ciphertext generated by each algorithm is shown for various message lengths. The theoretical maximum entropy is 8.0 bits/byte. (D) Operational Reliability. The percentage of successful decryptions over 1,000 trials for each tested data size. All algorithms were tested on data sizes up to 1MB.

Table 1: 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 | 0.03976475276814 | P |

ficing resistance to quantum adversaries.

2.4 Resistance against quantum optimization and search algorithms

To empirically quantify the resilience of Crypto-ncRNA against quantum adversaries, we executed simulations on a coherent photonic quantum computer by mapping the RNA folding problem to a Quadratic Unconstrained Binary Optimization model. The experimental setup employed a six-

qubit Quantum Approximate Optimization Algorithm circuit that incorporated initialization along with cost and mixer Hamiltonian layers. We introduced implicit hardware noise models typical of Noisy Intermediate-Scale Quantum devices, accounting for factors such as photon loss and coherence time limitations, while restricting the circuit depth to between one and four layers to mitigate severe decoherence. Under these conditions, the attack success probability was calculated based on the divergence between the final convergence energy and the theoretical minimum energy. The resulting probability of approximately 2.1×10^{-13} confirms a robust theoretical defense. While this simulation validates the fundamental hardness of the energy landscape, we acknowledge the scale disparity between this six-qubit model and a full-scale attack, which would necessitate fault-tolerant quantum computing to process the complete matrix. Furthermore, the inherent ruggedness of the RNA folding landscape imposes a significant computational penalty on Grover-based search algorithms. Any oracle query within a Grover attack requires verifying the structural conformation, thereby forcing the adversary to incur an $O(N^3)$ computational cost for each superposition state evaluation and effectively neutralizing the quadratic speedup typically associated with quantum search.

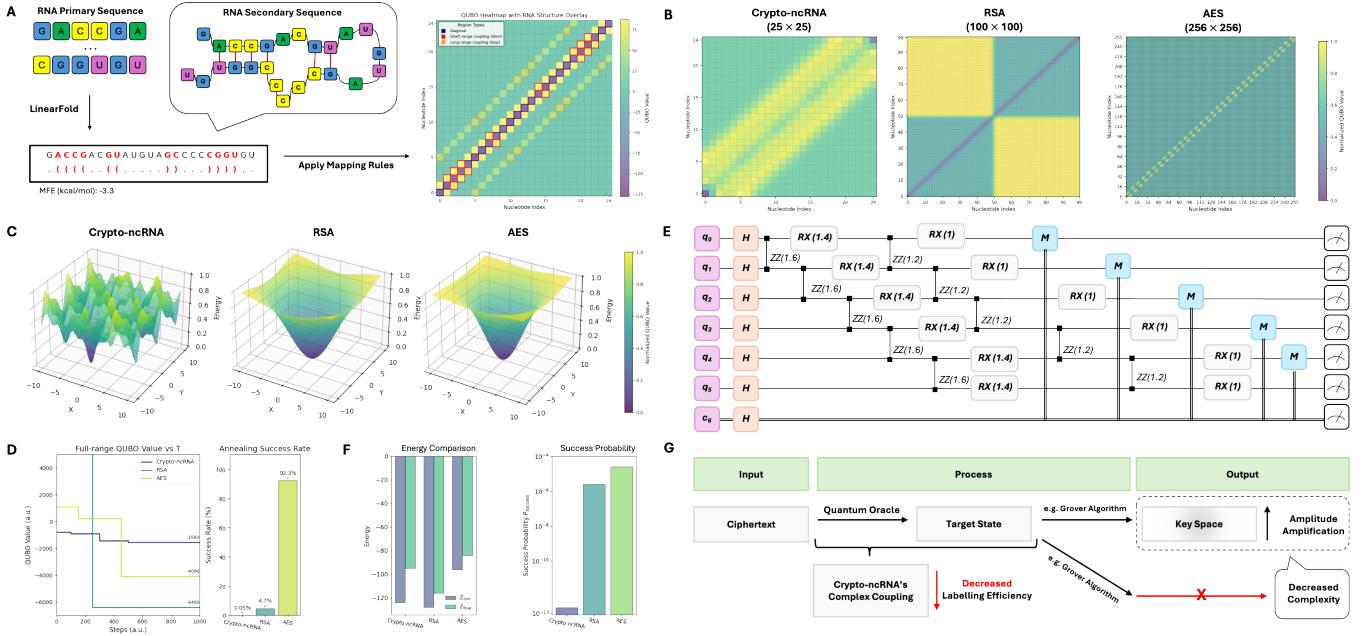


Figure 2: Summary of Quantum Test for Encryption Algorithm. (A) Mapping RNA Folding to QUBO. A diagram illustrating how RNA folding constraints, such as stem pairings and loop structures, are mapped to a banded QUBO matrix with short-range and long-range couplings. (B) QUBO Matrix Comparison. A visual comparison of the QUBO matrix structures for Crypto-ncRNA (banded dense), RSA (block-sparse), and AES (sparse diagonal). (C) Annealing Path Comparison. A conceptual depiction of quantum annealing paths for AES, RSA, and Crypto-ncRNA, showing the different energy landscapes they navigate. (D) Annealing Energy Evolution. A plot of energy evolution curves over annealing time for Crypto-ncRNA (purple), RSA (blue), and AES (green), based on 1000 samples. (E) QAOA Circuit Design. A schematic of the 6-qubit QAOA circuit used for the simulation, showing the initialization, Cost and Mixer layers, and mid-circuit measurement. (F) QAOA Success Probability. The calculated attack success probability for Crypto-ncRNA, RSA, and AES based on the final energy (E_{final}) achieved by the QAOA simulation relative to the theoretical minimum energy (E_{min}). A success is defined as the algorithm finding the exact ground state corresponding to the correct key ($E_{\text{final}} = E_{\text{min}}$). (G) Grover Attack Simulation. A workflow diagram illustrating how the complex coupling in Crypto-ncRNA’s QUBO matrix affects the Oracle and amplitude amplification stages of a Grover-based quantum attack.

