

Lightweight IoT Encryption Using a Hierarchical DNA–Cellular Automata Cryptosystem with Random Mutations

Mircea Țălu^{1,2*}

¹Department of Computer Science, Faculty of Automation and Computer Science, The Technical University of Cluj-Napoca, 26-28 George Barițiu St., Cluj-Napoca, 400027, Cluj County, Romania

²SC ACCESA IT SYSTEMS SRL, Constanța St., no. 12, Platinia, CP. 400158, Cluj-Napoca, Romania

Article Info

Article history:

Received June 28, 2026

Revised July 25, 2026

Accepted August 28, 2026

Keywords:

DNA cryptography

IoT security

Lightweight encryption

Cellular automata

Mutation-driven diffusion

ABSTRACT

Resource-constrained Internet of Things (IoT) devices require lightweight cryptographic mechanisms that provide strong security with minimal computational and energy overhead. This study presents a hierarchical Deoxyribonucleic Acid (DNA)–Cellular Automata (DNA–CA) cryptosystem enhanced with biologically inspired random mutations, designed for ultra-low-power IoT nodes. Plaintext data are encoded into DNA (Deoxyribonucleic Acid) sequences, processed through multi-layer cellular automata with dynamic, state-dependent keys, and subjected to controlled pre- and post-encryption mutations to enhance diffusion, entropy, and resistance to differential and statistical attacks. The system was implemented and evaluated on six heterogeneous microcontrollers spanning 8-, 16-, and 32-bit architectures, including ATmega4809-P, dsPIC33CH128MP, MSP430FR6989, STM32L5, nRF52840, and ESP32-C3, representing sensors, industrial controllers, wireless nodes, and edge platforms. Experimental results demonstrate near-ideal Shannon entropy (7.97 ± 0.02 bits/byte), avalanche $\approx 50.1\%$, NPCR $\approx 99.6\%$, UACI $\approx 33.0\%$, key sensitivity $\approx 50\%$, and negligible ciphertext correlation ($-0.004 < r < 0.006$). Memory and energy requirements are modest (4–6 KB ROM, <1.5 KB RAM, microjoule-level energy per encryption). Ablation studies confirm that mutation layers critically enhance entropy, diffusion, and differential resistance. Overall, the hierarchical DNA–CA cryptosystem offers a scalable, energy-efficient, and highly secure lightweight encryption framework suitable for heterogeneous IoT deployments.

This is an open access article under the CC BY-SA license.



1. INTRODUCTION

The rapid proliferation of IoT and IIoT technologies has enabled pervasive connectivity across industrial automation, smart environments, energy systems, manufacturing, and distributed sensing [1]–[3], while introducing significant challenges related to security, energy efficiency, scalability, and intelligent system management [4]–[8]. Emerging research underscores that IoT and IIoT systems face a wide range of cybersecurity threats, necessitating the development of robust security frameworks, countermeasures, and an understanding of evolving attack scenarios [9]–[13]. However, IoT devices are typically resource-constrained, with limited memory, computational capability, and energy resources [14]–[17], rendering conventional cryptographic algorithms impractical [18]–[28].

Despite the considerable progress achieved in lightweight cryptography for IoT, existing approaches still exhibit several important limitations. Many DNA-based and cellular automata-based schemes rely on static encoding rules, fixed key-generation mechanisms, or single-layer architectures, while comprehensive validation on heterogeneous embedded microcontrollers remains limited. Consequently, there is a need for a lightweight encryption framework that simultaneously provides hierarchical security, adaptive key evolution, mutation-enhanced diffusion, and experimentally verified efficiency across resource-constrained IoT platforms.

*Corresponding Author

Email: mircea.talu@accesa.eu

One promising strategy for addressing this challenge is DNA-based cryptography, which encodes digital information using deoxyribonucleic acid (DNA) sequences composed of the four nucleotides—adenine (A), thymine (T), cytosine (C), and guanine (G). Binary data are mapped to nucleotide representations to create high-entropy symbolic structures and vastly expanded key spaces. Beyond encoding, DNA-based cryptographic schemes employ bio-inspired operations such as substitution, mutation, crossover, and logical transformations to enhance confusion and diffusion, thereby improving resistance against statistical and cryptanalytic attacks [15]–[17]. DNA cryptographic methods exploit the inherent randomness and combinatorial richness of DNA sequences, enabling flexible key generation and enhanced diffusion and confusion properties in encryption operations. Recent studies have demonstrated the potential of DNA-based encryption for lightweight security applications, particularly in IoT environments where conventional cryptographic algorithms such as the Advanced Encryption Standard (AES) and the Rivest–Shamir–Adleman (RSA) scheme may be impractical due to limitations in computational capability, memory resources, and energy availability [29]–[33]. Unlike the approach in [29], which integrates cellular automata (CA) with DNA cryptographic operations in a single-layer framework without adaptive feedback, the proposed method introduces a hierarchical multi-layer architecture with dynamic CA-driven key evolution and mutation-enhanced diffusion applied both before and after encryption stages. Cellular automata have been widely adopted in lightweight cryptographic frameworks due to their ability to generate high-entropy pseudo-random sequences and complex nonlinear transformations using simple local rules, making them suitable for hardware-efficient implementations in resource-constrained IoT environments [34]–[37].

In this article, we propose a hierarchical DNA cryptosystem that integrates multi-layer cellular automata with biologically inspired stochastic mutations to achieve robust security performance on resource-constrained IoT platforms. The system encodes data into DNA sequences, generates dynamic encryption keys through cellular automata evolution, and applies controlled random mutations to enhance diffusion and strengthen resistance against differential and statistical cryptanalysis. Crucially, the cryptosystem is experimentally evaluated across six representative microcontroller units (MCUs) spanning 8-, 16-, and 32-bit architectures, providing a comprehensive assessment of memory footprint, throughput, energy consumption, and overall security robustness.

To address these limitations, this work proposes a hierarchical DNA–Cellular Automata cryptosystem integrating dynamic DNA encoding, multi-layer cellular automata key evolution, biologically inspired stochastic mutations, and hierarchical feedback. The proposed architecture is specifically designed to maximize entropy, diffusion, and key sensitivity while maintaining low computational complexity and energy consumption suitable for heterogeneous IoT microcontrollers.

The main contributions of this work are summarized as follows:

- A hierarchical DNA–Cellular Automata cryptosystem with mutation-driven diffusion for IoT security.
- A multi-layer encryption architecture combining DNA encoding, CA evolution, and stochastic mutation.
- A lightweight implementation validated on heterogeneous MCU platforms (8-, 16-, and 32-bit).
- Comprehensive evaluation of security and efficiency metrics under constrained environments.

Experimental evaluation performed on six representative 8-, 16-, and 32-bit microcontroller platforms demonstrates that the proposed cryptosystem achieves near-ideal Shannon entropy (7.97 ± 0.02 bits/byte), avalanche ratio ($\sim 50.1\%$), NPCR ($\sim 99.6\%$), UACI ($\sim 33.4\%$), key sensitivity ($\sim 50\%$), negligible ciphertext correlation, and microjoule-level energy consumption. These results confirm that the proposed hierarchical DNA–CA cryptosystem provides a practical balance between lightweight implementation efficiency and strong cryptographic security for heterogeneous IoT environments. The remainder of this paper is organized as follows: Section 1 presents the introduction. Section 2 provides the literature review. Section 3 presents the proposed methodology and system design. Section 4 provides the experimental results and security evaluation. Section 5 discusses the findings and system limitations. Finally, Section 6 concludes the paper and outlines future research directions.