3 Discussion

This study introduces Crypto-ncRNA as a post-quantum cryptographic primitive that leverages the simulated biophysical complexity of RNA folding to establish a security foundation orthogonal to traditional number-theoretic assumptions. While current global standardization efforts prioritize lattice-based and code-based cryptography [2, 3, 11], these approaches predominantly rely on structured algebraic hardness. The inherent risk of such mathematical structures is the potential existence of undiscovered symmetries that could be exploited by novel algorithms, a vulnerability strikingly illustrated by the recent breakage of the SIKE algorithm (based on SIDH) via classical attacks targeting its auxiliary torsion points [31]. To mitigate the systemic risk of a monochromatic algorithmic landscape, it is imperative to explore security paradigms rooted in physical entropy rather than purely abstract mathematics. By exploiting the thermodynamic ruggedness of the RNA energy landscape—characterized by deep kinetic traps and frustration [18, 32, 33]—Crypto-ncRNA provides a computational work-factor amplifier that is fundamentally distinct from the alge-

braic structures currently being standardized. In this framework, the industry-standard ChaCha20 cipher acts as the semantic security encapsulation layer, while the core quantum resistance is provided by the RNA-based key derivation process, ensuring that the system benefits from both established engineering reliability and novel bio-physical entropy.

While the present work validates Crypto-ncRNA as a software algorithm, it functions conceptually as a “digital twin” for a future ncRNA-based Physical Unclonable Function (ncRNA-PUF). In this framework, the software implementation serves not merely as a simulation but as a high-fidelity verification of the thermodynamic information density inherent in RNA folding. By enforcing an algorithmic dependency on the secondary structure prediction, specifically utilizing the $O(N^3)$ complexity of the LinearFold algorithm [19, 21, 25], we establish a computational barrier that mimics the physical intractability of measuring a specific molecular conformation without the correct environmental parameters. This approach aligns with the evolution of PUFs as essential trust anchors [34–37], extending the concept of biological feature extraction [38] to create a cryptographic primitive where the “key” is derived from the dynamic behavior of a

virtual biomolecule. This establishes a theoretical security upper bound for the system prior to the introduction of wet-lab experimental constraints.

Transitioning from this *in silico* verification to a physical realization of an ncRNA-PUF presents engineering challenges centered on readout fidelity and noise management; however, recent biotechnological advances outline a concrete roadmap for implementation. The primary challenge of rapid and accurate readout is increasingly addressable via third-generation nanopore sequencing, where recent iterations such as the Oxford Nanopore R10.4 flow cell have demonstrated the capability to resolve homopolymers and single-nucleotide variations with precision sufficient for structural inference [39–44]. A more critical hurdle lies in the stochastic nature of biochemical reactions, which introduces insertion, deletion, and substitution errors that are typically fatal to cryptographic determinism. To bridge the gap between noisy biological substrates and precise digital keys [45], the proposed architecture is compatible with advanced error-correction methodologies adapted from the DNA data storage domain. Specifically, the deployment of indel-correcting codes and robust decoding algorithms has proven effective in recovering error-free data from substantial sequencing noise [46–52]. By integrating these high-fidelity readout technologies with rigorous error-correcting schemes, the thermodynamic entropy captured by our algorithm can be reliably extracted from physical substrates, suggesting that an ncRNA-PUF system is technologically feasible within the near-term horizon.

The realization of such bio-physical security primitives offers distinct advantages over conventional silicon-based hardware security. Silicon PUFs, while widely deployed, have shown vulnerability to advanced machine learning modeling attacks and side-channel analysis, particularly when their challenge-response behaviors can be mathematically approximated [53–59]. Conversely, an ncRNA-PUF derives its security from the high-dimensional and non-linear interactions of molecular folding in solution, a process that resists electronic probing and fault injection attacks [60, 61]. This creates an orthogonal attack surface where security is anchored in chemical dynamics rather than semiconductor manufacturing variations [62–65]. By integrating these biophysical properties with rigorous definitions of quantum unclonability [66, 67], Crypto-ncRNA represents a step toward “bio-convergent security,” positioning biological complexity not just as a medium for storage, but as an active computational shield for the post-quantum digital infrastructure.

4 Materials and Methods

The *Crypto-ncRNA* framework establishes a bio-convergent cryptographic system by leveraging the biophysical properties of non-coding RNA (ncRNA). This paper presents a software algorithm, whose multi-tiered architecture (Figure 3) transforms plaintext into secure ciphertext. While the algorithm is a self-contained software contribution, its security model is inspired by the long-term vision of a physical ncRNA-based Physical Unclonable Function (PUF). A phys-

ical PUF would provide resistance against cloning and physical attacks by introducing molecular-level variability, a concept that informs the design choices and security analysis of the software version presented here.

4.1 The Crypto-ncRNA Computational Framework

The Crypto-ncRNA algorithm functions as a *biophysically-inspired, dual-layer cryptographic system*. Operating entirely *in silico*, it translates the thermodynamic complexity of RNA folding into a computational hardness assumption.

4.1.1 Data Encoding and Cartesian S-Box Generation

The transformation from the binary to the biological domain is achieved through a third-order Cartesian product of the nucleotide set $\{A, U, C, G\}$, which establishes a complete codon codebook comprising 64 unique combinations corresponding to a 6-bit binary input space. Defined as $S_{\text{codon}} = \{A, U, C, G\}^3 \rightarrow \{0, \dots, 63\}$, this mapping provides the substrate for information encoding. To introduce dynamic non-linearity, a user-defined seed drives a Pseudo-Random Number Generator (PRNG) to shuffle the codebook indices, thereby creating a randomized Codon S-Box. This initial substitution layer ensures that identical plaintext inputs map to divergent codon sequences under varying initialization vectors, effectively preconditioning the data before the biological folding simulation.

4.1.2 Security Architecture and Complexity Amplification

The algorithm integrates structural dependencies with statistical masking by utilizing the Structural P-Box, a primitive that exploits the computational intractability of RNA secondary structure prediction. Specifically, the Linear-Fold algorithm is employed to calculate the Minimum Free Energy (MFE) state, yielding a dot-bracket notation that classifies nucleotides into paired stems or unpaired loops. This topological information rigorously dictates the permutation rules, where the sequence is reordered based on structural classifications according to $S_{\text{folded}} \leftarrow \text{FoldPermute}(S_{\text{RNA}}, \text{Structure})$. By linking the permutation logic directly to the thermodynamic state, the system enforces a high sensitivity to input errors; minor deviations in the predicted structure trigger substantial disruptions in the final sequence order. Consequently, inverting this permutation without the precise structural key necessitates solving the RNA inverse folding problem, thereby amplifying the computational work-factor.

To secure this structural information, the folded sequence and permutation indices are encapsulated using the ChaCha20 symmetric stream cipher [68]:

$$C = \text{ChaCha20}(S_{\text{folded}} \parallel I_{\text{perm}}, K_{\text{dynamic}}) \parallel \text{Hash}(S_{\text{folded}})$$

This architecture serves as a computational work-factor amplifier for the pre-shared secret. In scenarios involving brute-force or Grover’s algorithm attacks [69], verifying a candidate key K_{dynamic} requires replicating the folding of the specific pre-shared seed (or password). Because the key derivation is algorithmically bound to the thermodynamic state,

A Sample Case:

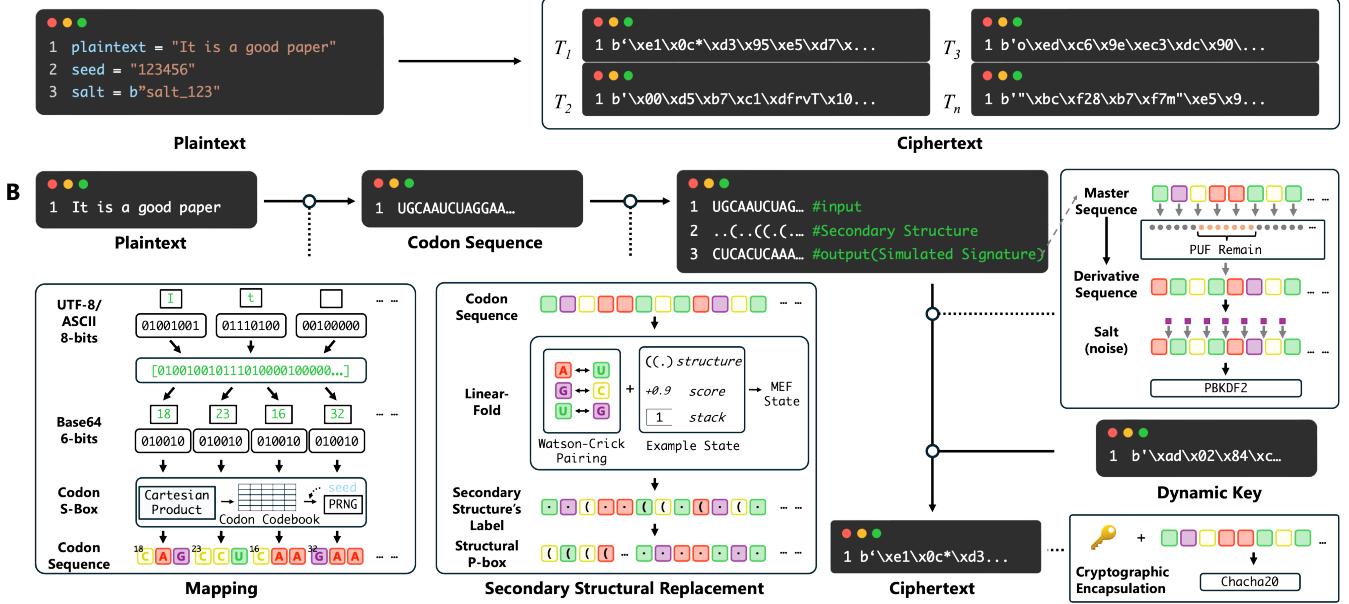


Figure 3: The Computational Workflow and Implementation Architecture of Crypto-ncRNA. (A) Ciphertext Diversity. Demonstrates the algorithm’s sensitivity to initialization parameters. A fixed plaintext combined with varying seeds and salts produces divergent ciphertexts ($T_1 \dots T_n$), ensuring high entropy. (B) Encryption Pipeline. The architecture consists of four sequential stages: 1. Mapping: Plaintext is converted into a codon sequence via a dynamically generated Codon S-Box (derived from a Cartesian product of nucleotides). 2. Structural Replacement: The LinearFold algorithm calculates the Minimum Free Energy (MFE) secondary structure. This topological information drives a Structural P-box to permute the sequence based on stem-loop classifications. 3. Dynamic Key Generation: A Master Sequence is extracted from the folded structure to simulate a PUF response, which is then processed via PBKDF2 to derive a unique session key. 4. Encapsulation: The structurally entangled payload is finally encrypted using ChaCha20 with the derived dynamic key.

validation necessitates running the computationally intensive RNA folding simulation (LinearFold, $O(N^3)$) to derive the correct $\mathbf{K}_{\text{dynamic}}$ from any guessed seed. This requirement imposes a significant computational penalty on every oracle query performed by an adversary trying to recover the seed.

4.2 Simulated Biophysical Key Derivation

While inspired by the theoretical concept of an ncRNA-based Physical Unclonable Function (PUF), the current implementation operates as a *Simulated PUF* within the software domain.

4.2.1 Dynamic Key Generation from Structural Topology

Rather than relying on simple static credentials, the encryption key $\mathbf{K}_{\text{dynamic}}$ is derived dynamically from the unique topological signature of an RNA sequence generated from a pre-shared secret (or password) [38]. A subsequence of this secret-derived folded structure is extracted to serve as a virtual biological response, which is subsequently processed through a key stretching algorithm defined by $\mathbf{K}_{\text{dynamic}} = \text{PBKDF2-HMAC-SHA256}(\Phi(\mathbf{S}_{\text{secret}}), \text{Salt}, 10^4)$ [70].

4.3 Mapping RNA Folding Constraints to QUBO

To quantify quantum hardness, the RNA folding problem is formulated as a Quadratic Unconstrained Binary Optimiza-

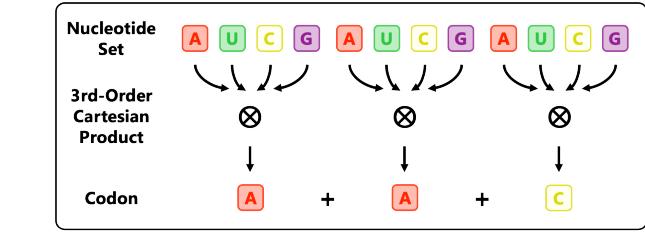
tion (QUBO) model [71]. For an RNA sequence of length N , the state of each nucleotide position i is represented by a binary variable $x_i \in \{0, 1\}$, where $x_i = 1$ denotes the formation of a base pair. The thermodynamic landscape is governed by the energy function $H_{\text{RNA}} = \sum_{i < j} J_{ij}x_i x_j + \sum_i h_i x_i$, where J_{ij} corresponds to pairing energies consistent with Watson-Crick rules. This Hamiltonian is subsequently transformed into the standard QUBO matrix form $H_{\text{QUBO}} = \mathbf{x}^T Q \mathbf{x}$. The resulting matrix Q incorporates dense coupling terms ($Q_{i,i+1} \approx 88$) derived from stem stacking constraints and long-range couplings ($Q_{i,i+5} \approx 44$) introduced by loop permutation rules, creating cross-dimensional interference that generates a rugged energy landscape resistant to quantum optimization [72].

The matrix Q incorporates dense coupling terms ($Q_{i,i+1} \approx 88$) derived from stem stacking constraints, and long-range couplings ($Q_{i,i+5} \approx 44$) introduced by the loop permutation rules. These constraints create cross-dimensional interference, resulting in a rugged energy landscape difficult for quantum optimizers to traverse.

4.4 Quantum Resistance Verification via QAOA

We evaluated the algorithm’s resilience using the Quantum Approximate Optimization Algorithm (QAOA). The target is to find the ground state of the Hamiltonian H_C encoding the

A Sample Case:



Permutated Seed: ... →
Codon Codebook (Combinatorial Space): 0 1 2 3 4 5 6 7
AAA AAC AAG AAU ACA ACC ACG ACU
8 9 10 11 12 13 14 15
AGA AGC AGG AGU AUC AUG AUU
16 17 18 19 20 21 22 23
CAA CAC CAG CAU CCC CCG CCA
24 25 26 27 28 29 30 31
CGA CGC CGG CGU CUA CUC CGU CGU
32 33 34 35 36 37 38 39
GAA GAC GAG GAU GCA GCC GCG GCU
40 41 42 43 44 45 46 47
GGA GGC GGG GGU GUA GUC GUG GUU
48 49 50 51 52 53 54 55
UAA UAC UAG UAU UCA UCC UCG UCU
56 57 58 59 60 61 62 63
UGA UGC UGG UGU UUA UUC UUG UUU