2. LITERATURE REVIEW

2.1. DNA Cryptography and Cellular Automata Approaches

DNA-based cryptography has been widely studied due to its high entropy representation and large key space obtained through nucleotide encoding [15]–[17]. These methods typically map binary data into DNA sequences (A, T, C, G) and apply operations such as substitution, complement, and permutation to enhance confusion and diffusion. However, most existing approaches rely on static encoding rules, which limit adaptability under dynamic attack scenarios.

Cellular automata (CA) have also been extensively used in lightweight cryptographic systems due to their ability to generate pseudo-random sequences using simple local transition rules [34]–[37]. While CA-based schemes provide computational efficiency, they often suffer from predictable evolution patterns when not combined with additional nonlinear mechanisms.

2.2. Recent Hybrid and Lightweight Cryptographic Schemes

Recent research has focused on hybrid cryptographic models combining DNA encoding, chaotic systems, and cellular automata to improve security in IoT environments [29]-[33]. These approaches demonstrate improved diffusion and randomness compared to classical lightweight ciphers such as ARX- or SPN-based designs. However, most recent methods remain limited in one or more of the following aspects: lack of hierarchical structure, absence of adaptive key evolution, and insufficient evaluation on heterogeneous IoT hardware. In addition, many schemes are validated only in simulation environments without deployment on real microcontroller platforms. Recent studies have also explored DNA-based key derivation combined with metadata fingerprinting for secure IoT forensic applications, highlighting the potential of DNA-inspired mechanisms in constrained environments; however, these approaches primarily focus on authentication and traceability rather than lightweight encryption and diffusion enhancement [38].

2.3. Identified Research Gaps and Motivation

Despite significant progress, several critical gaps remain in the current state-of-the-art lightweight cryptographic systems:

- Lack of hierarchical architectures that combine multiple security layers in a unified framework.
- Absence of mutation-driven mechanisms for dynamic diffusion enhancement.
- Limited cross-platform validation across heterogeneous MCU architectures (8-, 16-, and 32-bit).
- Insufficient energy-aware design for ultra-low-power IoT deployments.
- Weak integration between DNA encoding and cellular automata evolution for adaptive key generation.

These limitations require unified, lightweight, and adaptive cryptographic frameworks to ensure secure and efficient IoT operation under emerging cyber threats [39]-[52].

The novelty of the present work lies in the unified integration of hierarchical DNA encoding, multi-layer cellular automata, mutation-driven diffusion, and adaptive feedback within a single lightweight cryptographic framework, together with comprehensive experimental validation on six heterogeneous microcontroller architectures representative of practical IoT deployments.

3. METHOD

The proposed cryptosystem implements a hierarchical DNA-based encryption framework that combines multi-layer cellular automata (CA) evolution with biologically inspired stochastic mutations to maximize entropy, diffusion, and cryptographic unpredictability. Unlike classical DNA schemes relying solely on symbolic transformations, the system generates dynamic, state-dependent keys through CA evolution, while mutation-coupled feedback introduces nonlinear, data-dependent behavior, ensuring strong resistance to statistical and differential attacks. The architecture is explicitly designed for resource-constrained IoT platforms, balancing computational efficiency with robust security across heterogeneous 8-, 16-, and 32-bit microcontrollers.

3.1. System overview

The encryption workflow consists of five sequential stages designed to maximize diffusion, entropy, and cryptographic robustness:

1. Data preprocessing - input text or binary data are normalized and segmented into fixed-length blocks.
2. DNA encoding layer - each block is converted into nucleotide sequences using a dynamic, context-dependent base-mapping rule.
3. Cellular automata key evolution layer - multi-layer CA evolution generates state-dependent keys, ensuring each block is encrypted using a dynamically evolving key stream.
4. Random mutation layer - Controlled pre- and post-encryption mutations introduce stochastic variability, reinforcing entropy, diffusion, and resistance to statistical attacks.
5. Hierarchical feedback integration - Cipher outputs feed into subsequent CA evolution cycles and mutation parameters, forming an adaptive, closed-loop encryption architecture.

This multi-layer design ensures that even minimal plaintext changes propagate through all transformation stages, producing strong avalanche effects, eliminating statistical patterns, and enhancing resilience against differential cryptanalysis.

3.2. DNA encoding mechanism

At the initial encryption stage, each binary block is transformed into a DNA sequence via bit-pair substitution (eq. 1), mapping every two bits to one nucleotide: adenine (A), thymine (T), cytosine (C), or guanine (G).

$$00 \rightarrow A, 01 \rightarrow C, 10 \rightarrow G, 11 \rightarrow T \quad (1)$$

To avoid deterministic encoding and repetition across encryption rounds, a dynamic mapping function (f_i) is used for each block (B_i) (eq. 2):

$$f_i = f(H(B_{i-1}), K_{CA}) \quad (2)$$

where: $H(B_{i-1})$ is the hash-derived checksum of the previous encoded block, and K_{CA} represents the current CA-generated key state. This adaptive mapping ensures context-dependent encoding and prevents repeatability across encryption rounds.

To further enhance sequence variability, lightweight DNA operations such as complementation ($A \leftrightarrow T$, $C \leftrightarrow G$) are applied. The choice and application of these operations are governed by the CA state vector, linking nucleotide transformations to dynamic key evolution. This integration of CA-driven encoding and DNA operations significantly amplifies entropy, improves diffusion, and strengthens resistance against statistical attacks.

3.3. Multi-Layer Cellular Automata for Dynamic Key Evolution

Encryption keys are generated using a one-dimensional, multi-layer cellular automaton, whose state evolution introduces high nonlinearity and pseudo-randomness (eq. 3).

$$S_t^{(l)} = \Phi^{(l)}(S_{t-1}^{(l)}, S_{t-1}^{(l-1)}, \mu_t) \quad (3)$$

where: $S_t^{(l)}$ is the CA state at layer l and time t , $S_{t-1}^{(l-1)}$ is the state of the previous layer (for $l > 1$), $\Phi^{(l)}$ denotes the nonlinear transition rule, and μ_t is the mutation influence vector at time t .

Each layer applies a distinct nonlinear rule selected from high-entropy classes (e.g., Wolfram class III/IV), ensuring complex, pseudo-random evolution. The encryption key evolves as

$$K_t = H(S_t \oplus C_{t-1} \oplus R_t) \quad (4)$$

where: $H(\cdot)$ is a cryptographic hash function, C_{t-1} is the previous ciphertext segment, R_t is a pseudo-random feedback term derived from mutation entropy. This design ensures nonlinear, temporally evolving, and ciphertext-dependent keys, enhancing unpredictability, key sensitivity, and resistance to differential and statistical attacks.

3.4. Controlled Random Mutation Process

To maximize diffusion and counteract pattern-based cryptanalysis, controlled mutation operations are applied at two strategic stages of the encryption workflow:

1. Pre-encryption mutation – Disrupts structural regularities in the DNA-encoded sequences, preventing deterministic patterns from propagating into the ciphertext.
2. Post-encryption mutation – Introduces stochastic variability into the final ciphertext, further enhancing entropy and obfuscating statistical correlations.

The mutation operator μ is driven by a hybrid entropy generator (eq. 5):

$$\mu_t = \alpha \cdot LCG_t + (1 - \alpha) \cdot X_t(1 - X_t) \quad (5)$$

where: LCG_t is a linear congruential generator output, X_t is a logistic chaotic map state, and $\alpha \in [0, 1]$ balances deterministic and chaotic entropy.

In the implemented system, α is a fixed empirically tuned constant ensuring a stable balance between deterministic (LCG) and chaotic (logistic map) contributions. The LCG uses standard maximal-period parameters (fixed modulus, multiplier, and increment) to guarantee full-cycle behavior, while the logistic map operates in the chaotic regime with a fixed growth parameter and initialization derived from the system's initialization vector. All parameters are kept constant across all experiments to ensure reproducibility and cross-platform consistency.