Codon S-Box: 23 P-0 25 P-1 7 ACU 22 P-3 45 P-2 GUC 33 P-4 GAC 19 P-5 CAU 59 P-6 UGU
46 P-7 9 P-8 40 P-9 18 P-10 42 P-11 31 P-12 16 P-13 39 P-14 48 P-15 36 P-16 41 P-17 29 P-18 20 P-19 11 P-20 50 P-21 26 P-22 57 P-23 54 P-24 89 P-25 GCA GGC 24 P-26 55 P-27 4 P-28 57 P-29 10 P-30 30 P-31 60 P-32 28 P-33 44 P-34 26 P-35 12 P-36 35 P-37 53 P-38 32 P-39 58 P-40 13 P-41 102 P-42 56 P-43 52 P-44 137 P-45 91 P-46 31 P-47 127 P-48 1 UAU 2 AAG CGU 27 P-49 37 P-50 5 34 P-51 43 P-52 1 P-53 1 UUG 61 UUC AGA 8 P-54 63 UAU 15 P-55 77 P-56 34 P-57 47 P-58 1 P-59 34 P-60 1 AUG

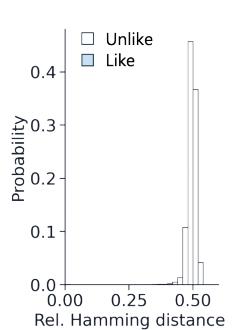
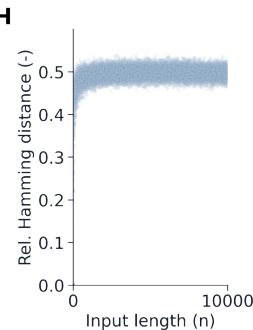
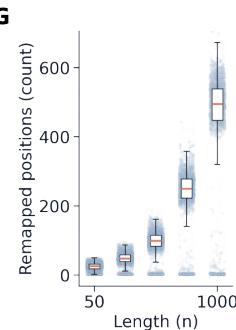
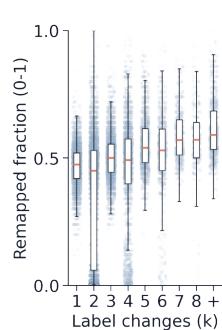
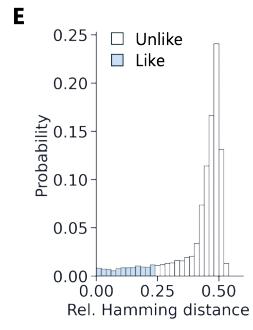
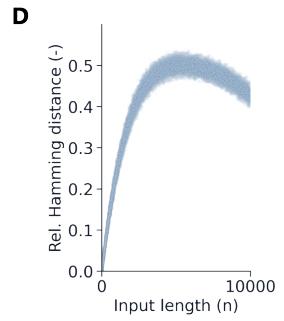
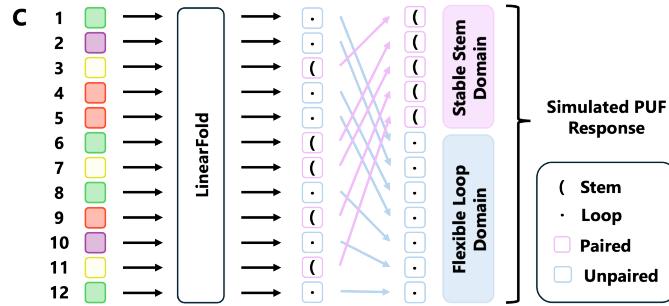
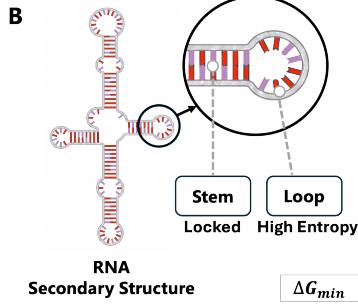


Figure 4: Biophysical Mapping Principles and Statistical Validation of Structural Entanglement. (A–C) Construction of Bio-inspired Primitives. The transformation from digital bits to biological complexity. (A) illustrates the Codon S-Box generation via a 3rd-order Cartesian product of nucleotides ($4^3 = 64$), mapping 6-bit inputs to a randomized codon codebook. (B–C) depict the Structural P-Box, where the LinearFold algorithm derives secondary structures (stems vs. loops) to topologically permute the sequence. (D–G) Sensitivity and Error Intolerance Analysis. A statistical quantification of the algorithm’s security properties. While (D–E) show the baseline randomness of the S-Box alone, (F–G) critically demonstrate the structural avalanche effect of the P-Box. The results indicate that even minimal errors in structural labeling (small k) trigger widespread index remapping. (H–I) Cumulative Randomness Verification. Validation of the full system (S-Box + P-Box). The results show a rapid and stable convergence to an ideal Hamming distance of ≈ 0.5 with over 99% confidence.

QUBO problem:

$$H_C = \sum_i Q_{ii} Z_i + \sum_{i < j} Q_{ij} Z_i \otimes Z_j$$

The QAOA evolution involves alternating applications of the cost Hamiltonian H_C and a mixer Hamiltonian $H_M = \sum X_i$:

$$|\psi(\gamma, \beta)\rangle = \prod_{k=1}^p e^{-i\beta_k H_M} e^{-i\gamma_k H_C} |+\rangle^{\otimes n}$$

The success probability of a quantum attack is defined as the probability of measuring the state corresponding to the correct key (global minimum energy E_{\min}):

$$P_{\text{success}} = |\langle \mathbf{x}_{\text{key}} | \psi(\gamma, \beta) \rangle|^2 \approx \exp(-(E_{\text{final}} - E_{\min}))$$

Our simulations on a coherent photonic quantum computer (CPQC-1) [73] indicate that Crypto-ncRNA’s QUBO matrix

exhibits a negligible success probability ($P_{\text{success}} \approx 2.1 \times 10^{-13}$), confirming robust resistance against near-term quantum attacks.

4.5 Implementation, Benchmarking, and Statistical Validation

The Crypto-ncRNA framework was implemented in Python (v3.12), utilizing standard libraries for numerical computation and cryptographic operations to ensure reproducibility. Comparative benchmarking was conducted against classical algorithms using the pycryptodome library (v3.21.0) [74], specifically employing AES-256 in Cipher Block Chaining (CBC) mode with PKCS7 padding [75] and RSA-2048 with PKCS#1 Optimal Asymmetric Encryption Padding (OAEP) [76]. To verify the cryptographic integrity of the generated ciphertext, the output was subjected to the NIST SP 800-22

Statistical Test Suite [77, 78]. This assessment involved analyzing ciphertext samples from multiple independent trials across varying message lengths to rigorously quantify indistinguishability from random noise, ensuring the system meets established security standards for cryptographic applications.

Acknowledgments

This work was supported by the Natural Science Foundation of Xinjiang Uygur Autonomous Region (Grant Number: 2024D01C216) and the “Tianchi Talents” introduction plan. We acknowledge QBoson Quantum Technology for providing access to their CPQC-1 quantum computer and Kaiwu SDK for the quantum evaluation portion of this study.

Declarations

Author Contributions

X.W., Y.W., and T.-Y.H. designed and performed research; T.-Y.H. prepared figures; K.W. provided funding, supervision, and contributed to manuscript editing; and X.W., Y.W., T.-Y.H., and Z.J. contributed to manuscript editing.

Competing Interests

The authors declare no competing interests.

Code Availability

The code used in this article can be obtained from GitHub: <https://github.com/JLU-WangXu/crypto-ncRNA>

References

- [1] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE, November 1994.
- [2] Lily Chen, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, et al. Report on post-quantum cryptography. Technical report, US Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2016.
- [3] Gorjan Alagic, Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, et al. Status report on the third round of the nist post-quantum cryptography standardization process. Technical report, NIST, 2022.
- [4] Gorjan Alagic, Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, et al. Status report on the first round of the nist post-quantum cryptography standardization process. Technical report, NIST, 2019.
- [5] C. Balamurugan, K. Singh, G. Ganesan, and M. Rajarajan. Post-quantum and code-based cryptography—some prospective research directions. *Cryptography*, 5(4):38, 2021.
- [6] Rutuja Bavdekar, Esha J Chopde, Ayush Agrawal, Anshul Bhatia, and Kavita Tiwari. Post quantum cryptography: a review of techniques, challenges and standardizations. In *2023 International Conference on Information Networking (ICOIN)*, pages 146–151. IEEE, january 2023.
- [7] Mohit Kumar and Prasant Pattnaik. Post quantum cryptography (pqc)-an overview. In *2020 IEEE High Performance Extreme Computing Conference (HPEC)*, pages 1–9. IEEE, september 2020.
- [8] David Ott and Chris Peikert. Identifying research challenges in post quantum cryptography migration and cryptographic agility. *arXiv preprint arXiv:1909.07353*, 2019.
- [9] Harpreet Singh. Managing the quantum cybersecurity threat: Harvest now, decrypt later. In *Quantum Computing*, pages 142–158. CRC Press, 2023.
- [10] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, and D. Smith-Tone. Status report on the second round of the NIST post-quantum cryptography standardization process. Technical report, National Institute of Standards and Technology (NIST), 2020. NISTIR 8309.
- [11] D. J. Bernstein and T. Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, 2017.
- [12] K Basu, D Soni, M Nabeel, and R Karri. Nist post-quantum cryptography-a hardware evaluation study. *Cryptology ePrint Archive*, 2019.
- [13] L. M. Adleman. Molecular computation of solutions to combinatorial problems. *Science*, 266(5187):1021–1024, 1994.
- [14] P. E. Leopold, M. Montal, and J. N. Onuchic. Protein folding funnels: a kinetic approach to the sequence-structure relationship. *Proceedings of the National Academy of Sciences*, 89(18):8721–8725, 1992.
- [15] J. D. Bryngelson, J. N. Onuchic, N. D. Soccia, and P. G. Wolynes. Funnels, pathways, and the energy landscape of protein folding: a synthesis. *Proteins: Structure, Function, and Bioinformatics*, 21(3):167–195, 1995.
- [16] J. N. Onuchic, Z. Luthey-Schulten, and P. G. Wolynes. Theory of protein folding: the energy landscape perspective. *Annual review of physical chemistry*, 48(1):545–600, 1997.
- [17] O. F. Kuzu, L. J. T. Granerud, and F. Saatcioglu. Navigating the landscape of protein folding and proteostasis: from molecular chaperones to therapeutic innovations. *Signal Transduction and Targeted Therapy*, 10(1):358, 2025.