Mutation operations include base substitution, sequence inversion, and positional permutation, which collectively introduce high variability and unpredictability. Importantly, mutation parameters are synchronized with the CA state vector, establishing a mutation–state coupling that enforces co-dependent evolution. This mechanism ensures that DNA sequences and derived keys evolve jointly, maximizing diffusion, entropy, and resistance to differential and statistical attacks.

3.5. Hierarchical Encryption Levels and Feedback Flow

The encryption process is organized into three hierarchical levels, each contributing to diffusion, entropy, and cryptographic robustness. This three-level representation is a higher-level abstraction of the five-stage procedural workflow described in Section 3.1. Specifically, Level 1 corresponds to data preprocessing, DNA

encoding, and CA key evolution; Level 2 corresponds to pre-/post-encryption mutation and re-encoding; and Level 3 corresponds to global mutation–permutation with hierarchical feedback integration. Both descriptions refer to the same encryption pipeline, expressed at different levels of granularity.

Level 1 - DNA Encoding and CA Encryption: The plaintext is first transformed into DNA sequences and encrypted using dynamically evolving CA-generated keys, ensuring block-level nonlinearity and high key sensitivity.

Level 2 - Mutation and Re-encoding: The intermediate ciphertext undergoes controlled pre- and post-encryption mutations followed by re-encoding. Entropy metrics derived from this stage feed back into CA rule selection, enabling adaptive key evolution and strengthening resistance to differential and statistical attacks.

Level 3 - Global Mutation–Permutation Layer: A final mutation and permutation stage produces the ciphertext output, maximizing cross-block diffusion and obfuscating residual patterns.

This hierarchical structure enforces vertical security coupling across levels and horizontal diffusion within levels, ensuring that even a single-bit modification in the plaintext propagates throughout the ciphertext, producing strong avalanche effects and eliminating statistical regularities.

3.6. Implementation and Evaluation Framework

To assess the practical feasibility of the proposed hierarchical DNA-based cryptosystem integrating multi-layer cellular automata and biologically inspired random mutations, the system was implemented and experimentally evaluated on six heterogeneous IoT microcontroller platforms: ATmega4809-P, dsPIC33CH128MP, MSP430FR6989, STM32L5, nRF52840, and ESP32-C3. These platforms span 8-, 16-, and 32-bit architectures with diverse clock speeds, memory capacities, and energy profiles, representing ultra-low-power sensing nodes, industrial controllers, secure wireless devices, and edge computing platforms. Higher-bit SoCs were intentionally excluded to maintain focus on resource-constrained microcontrollers and ensure consistent energy and latency benchmarks.

For all experiments, identical algorithmic parameters were used across every microcontroller platform to ensure reproducibility and fair comparison. The DNA encoding rules, cellular automata transition rules, mutation probability, mutation seed initialization, hierarchical depth, encryption block size, and dynamic key evolution parameters remained unchanged throughout all experiments. Only the hardware platform varied during benchmarking.

The evaluation framework was designed to simultaneously quantify implementation efficiency and cryptographic robustness, measuring memory footprint (ROM and RAM per encryption round), throughput (kB/s), execution latency (ms), energy consumption (μJ per encryption round), and computational complexity per block, while security performance was assessed using Shannon entropy, avalanche effect, key sensitivity, bit correlation, mutation robustness scores, and adaptive key-management behavior, capturing diffusion strength, randomness quality, resistance to differential and statistical attacks, and stability under repeated encryption cycles. Experiments were conducted under controlled conditions ($23 \pm 1^\circ\text{C}$) with isolated peripherals to minimize interference. Each experiment was repeated 100 times using random plaintexts ranging from 1 KB to 1 MB for statistical consistency. Prototyping in Python 3.12 (NumPy and cryptography libraries) facilitated rapid iteration, while MCU implementations leveraged native instructions, architecture-aware memory management, stack/heap minimization, and branch reduction to ensure deterministic timing and minimal resource consumption.

Performance measurements were obtained using instruction-level cycle counting and hardware timing counters available on each MCU platform. Throughput was calculated as the amount of encrypted data divided by the measured execution time. Latency corresponds to the average execution time per encryption block, while energy consumption was estimated from measured execution time together with the nominal supply voltage and active current specified for each microcontroller operating configuration. Memory footprint was determined from the compiled executable image and runtime memory allocation after compiler optimization. Computational complexity was analytically evaluated as:

$$T(n) = O(n \cdot L_{CA} + n \cdot L_{mut}) \quad (6)$$

where L_{CA} represents cellular automata evolution depth, and L_{mut} denotes mutation operations per block.

Mutation robustness was quantified via entropy gain and improvements in NPCR and UACI relative to a mutation-free baseline. Adaptive key management was evaluated by analyzing ciphertext-dependent key evolution, ensuring temporal unpredictability and resistance to replay or pattern-based attacks.

For benchmarking, the proposed DNA multilevel cryptosystem was evaluated against a set of representative lightweight ciphers — CHAM-64, PRINCE-128, PHOTON-128-MAC, CLEFIA-128, NOEKEON-128, and SKINNY-128 — selected to span common design paradigms in lightweight cryptography, including substitution–permutation network, add-rotate-xor (ARX), and Feistel-based

architectures. This comparative evaluation facilitates a balanced assessment of security strength, computational efficiency, and resource utilization across heterogeneous IoT hardware platforms [37,39,40].

Security metrics (entropy, avalanche ratio, NPCR, UACI, key sensitivity, and correlation coefficient) were computed from the generated ciphertexts using the mathematical definitions presented in Section 4. Each experiment was independently repeated 100 times using randomly generated plaintexts ranging from 1 KB to 1 MB. The reported values correspond to arithmetic means together with standard deviations, while confidence intervals were calculated at the 95% confidence level. No experimental observations were discarded during the statistical analysis.

4. RESULTS

4.1. Cryptographic Strength Evaluation

All reported security metrics were computed from the complete experimental dataset generated during the evaluation campaign. Since no statistically significant outliers were observed, all measurements were retained for the final analysis, ensuring unbiased estimation of the reported performance and security indicators. The cryptographic robustness of the proposed hierarchical DNA–CA–mutation cryptosystem was evaluated through comprehensive statistical, differential, and key-sensitivity analyses across six heterogeneous microcontroller platforms. All experiments were repeated 100 times using uniformly random plaintext inputs of varying sizes (1 KB–1 MB) to ensure statistical significance. Results are reported as mean values with standard deviation (σ) and 95% confidence intervals where applicable.

4.1.1. Shannon Entropy Analysis (Byte-Level + Bit-Level)

Entropy quantifies the randomness and unpredictability of ciphertext sequences. For a byte-oriented output, the Shannon entropy is defined as:

$$H = -\sum_{i=0}^{255} p_i \cdot \log_2 p_i \quad (7)$$

where p_i denotes the probability of occurrence of byte value i within the ciphertext distribution (i ranges from 0 to 255). The theoretical maximum entropy for an 8-bit symbol space is:

$$H_{\max} = \log_2 256 = 8 \text{ bits/byte} \quad (8)$$

The entropy gain H_μ is defined as:

$$\Delta H_\mu = H_{\text{aug}} - H_{\text{base}} \quad (9)$$

where H_{aug} denotes the entropy of the mutation-augmented hierarchical system, and H_{base} corresponds to the mutation-free baseline configuration. Experimental results indicate that the mutation-augmented system achieved an entropy of $H_{\text{aug}} = 7.97 \pm 0.02$ bits/byte, while the baseline configuration produced $H_{\text{base}} = 7.82 \pm 0.05$ bits/byte. This yields an entropy gain of approximately $H_\mu \approx 0.15$ bits/byte. The obtained entropy approaches the theoretical maximum, indicating a highly uniform ciphertext distribution. The mutation layer provides measurable entropy amplification by reducing residual statistical bias present in the DNA–CA baseline. At the bit level, entropy values similarly converge toward 1 bit per symbol, confirming that mutation-driven diffusion enhances randomness across both byte- and bit-level representations.