- [18] S. V. Solomatin, M. Greenfeld, S. Chu, and D. Herschlag. Multiple native states reveal persistent ruggedness of an rna folding landscape. *Nature*, 463(7281):681–684, 2010.
- [19] M. Zuker and P. Stiegler. Optimal computer folding of large rna sequences using thermodynamics and auxiliary information. *Nucleic acids research*, 9(1):133–148, 1981.
- [20] M. Zuker and D. Sankoff. Rna secondary structures and their prediction. *Bulletin of Mathematical Biology*, 46(4):591–621, 1984.
- [21] E. Rivas and S. R. Eddy. A dynamic programming algorithm for rna structure prediction including pseudoknots. *Journal of molecular biology*, 285(5):2053–2068, 1999.
- [22] T. Akutsu. Dynamic programming algorithms for rna secondary structure prediction with pseudoknots. *Discrete Applied Mathematics*, 104(1-3):45–62, 2000.
- [23] R. Masuki, D. Liew, and E. H. Yong. Hierarchical analysis of rna secondary structures with pseudoknots based on sections. *PLOS Computational Biology*, 22(1):e1013904, 2026.
- [24] J. Katz and Y. Lindell. *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC, 2007.
- [25] 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.
- [26] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum approximate optimization algorithm. *arXiv preprint arXiv:1411.4028*, 2014.
- [27] M. Sommerhalder. Hardware security module. In *Trends in Data Protection and Encryption Technologies*, pages 83–87, 2023.
- [28] 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.
- [29] D. Selent. Advanced encryption standard. *Rivier Academic Journal*, 6(2):1–14, 2010.
- [30] National Institute of Standards and Technology. Advanced encryption standard (aes). Technical Report FIPS PUB 197, U.S. Department of Commerce, November 2001.
- [31] W. Castryck and T. Decru. An efficient key recovery attack on SIDH. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 423–447, Cham, April 2023. Springer Nature Switzerland.
- [32] I. Tinoco Jr and C. Bustamante. How rna folds. *Journal of Molecular Biology*, 293(2):271–281, 1999.
- [33] S. J. Chen and K. A. Dill. Rna folding energy landscapes. *Proceedings of the National Academy of Sciences*, 97(2):646–651, 2000.
- [34] Roel Maes and Ingrid Verbauwhede. Physically unclonable functions: A study on the state of the art and future research directions. In *Towards Hardware-Intrinsic Security: Foundations and Practice*, pages 3–37, 2010.
- [35] Roel Maes. Physically unclonable functions: Concept and constructions. In *Physically unclonable functions: constructions, Properties and applications*, pages 11–48. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
- [36] Yang Gao, Said F Al-Sarawi, and Derek Abbott. Physical unclonable functions. *Nature Electronics*, 3(2):81–91, 2020.
- [37] B. Cambou, M. Gowanlock, B. Yildiz, D. Ghahaimian-doab, 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.
- [38] W. Zhou, D. Melamed, G. Banyai, et al. Expanding the binding specificity for rna recognition by a puf domain. *Nature Communications*, 12:5107, 2021.
- [39] D. Branton, D. W. Deamer, A. Marziali, H. Bayley, S. A. Benner, T. Butler, M. Di Ventra, S. Garaj, M. Gracheva, D. Ly, J. Makaric, A. Meller, M. Wanunu, and J. A. Schloss. The potential and challenges of nanopore sequencing. *Nature biotechnology*, 26(10):1146–1153, 2008.
- [40] D. Deamer, M. Akeson, and D. Branton. Three decades of nanopore sequencing. *Nature biotechnology*, 34(5):518–524, 2016.
- [41] Y. Wang, Y. Zhao, A. Bollas, Y. Wang, and K. F. Au. Nanopore sequencing technology, bioinformatics and applications. *Nature biotechnology*, 39(11):1348–1365, 2021.
- [42] Y. Ni, X. Liu, Z. M. Simeneh, M. Yang, and R. Li. Benchmarking of Nanopore R10. 4 and R9. 4.1 flow cells in single-cell whole-genome amplification and whole-genome shotgun sequencing. *Computational and Structural Biotechnology Journal*, 21:2352–2364, 2023.
- [43] T. Zhang, H. Li, S. Ma, J. Cao, H. Liao, Q. Huang, and W. Chen. The newest Oxford Nanopore R10. 4.1 full-length 16S rRNA sequencing enables the accurate resolution of species-level microbial community