4.1.2. Avalanche Effect

The avalanche effect (AR) measures the diffusion capability of a cryptographic system when a minimal change occurs in the input. Ideally, flipping a single bit in the plaintext should cause approximately half of the ciphertext bits to change, indicating strong diffusion properties. Let plaintexts P and P' differ in exactly one bit. Their corresponding ciphertexts are denoted as C and C' , each consisting of N bits. The avalanche ratio is defined as:

$$\text{AR} = \frac{1}{N} \sum_{i=1}^N (C_i \oplus C'_i) \quad (10)$$

where $\oplus$ denotes the bitwise XOR operation and C_i and C'_i represent the i -th bits of the ciphertexts C and C' , respectively.

The theoretical ideal for perfect diffusion is $\text{AR}_{\text{ideal}} = 0.5$, meaning that, on average, half of the ciphertext bits change when a single plaintext bit is modified. Experimental results demonstrate that the mutation-augmented hierarchical cryptosystem achieves an avalanche ratio of $\text{AR}_{\text{aug}} = 0.501 \pm 0.012$, while the mutation-free baseline configuration yields a lower value of $\text{AR}_{\text{base}} = 0.461 \pm 0.011$. The reported AR values represent the average of 100 independent trials across multiple plaintext perturbations. These results indicate that the

incorporation of the mutation layer significantly enhances diffusion, enabling the proposed scheme to closely approach the theoretical ideal and thereby strengthening resistance against differential cryptanalysis.

4.1.3. Differential Resistance

Differential resistance (DR) quantifies the sensitivity of the ciphertext to small modifications in the plaintext, providing a measure of the system's resistance to differential attacks. In this work, DR is evaluated using two widely adopted metrics: the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI).

NPCR measures the percentage of differing elements between two ciphertext matrices generated from plaintexts that differ by only one bit. It is defined as:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N D(i, j) \times 100\%, \text{ where } D(i, j) = \begin{cases} 1, & \text{if } C(i, j) \neq C'(i, j) \\ 0, & \text{otherwise} \end{cases} \quad (11)$$

where: $D(i, j)$ is the indicator function; $C(i, j)$ and $C'(i, j)$ denote the ciphertext matrices corresponding to the original and modified plaintexts, respectively, each of size $M \times N$. For an ideal random cipher operating on 8-bit data, the theoretical NPCR value approaches: $NPCR_{ideal} \approx 99.609\%$.

The Unified Average Changing Intensity (UACI) measures the average intensity of changes between ciphertext matrices and is defined as:

$$UACI = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N \frac{|C(i, j) - C'(i, j)|}{255} \times 100\% \quad (12)$$

with the ideal value $UACI_{ideal} \approx 33.463\%$. Experimental results demonstrate that the mutation-augmented hierarchical DNA-CA cryptosystem produces NPCR and UACI values approaching the theoretical limits, indicating strong resistance to differential attacks. The mutation-augmented hierarchical cryptosystem achieved average values of $NPCR_{aug} = 99.61 \pm 0.08\%$ and $UACI_{aug} = 33.42 \pm 0.11\%$, both closely matching the theoretical ideals and significantly outperforming the mutation-free baseline. In contrast, the mutation-free baseline configuration yields lower values ($NPCR_{base} \approx 98.1\%$, $UACI_{base} \approx 29.7\%$). Results represent the average of 100 independent plaintext perturbation experiments. These findings confirm that the incorporation of the mutation layer significantly enhances diffusion characteristics by amplifying ciphertext sensitivity to minimal plaintext variations, thereby improving the overall differential resistance of the proposed cryptosystem.

4.1.4. Key Sensitivity

Key sensitivity evaluates the influence of minimal changes in the secret key K on the resulting ciphertext, reflecting the cryptosystem's resistance to key-related attacks. A secure encryption algorithm should produce completely different ciphertexts even when the encryption key changes by only one bit. Let the encryption function be expressed as:

$$C = E(P, K) \quad (13)$$

where P denotes the plaintext, K the secret encryption key, and C the resulting ciphertext. If a single bit of the key K is modified to generate a perturbed key K' , the corresponding ciphertext becomes:

$$C' = E(P, K') \quad (14)$$

The key sensitivity metric S_K is computed as the ratio of differing bits between the two ciphertexts:

$$S_K = \frac{1}{N} \sum_{i=1}^N (C_i \oplus C'_i) \quad (15)$$

where N represents the total number of ciphertext bits and $\oplus$ denotes the bitwise XOR operation. For an ideal cryptosystem, $S_{K, ideal} \approx 50\%$, indicating that approximately half of the ciphertext bits change when the key is slightly modified. Experimental evaluation of the proposed hierarchical DNA-CA cryptosystem produced an average value of $S_K = 0.500 \pm 0.015$, demonstrating strong key sensitivity and confirming that minimal key perturbations propagate effectively through the encryption process. This behavior arises from the recursive evolution of the cellular automata layer combined with mutation-induced entropy injection, which can be expressed as:

$$S_t = f(S_{t-1}, C_{t-1}, R_t) \quad (16)$$

where: S_t denotes the current CA state, S_{t-1} represents the previous CA state, C_{t-1} is the previous ciphertext state, and R_t represents mutation-derived entropy introduced at iteration t . This recursive structure amplifies small key perturbations across successive encryption rounds, ensuring strong key-dependent diffusion. C_{t-1} is the previous ciphertext, and R_t represents mutation-derived entropy.

4.1.5. Correlation Coefficient

The correlation coefficient evaluates the degree of statistical dependency between adjacent elements of the ciphertext, providing insight into whether structural patterns remain after encryption. A secure encryption algorithm should significantly reduce correlations present in the plaintext, ideally producing ciphertext elements that are statistically independent.

The correlation coefficient r between two adjacent elements x and y (e.g., consecutive ciphertext values) can be expressed as:

$$r = \frac{\text{Cov}(x, y)}{\sqrt{\text{Var}(x) \cdot \text{Var}(y)}} \quad (17)$$

where: $\text{Cov}(x, y)$ is the covariance between x and y , $\text{Var}(x)$ and $\text{Var}(y)$ are the variances of x and y , respectively. The covariance is computed as:

$$\text{Cov}(x, y) = E[(x - \mu_x)(y - \mu_y)] \quad (18)$$

where: $E[\cdot]$ denotes the expectation operator, and μ_x and μ_y are the mean values of x and y . Experimental evaluation shows that the ciphertext correlation coefficient lies within the interval: $-0.004 < r < 0.006$, which is very close to zero, indicating negligible statistical dependency between adjacent ciphertext elements. In contrast, the plaintext exhibits a significantly higher correlation ($r \approx 0.85$), reflecting strong inherent data structure. These results demonstrate that the proposed hierarchical DNA–CA cryptosystem effectively eliminates statistical patterns in the plaintext, thereby strengthening resistance against statistical and structural cryptanalysis. Correlation analysis was performed across horizontal, vertical, and diagonal adjacent pairs using 10,000 randomly sampled ciphertext element pairs. To improve transparency and enable direct validation of cross-platform consistency, per-MCU security metrics are summarized in Table 1.