- profiling. *Applied and environmental microbiology*, 89(10):e00605–23, 2023.
- [44] N. D. Sanderson, N. Kapel, G. Rodger, H. Webster, S. Lipworth, T. L. Street, et al. Comparison of R9. 4.1/Kit10 and R10/Kit12 Oxford Nanopore flowcells and chemistries in bacterial genome reconstruction. *Microbial genomics*, 9(1):000910, 2023.
- [45] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Advances in Cryptology – EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques*, volume 3027 of *Lecture Notes in Computer Science*, pages 523–540. Springer Berlin Heidelberg, 2004.
- [46] W. H. Press. Fast trimer statistics facilitate accurate decoding of large random DNA barcode sets even at large sequencing error rates. *PNAS Nexus*, 1(5):pgac252, 2022.
- [47] J. A. Hawkins, S. K. Jones Jr, I. J. Finkelstein, and W. H. Press. Indel-correcting DNA barcodes for high-throughput sequencing. *Proceedings of the National Academy of Sciences*, 115(27):E6217–E6226, 2018.
- [48] L. Organick, S. D. Ang, Y. J. Chen, R. Lopez, S. Yekhanin, K. Makarychev, et al. Random access in large-scale DNA data storage. *Nature biotechnology*, 36(3):242–248, 2018.
- [49] T. Heinis, R. Sokolovskii, and J. J. Alnasir. Survey of information encoding techniques for DNA. *ACM Computing Surveys*, 56(4):1–30, 2023.
- [50] E. Bencurova, A. Akash, R. C. Dobson, and T. Dan-dekar. DNA storage—from natural biology to synthetic biology. *Computational and Structural Biotechnology Journal*, 21:1227–1235, 2023.
- [51] W. H. Press and J. A. Hawkins. An indel-resistant error-correcting code for DNA-based information storage. *arXiv preprint arXiv:1812.01112*, 2018.
- [52] W. H. Press, J. A. Hawkins, S. K. Jones Jr, J. M. Schaub, and I. J. Finkelstein. HEDGES error-correcting code for DNA storage corrects indels and allows sequence constraints. *Proceedings of the National Academy of Sciences*, 117(31):18489–18496, 2020.
- [53] 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.
- [54] F. Gebali and M. Mamun. Review of physically unclonable functions (pufs): Structures, models, and algorithms. *Frontiers in Sensors*, 2:751748, 2022.
- [55] A. Maiti, V. Gunreddy, and P. Schaumont. A systematic method to evaluate and compare the performance of physical unclonable functions. In *Embedded systems design with FPGAs*, pages 245–267. Springer New York, New York, NY, 2012.
- [56] G. T. Becker. The gap between promise and reality: On the insecurity of XOR arbiter PUFs. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 535–555, Berlin, Heidelberg, September 2015. Springer Berlin Heidelberg.
- [57] N. P. Bhatta and F. Amsaad. Advancing PUF security machine learning assisted modeling attacks. In *2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 805–808. IEEE, July 2024.
- [58] C. Shepherd, K. Markantonakis, N. Van Heijningen, D. Abulkassimi, C. Gaine, T. Heckmann, and D. Naccache. Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis. *Computers & Security*, 111:102471, 2021.
- [59] S. Kaur, B. Singh, and H. Kaur. Stratification of hardware attacks: Side channel attacks and fault injection techniques. *SN Computer Science*, 2(3):183, 2021.
- [60] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas. PUF modeling attacks on simulated and silicon data. *IEEE transactions on information forensics and security*, 8(11):1876–1891, 2013.
- [61] H. Wang, W. Hao, Y. Tang, B. Zhu, W. Dong, and W. Liu. Deep neural network modeling attacks on arbiter-PUF-based designs. *Cybersecurity*, 8(1):11, 2025.
- [62] 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.
- [63] 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.
- [64] M. Mondal and K. S. Ray. Review on dna cryptography. *International Journal of Bioinformatics and Intelligent Computing*, 2(1):44–72, 2023.
- [65] H. Im, J. Yoon, B. So, J. Choi, D. H. Park, S. Kim, and W. Park. Four-dimensional physical unclonable functions and cryptographic applications based on time-varying chaotic phosphorescent patterns. *ACS Nano*, 18(18):11703–11716, 2024.
- [66] M. Arapinis, M. Delavar, M. Doosti, and E. Kashefi. Quantum physical unclonable functions: Possibilities and impossibilities. *Quantum*, 5:475, 2021.

- [67] Y. Zhang, F. Wang, J. Chao, M. Xie, H. Liu, M. Pan, and C. Fan. DNA origami cryptography for secure communication. *Nature Communications*, 10(1):5469, 2019.
- [68] Daniel J. Bernstein. Chacha, a variant of salsa20. In *Workshop Record of SASC*, volume 8, pages 3–5, jan 2008.
- [69] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.
- [70] Burt Kaliski. Pkcs #5: Password-based cryptography specification version 2.0. RFC 2898, IETF, September 2000.
- [71] Fred Glover, Gary Kochenberger, and Yu Du. A tutorial on formulating and using qubo models. *arXiv preprint arXiv:1811.11538*, 2018.
- [72] Tadashi Kadowaki and Hidetoshi Nishimori. Quantum annealing in the transverse ising model. *Physical Review E*, 58(5):5355, 1998.
- [73] QBoson Quantum Technology. Overview — kaiwu sdk documentation. <https://kaiwu-sdk-docs.qboson.com/en/source/introduction.html>, 2022. Accessed: 2025-08-01.
- [74] The PyCryptodome contributors. Pycryptodome. <https://www.pycryptodome.org/>, 2024. Version 3.21.0.
- [75] B. Kaliski. PKCS#7: Cryptographic Message Syntax Version 1.5. RFC 2315, IETF, 1998.
- [76] K. Moriarty, B. Kaliski, J. Jonsson, and A. Rusch. PKCS#1: RSA Cryptography Specifications Version 2.2. RFC 8017, IETF, 2016.
- [77] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, and San Vo. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical Report SP 800-22, US Department of Commerce, Technology Administration, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2001.
- [78] Lawrence E Bassham III, Andrew L Rukhin, Juan Soto, James R Nechvatal, Miles E Smid, Elaine B Barker, Stefan D Leigh, Mark Levenson, Mark Vangel, and David L Banks. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Technical Report SP 800-22 Rev. 1a, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2010.