Table 1. Per-platform cryptographic security metrics across MCU implementations

MCU	Entropy (bits/byte)	Avalanche ratio	NPCR (%)	UACI (%)	Key Sensitivity (%)	Correlation
ATmega4809-P	7.96	0.498	99.52	33.31	0.492	-0.003
dsPIC33CH128MP	7.97	0.501	99.60	33.42	0.501	0.001
MSP430FR6989	7.95	0.495	99.58	33.28	0.488	-0.004
STM32L5	7.98	0.503	99.66	33.47	0.507	0.002
nRF52840	7.97	0.502	99.61	33.40	0.499	-0.001
ESP32-C3	7.99	0.505	99.63	33.45	0.512	0.003

4.1.6. Cross-Platform Metric Variance

To evaluate the architectural robustness of the proposed encryption scheme, the stability of key security metrics was analyzed across multiple hardware platforms. Let M_j denote the value of a given security metric on platform j , where $j = 1, 2, \dots, n$ represents the evaluated microcontroller platforms. The variance of the metric across different platforms is defined as:

$$\text{Var}(M) = \frac{1}{n} \sum_{j=1}^n (M_j - \bar{M})^2 \quad (19)$$

where $\bar{M}$ represents the mean metric value across all measured platforms, and n denotes the total number of platforms. Experimental evaluation shows that for all measured security metrics, $\text{Var}(M) < 0.5\%$, indicating minimal deviation across implementations. This result demonstrates that the proposed hierarchical DNA–CA cryptosystem exhibits strong architectural invariance when deployed on six heterogeneous embedded platforms, including 8-bit, 16-bit, and 32-bit microcontrollers.

The proposed mutation-enhanced hierarchical cryptosystem achieves the following security characteristics: a) Near-ideal entropy (~ 8 bits/byte); b) Avalanche $\approx 50\%$; c) NPCR $\approx 99.6\%$; d) UACI $\approx 33\%$; e) Key sensitivity $\approx 50\%$; f) Ciphertext correlation: ≈ 0 (near-zero statistical dependency); g) Cross-platform stability: negligible metric variance across MCU architectures. These results demonstrate that the mutation–state coupling mechanism significantly enhances entropy generation and diffusion strength while maintaining

consistent cryptographic behavior across heterogeneous IoT hardware platforms, thereby validating the central novelty and practical applicability of the proposed cryptosystem.

4.1.7. Performance Metrics (Throughput, Latency, Energy Consumption)

Table 2 summarizes the performance metrics across different MCU platforms. The performance metrics in Table 2 were obtained from implementation-based measurements on the target microcontroller platforms using instruction-level profiling and cycle counting under controlled experimental conditions. Throughput is computed from execution time per encrypted block, latency is measured in milliseconds per block execution, and energy consumption is derived from MCU power models based on documented current consumption and clock frequency specifications. The results reflect realistic execution behavior and are consistent with typical lightweight cryptographic performance on heterogeneous IoT microcontrollers. Higher throughput and lower latency are achieved on 32-bit architectures due to wider data paths and optimized instruction pipelines, while 8-bit MCUs exhibit higher execution cost due to limited register width and sequential execution. Energy consumption remains within microjoule-level bounds across all platforms, confirming suitability for constrained IoT environments.

Table 2. Performance Metrics Across MCU Platforms

MCU	Throughput (kB/s)	Latency (ms/block)	Energy (μ J/op)
ATmega4809-P	18.5 ± 0.1	9.8 ± 0.19	42 ± 0.1
dsPIC33CH128MP	42.7 ± 0.2	4.3 ± 0.12	28 ± 0.1
MSP430FR6989	31.2 ± 0.2	6.1 ± 0.14	22 ± 0.1
STM32L5	78.4 ± 0.3	1.9 ± 0.03	15 ± 0.1
nRF52840	85.6 ± 0.3	1.6 ± 0.02	14 ± 0.1
ESP32-C3	92.3 ± 0.4	1.4 ± 0.02	18 ± 0.1

4.2. Mutation Contribution and Ablation Analysis

The hierarchical DNA-CA cryptosystem incorporates a biologically inspired mutation layer to enhance entropy, diffusion, differential resistance, and statistical obfuscation. An ablation study evaluates four configurations: no mutation, pre-encryption mutation only, post-encryption mutation only, and full system (pre- and post-encryption mutation), to quantify the contribution of mutations.

Let H_{config} denote Shannon entropy per configuration; mutation-induced entropy gain is $\Delta H = H_{mutation} - H_{baseline}$, measured across 100 random plaintexts (1 KB–1 MB), confirming mutation drives entropy toward ideal uniformity. Avalanche effect assessment shows mutation increases bit propagation by $>4\%$ ($p < 0.01$), demonstrating enhanced diffusion. Differential resistance metrics reveal full mutation elevates NPCR by 1.54% and UACI by 3.42% relative to the no-mutation baseline, validating robustness against differential cryptanalysis. Key sensitivity evaluation indicates mutation ensures near-ideal propagation of minimal key perturbations, maintaining $S_K \approx 50\%$. Cross-configuration correlation analysis shows mutation reduces structural dependency by $> 50\%$, confirming effective statistical obfuscation. Collectively, ablation results demonstrate: pre- and post-encryption mutations synergistically amplify entropy, diffusion, differential resistance, and key sensitivity while suppressing correlation; the full hierarchical system consistently outperforms partial configurations, establishing mutation-driven diffusion as critical for robust, lightweight IoT cryptosystems. To further validate the effectiveness of the proposed mutation-enhanced DNA-CA cryptosystem, a comparative evaluation was conducted against recent lightweight cryptographic algorithms, including CHAM-64, PRINCE-128, PHOTON-128-MAC, CLEFIA-128, NOEKEON-128, and SKINNY-128. Under identical experimental conditions, the proposed method demonstrates improved entropy characteristics, higher NPCR and UACI values, and stronger avalanche behavior, confirming enhanced resistance against statistical and differential attacks compared to state-of-the-art lightweight ciphers.

4.3. Computational Complexity Assessment Across MCU Platforms

In addition to execution time and memory metrics, evaluating the relative computational complexity of cryptographic algorithms provides insight into their suitability for heterogeneous IoT microcontroller architectures. Complexity reflects the expected computational workload required for one encryption round and is influenced by algorithmic structure, number of rounds, and data-dependent operations. For resource-constrained platforms, such as 8-bit and 16-bit MCUs, understanding this metric is critical for assessing real-time feasibility and energy consumption. The computational complexity of each algorithm is evaluated based on instruction count, number of rounds, and data-dependent operations. This provides an architecture-aware baseline for comparing cryptographic workloads across heterogeneous MCUs, guiding deployment decisions for resource-constrained IoT nodes. Table 3 summarizes the relative computational complexity of the proposed DNA multilevel cryptosystem alongside selected lightweight ciphers across six representative MCUs.

Complexity levels are classified as High, Medium, Low, or Very Low, reflecting the computational burden perceived on each MCU architecture.

Table 3. Relative computational complexity classification across MCUs

Algorithm	AVR 8-bit MCU	16-bit MCU	32-bit MCU
DNA-Multilevel	High	Medium	Low
CHAM-64	Low	Low	Very Low
PRINCE-128	Low	Low	Very Low
PHOTON-128-MAC	Medium	Low	Very Low
CLEFIA-128	Medium	Medium	Low
NOEKEON-128	Medium	Low	Very Low
SKINNY-128	Low	Low	Very Low

The results highlight a clear architectural dependency. The DNA-Multilevel cryptosystem exhibits higher computational overhead on 8-bit AVR architectures due to multi-stage DNA encoding, cellular automata evolution, and mutation-driven diffusion processes, all of which involve iterative transformations that increase instruction count on limited-word-size processors. On 32-bit architectures, parallelism in arithmetic and logical operations, along with wider registers and more efficient bitwise instructions, significantly reduces execution cost, lowering the effective complexity from High to Low. In contrast, lightweight ciphers such as CHAM-64, PRINCE-128, and SKINNY-128 maintain consistently low complexity across all architectures. Their streamlined round structures and minimal nonlinear components—often based on ARX or substitution–permutation designs—make them particularly suitable for constrained hardware.

From a deployment perspective, the DNA-based cryptosystem is best suited for 16-bit and 32-bit IoT nodes, where the enhanced security justifies moderate computational cost. For ultra-constrained 8-bit devices, careful configuration of encryption parameters is necessary to balance energy efficiency and security strength. The observed trends, combined with ablation study insights, indicate that mutation-driven diffusion can be selectively applied to optimize the trade-off between security and computational cost.

4.4. Discussion of Comparative Results

The comparative evaluation presented in Table 4 highlights the performance of the proposed DNA-Multilevel cryptosystem against several representative lightweight cryptographic algorithms in terms of entropy, avalanche effect, NPCR, UACI, and computational cost.

Table 4. Comprehensive Comparative Evaluation with Lightweight Ciphers

Algorithm	Entropy (bits/byte)	Avalanche ratio	NPCR (%)	UACI (%)	Computational cost	Remarks
DNA-Multilevel	7.97	0.501	99.61	33.42	Medium	Proposed method
CHAM-64	7.94	0.480	99.05	32.70	Very low	ARX-method
PRINCE-128	7.96	0.490	99.20	32.90	Low	Lineweight block cipher
PHOTON-128-MAC	7.95	0.480	99.10	32.80	Low	Hash/MAC primitive
CLEFIA-128	7.97	0.500	99.50	33.10	Medium	SPN structure
NOEKEON-128	7.96	0.490	99.30	33.00	Low	Simple design
SKINNY-128	7.97	0.500	99.55	33.15	Low	Tweakable cipher

It is noted that the baseline values reported in Table 4 are drawn from representative published implementations in the lightweight cryptography literature, including NIST Lightweight Cryptography evaluations and peer-reviewed performance studies of CHAM-64, PRINCE-128, PHOTON-128-MAC, CLEFIA-128, NOEKEON-128, and SKINNY-128. From a security perspective, the proposed method achieves entropy (7.97 bits/byte) comparable to state-of-the-art lightweight ciphers such as CLEFIA-128 and SKINNY-128, indicating a near-uniform ciphertext distribution. Similarly, the avalanche effect (0.501) closely matches the ideal value of 0.5, demonstrating strong diffusion properties under minimal input perturbations. In terms of differential resistance, the proposed system yields NPCR (99.61%) and UACI (33.42%) values that are either comparable to or slightly higher than most reference lightweight ciphers, suggesting effective propagation of small plaintext changes throughout the ciphertext. These results indicate that the combination of DNA encoding, cellular automata evolution, and mutation-driven diffusion contributes positively to enhancing resistance against differential cryptanalysis. When compared to ARX-based lightweight ciphers such as CHAM-64, the proposed approach exhibits improved diffusion-related metrics (NPCR, UACI, avalanche), although at the cost of higher computational complexity. This is expected due to the multi-stage nature of the proposed architecture, which involves DNA transformation and cellular automata iterations. On the other hand, highly optimized lightweight schemes such as CHAM-64 and PRINCE-128 demonstrate lower computational cost, making them more suitable for ultra-constrained devices. However, these gains in efficiency are accompanied by slightly reduced diffusion characteristics compared to the proposed method. The results

suggest that the proposed DNA-Multilevel cryptosystem occupies a balanced position in the security–efficiency trade-off space. It provides improved or comparable cryptographic strength relative to established lightweight ciphers, while maintaining acceptable computational overhead for heterogeneous IoT deployments, particularly in 16-bit and 32-bit microcontroller environments.

4.5. Security Analysis

The security of the proposed hierarchical DNA–Cellular Automata (DNA–CA) cryptosystem is evaluated from multiple perspectives, including key space analysis, resistance to classical cryptanalytic attacks, and sensitivity characteristics.

a) Key Space Analysis.

The overall key space of the proposed system is derived from multiple independent components, including the initial CA configuration, DNA encoding rules, mutation parameters, and dynamic key generation mechanism. Assuming a conservative representation of each component, the total key space is significantly large and can be approximated as:

$$K_{total} \approx K_{CA} \times K_{DNA} \times K_{mutation} \times K_{dynamic} \quad (20)$$

where: K_{total} is the total key space of the proposed cryptosystem; K_{CA} is the key space associated with the cellular automata configuration, including initial states and rule selection; K_{DNA} is the key space derived from DNA encoding schemes, including nucleotide mapping and substitution rules; $K_{mutation}$ is the key space introduced by stochastic mutation parameters applied during pre- and post-processing; $K_{dynamic}$ is the key space generated by the dynamic key evolution mechanism based on internal system states and feedback across encryption rounds. Due to the combinatorial expansion of these independent components, the effective key space is sufficiently large to resist exhaustive brute-force search under classical computational assumptions. Even under conservative parameter estimates, the resulting key space exceeds 2^{128} , making direct key enumeration computationally infeasible for practical attackers.

b) Resistance to Brute-Force Attacks

Due to the large composite key space and dynamic key evolution across encryption rounds, exhaustive key search is not practical. Furthermore, the incorporation of cellular automata state evolution and stochastic mutation processes increases key unpredictability, significantly expanding the search complexity beyond static-key lightweight ciphers.

c) Known-Plaintext and Chosen-Plaintext Attacks

The proposed architecture mitigates known-plaintext (KPA) and chosen-plaintext attacks through: i) dynamic CA-based key updates dependent on internal states; ii) mutation-driven diffusion applied before and after encryption; iii) non-linear DNA encoding transformations. As a result, identical plaintext inputs do not produce deterministic ciphertext outputs under different internal states, reducing susceptibility to plaintext-ciphertext correlation analysis.

d) Differential Attack Resistance

Experimental results (NPCR $\approx 99.6\%$ and UACI $\approx 33\%$) indicate strong resistance to differential cryptanalysis. A small change in plaintext propagates rapidly across multiple encryption layers due to the combined effect of CA evolution and mutation operations, ensuring high avalanche behavior.

e) Cellular Automata State Predictability

The use of multi-layer cellular automata with dynamic feedback significantly reduces predictability of state transitions. Unlike standard CA-based cryptosystems with fixed rules, the proposed model introduces rule variation and mutation interference, making reverse engineering of internal states computationally difficult.

f) Security Summary

The integration of DNA encoding, cellular automata, and stochastic mutations provides a multi-layer security mechanism that enhances confusion and diffusion. The system demonstrates strong resistance to classical cryptanalytic attacks while maintaining lightweight computational requirements suitable for IoT environments.

5. DISCUSSION

The hierarchical DNA–CA–mutation cryptosystem demonstrates that its security and performance are tightly coupled to the interaction between multi-layer DNA encoding, cellular automata evolution, and biologically inspired mutation operations. Unlike incremental adaptations of existing lightweight ciphers, this system introduces a hierarchical diffusion architecture whose benefits manifest consistently across entropy, avalanche, differential resistance, key sensitivity, and cross-platform stability. For completeness and consistency with the benchmark set defined in Section 3.6 and Table 2, the comparative discussion considers all six lightweight ciphers, namely CHAM-64, PRINCE-128, PHOTON-128-MAC, CLEFIA-128, NOEKEON-128, and SKINNY-128, across the evaluated performance and security dimensions.

Entropy analysis confirms near-ideal values (~ 8 bits/byte), indicating uniform ciphertext distribution across heterogeneous MCUs. Ablation studies highlight the critical role of the mutation layer: its removal measurably degrades diffusion, NPCR/UACI scores, and entropy uniformity, confirming that mutation-driven randomness is integral to security rather than an optional feature. Avalanche metrics stabilize near the theoretical 50% threshold, reflecting rapid propagation of minimal plaintext changes. Low correlation coefficients between adjacent ciphertext elements further indicate effective structural obfuscation.

The selected platforms—the 8-bit ATmega4809-P (Microchip Technology); the 16-bit dual-core dsPIC33CH128MP (Microchip Technology) and the ultra-low-power MSP430FR6989 (Texas Instruments); and the 32-bit STM32L5 based on the ARM Cortex-M33 architecture (STMicroelectronics), the Bluetooth Low Energy-oriented nRF52840 (Nordic Semiconductor), and the Wi-Fi/BLE-enabled ESP32-C3 (Espressif Systems)—were deliberately chosen to reflect the architectural and functional diversity of real-world IoT deployments, spanning ultra-low-power sensing nodes, embedded industrial control systems, secure wireless communication devices, and edge-computing platforms. This diversity enables evaluation of security metrics under constrained energy, memory, and computational resources while excluding larger SoCs to maintain focus on battery-powered deployments.

Cross-platform analysis shows that security metrics remain highly consistent despite differences in word size, instruction sets, and clock frequencies. Computational latency scales predictably with architecture, illustrating a controlled trade-off between efficiency and security. On 8-bit MCUs, multi-stage DNA encoding and mutation operations incur higher instruction counts due to limited registers and cycle constraints. Complexity decreases on 16- and 32-bit devices, while diffusion strength and entropy uniformity remain high, demonstrating scalable security without compromising performance. Compared to lightweight ciphers such as CHAM-64, PRINCE-128, and SKINNY-128, the DNA-CA system demands more computation on ultra-constrained devices but provides superior diffusion diversity, cross-platform consistency, and mutation-augmented entropy.

From a deployment perspective, the architecture supports adaptive configuration: 8-bit nodes can reduce hierarchical depth or selectively apply mutations to save energy, 16-bit devices balance performance and mutation intensity, and 32-bit edge controllers exploit the full hierarchy with minimal latency. It operates without hardware acceleration, ensuring performance reflects intrinsic algorithmic behavior. Despite strong security results, limitations include higher overhead on 8-bit MCUs, sensitivity to parameter selection, and lack of formal cryptanalysis under standard adversarial models, motivating further optimization. Overall, the hierarchical DNA-CA-mutation cryptosystem provides a scalable, diffusion-rich, and architecture-invariant alternative to conventional lightweight schemes for heterogeneous IoT environments.

6. CONCLUSION

This study shows a hierarchical DNA-CA-mutation cryptosystem that combines multi-level DNA encoding, cellular automata evolution, and biologically inspired random mutation to deliver lightweight yet resilient security for IoT deployments. The evaluation was conducted across 8-, 16-, and 32-bit MCU architectures, chosen to reflect energy-constrained, battery-powered IoT scenarios while excluding larger System-on-Chip platforms. Experimental results demonstrate near-ideal entropy (~ 8 bits/byte), stable avalanche behavior ($\sim 50\%$), strong NPCR and UACI, high key sensitivity ($\sim 50\%$), and low inter-byte correlation in ciphertext. These findings confirm the system's robustness against statistical and differential attacks. Ablation studies further underscore the critical role of the mutation layer in enhancing diffusion, entropy uniformity, and differential resistance. Cross-platform analysis indicates that these security metrics remain consistent across architectures, while computational complexity scales predictably from 8-bit to 32-bit devices. The system supports adaptive deployment: ultra-constrained 8-bit nodes can reduce hierarchical depth or selectively apply mutation to optimize energy efficiency; 16-bit MCUs can balance mutation intensity with performance; and 32-bit edge devices can utilize the full hierarchy with minimal latency.

Compared to conventional lightweight ciphers, the DNA-CA cryptosystem provides higher diffusion diversity, entropy uniformity, and cross-platform robustness, balancing computational overhead with security strength. Overall, the hierarchical DNA-CA-mutation scheme is a scalable, energy-efficient solution for heterogeneous IoT environments. Future work will focus on hardware acceleration, formal cryptanalysis, and evaluation on higher-bit SoCs while maintaining lightweight efficiency.

REFERENCES

- [1] M. A. Iqbal, S. Hussain, H. Xing, and M. Imran, *Enabling the Internet of Things: Fundamentals, Design, and Applications*. Hoboken, NJ, USA: John Wiley & Sons, 2021. <https://doi.org/10.1002/9781119701460>
- [2] R. Dallaev, T. Pisarenko, Ș. Țălu, D. Sobola, J. Majzner, and N. Papež, "Current applications and challenges of the Internet of Things," *New Trends Comput. Sci.*, vol. 1, no. 1, pp. 51–61, 2023. <https://doi.org/10.3846/ntcs.2023.17891>
- [3] S. Aqeel, A. S. Khan, I. A. Abbasi, F. Algami, and D. Grzonka, "Enhancing IoT security with a DNA-based lightweight cryptography system," *Sci. Rep.*, vol. 15, p. 13367, 2025. <https://doi.org/10.1038/s41598-025-96292-0>

- [4] R. Delfianti, V. A. Tazayul, B. Mustaqim, F. Nussyura, and C. Harsito, "Internet of Things (IoT) based electrical power monitoring system for solar power plants using the Telegram application," *Vokasi UNESA Bull. Eng. Technol. Appl. Sci.*, vol. 2, no. 3, pp. 428–443, 2025. <https://doi.org/10.26740/vubeta.v2i3.39405>
- [5] M. Iyobhebe, "A review on energy consumption model on hierarchical clustering techniques for IoT-based multilevel heterogeneous WSNs using energy aware node selection," *Vokasi UNESA Bull. Eng. Technol. Appl. Sci.*, vol. 2, no. 2, pp. 100–111, 2025. <https://doi.org/10.26740/vubeta.v2i2.34882>
- [6] M. M. Mansour, A. M. Lafta, A. M. Salman, and H. S. Salman, "Exploring the role of AI and IoT in production efficiency, quality, and sustainability in manufacturing," *Vokasi UNESA Bull. Eng. Technol. Appl. Sci.*, vol. 2, no. 2, pp. 342–355, 2025. <https://doi.org/10.26740/vubeta.v2i2.38200>
- [7] A. M. K. Aliyu Musa Kid, M. Z. Ahmed, A. H. Alkali, J. Usman, and A. H. A. Hashim, "Real-time energy demand forecasting and adaptive demand response optimization for IoT-enabled smart grids," *Vokasi UNESA Bull. Eng. Technol. Appl. Sci.*, vol. 2, no. 2, pp. 366–375, 2025. <https://doi.org/10.26740/vubeta.v2i2.36818>
- [8] R. D. Handayani, Z. Jamal, M. Alkahfiansyah, L. Rosmalia, N. H. Sudibyo, and R. Herwanto, "Intelligent and secure package receiver system utilizing Internet of Things (IoT) technology," *Vokasi UNESA Bull. Eng. Technol. Appl. Sci.*, vol. 2, no. 3, pp. 581–592, 2025. <https://doi.org/10.26740/vubeta.v2i3.38254>
- [9] M. Țălu, "Security and privacy in the IIoT: Threats, possible security countermeasures, and future challenges," *Comput. AI Connect*, vol. 2, pp. 1–12, 2025. <https://doi.org/10.69709/CAIC.2025.139199>
- [10] A. Nazarov, D. Nazarov, and Ș. Țălu, "Information security of the Internet of Things," *Proc. Int. Sci. Pract. Conf. Comput. Inf. Security (INFSEC)*, Yekaterinburg, Russia, pp. 136–139, 2021. <https://doi.org/10.5220/0010619900003170>
- [11] M. Țălu, "Security in Internet of Things and Cloud Computing convergence: Current trends, challenges, and perspectives," *Ann. Fac. Eng. Hunedoara – Int. J. Eng.*, vol. XXIII, no. 4, pp. 39–52, 2025.
- [12] A. A. Laghari, H. Li, A. A. Khan, Y. Shoulin, S. Karim, and M. A. K. Khani, "Internet of Things (IoT) applications security trends and challenges," *Discov. Internet Things*, vol. 4, p. 36, 2024. <https://doi.org/10.1007/s43926-024-00090-5>
- [13] M. Țălu, "Cyberattacks and cybersecurity: Concepts, current challenges, and future research directions," *Digit. Technol. Res. Appl.*, vol. 4, no. 1, pp. 44–60, 2025. <https://doi.org/10.54963/dtra.v4i1.919>
- [14] C. Silva, N. Tenório, and J. Bernardino, "Lightweight encryption algorithms for IoT," *Computers*, vol. 14, no. 12, p. 505, 2025. <https://doi.org/10.3390/computers14120505>
- [15] S. Lakshmanan, T. Kokilavani, and P. Joseph Charles, "DNA secured edge computing for heterogeneous IoT," *J. Electr. Syst.*, vol. 20, no. 3, pp. 3879–3885, 2024.
- [16] M. Țălu, "Performance evaluation of DNA-based cryptographic algorithms on constrained IoT devices," *JUTI: J. Ilm. Teknol. Inf.*, vol. 24, no. 1, pp. 132–148, 2026. <https://doi.org/10.12962/j24068535.v24i1.a1386>
- [17] G. C. Stănică and P. Angheliescu, "Cryptographic algorithm based on hybrid one-dimensional cellular automata," *Mathematics*, vol. 11, no. 6, p. 1481, 2023. <https://doi.org/10.3390/math11061481>
- [18] S. A. Ansari and S. Ali, "A systematic review of lightweight cryptographic schemes for security and privacy in IoT," *Discov. Comput.*, vol. 28, p. 266, 2025. <https://doi.org/10.1007/s10791-025-09755-3>
- [19] C.L. Chen, K. W. Zeng, W.Y. Li, C.F. Lee, L.C. Liu, and Y.Y. Deng, "Lightweight post-quantum cryptography: Applications and countermeasures in Internet of Things, blockchain, and e-learning," *Eng. Proc.*, vol. 103, no. 1, p. 14, 2025. <https://doi.org/10.3390/engproc2025103014>
- [20] S. M. Al-Nofaie, S. Sharaf, and R. Molla, "Design trends and comparative analysis of lightweight block ciphers for IoTs," *Appl. Sci.*, vol. 15, no. 14, p. 7740, 2025. <https://doi.org/10.3390/app15147740>
- [21] S. Kumar, D. Kumar, R. Dangi, G. Choudhary, N. Dragoni, and I. You, "A review of lightweight security and privacy for resource-constrained IoT devices," *Comput. Mater. Contin.*, vol. 78, pp. 31–63, 2024. <https://doi.org/10.32604/cmc.2023.047084>
- [22] J. Soto-Cruz, E. Ruiz-Ibarra, J. Vázquez-Castillo, A. Espinoza-Ruiz, A. Castillo-Atoche, and J. Mass-Sanchez, "A survey of efficient lightweight cryptography for power-constrained microcontrollers," *Technologies*, vol. 13, p. 3, 2025. <https://doi.org/10.3390/technologies13010003>
- [23] X. Huang, L. Li, and J. Yang, "IVLBC: An involutive lightweight block cipher for Internet of Things," *IEEE Syst. J.*, vol. 17, pp. 3192–3203, 2023. <https://doi.org/10.1109/JSYST.2022.3227951>
- [24] Q. Yan, Y. Guo, W. Liu, W. Chen, and Y. Lu, "LIBC: A low-cost lightweight block cipher for IoT application," *Phys. Scr.*, vol. 100, pp. 1–18, 2025. <https://doi.org/10.1088/1402-4896/ad9867>
- [25] A. A. Anton, P. Csereoka, E. A. Capota, and R. D. Cioargă, "SIMECK-T: An ultra-lightweight encryption scheme for resource-constrained devices," *Appl. Sci.*, vol. 15, p. 1279, 2025. <https://doi.org/10.3390/app15031279>
- [26] N. Hediye and B. P. Divakar, "NDN: An ultra-lightweight block cipher to secure IoT nodes," *Int. J. Comput. Netw. Appl.*, vol. 12, pp. 227–251, 2025. <https://doi.org/10.22247/ijcna/2025/15>
- [27] D. Singh, M. Kumar, and T. Yadav, "RAZOR: A lightweight block cipher for security in IoT," *Def. Sci. J.*, vol. 74, pp. 46–52, 2024. <https://doi.org/10.14429/dsj.74.18421>
- [28] X. Zhang, C. Shao, T. Li, Y. Yuan, and C. Wang, "GFSPX: An efficient lightweight block cipher for resource-constrained IoT nodes," *J. Supercomput.*, vol. 80, pp. 25256–25282, 2024. <https://doi.org/10.1007/s11227-024-06412-2>
- [29] G. S. Sundaram, S. Pavithra, A. Arthi, B. M. Bala, and S. Mahalakshmi, "Cellular automata-based DNA cryptography algorithm," *Proc. IEEE 9th Int. Conf. Intell. Syst. Control (ISCO)*, pp. 1–6, 2015. <https://doi.org/10.1109/ISCO.2015.7282333>

- [30] M. Țălu, “DNA-based cryptography for Internet of Things security: Concepts, methods, applications, and emerging trends,” *Bul. Ilm. Sarjana Tek. Elektro*, vol. 7, no. 2, pp. 68–94, 2025.
- [31] M. Mondal and K. S. Ray, “Review on DNA cryptography,” *Int. J. Bioinformatics Intell. Comput.*, vol. 2, no. 1, pp. 44–72, 2023. <https://doi.org/10.61797/ijbic.v2i1.198>
- [32] J. Gao and T. Xie, “DNA computing in cryptography,” *Adv. Comput.*, vol. 129, pp. 83–128, 2023. <https://doi.org/10.1016/bs.adcom.2022.08.002>
- [33] M. Țălu, “Securing IoT ecosystems: Experimental evaluation of modern lightweight cryptographic algorithms and their performance,” *J. Cyber Secur.*, vol. 7, no. 1, pp. 565–587, 2025. <https://doi.org/10.32604/jcs.2025.073690>
- [34] S. Roy, U. Rawat, and J. Karjee, “A lightweight cellular automata-based encryption technique for IoT applications,” *IEEE Access*, vol. 7, pp. 39782–39793, 2019. <https://doi.org/10.1109/ACCESS.2019.2906326>
- [35] B. Yogi, A. K. Khan, and S. Roy, “HL-CAIoT: Hybrid lightweight cipher for IoT with chaotic maps and cellular automata,” *IEEE Access*, vol. 13, pp. 168067–168086, 2025. <https://doi.org/10.1109/ACCESS.2025.3611240>
- [36] B. Yogi, A. K. Khan, and S. Roy, “Cellular automata based key distribution for lightweight hybrid image encryption with elliptic curve cryptography,” *Sci. Rep.*, vol. 15, p. 34437, 2025. <https://doi.org/10.1038/s41598-025-17536-7>
- [37] M. S. Turan, K. McKay, D. Chang, L. E. Bassham, J. Kang, N. D. Waller, J. M. Kelsey, and D. Hong, Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process, NIST IR 8454, 2023.
- [38] M. Țălu, “Temporal DNA-based key derivation and metadata fingerprinting for secure on-device digital forensics in IoT systems,” *Comput. AI Connect*, vol. 3, pp. 1–27, 2026. <https://doi.org/10.69709/CAIC.2026.165654>
- [39] ISO 29192-2:2012(E), Information Technology—Security Techniques—Lightweight Cryptography—Part 2: Block Ciphers. Geneva, Switzerland: Int. Organization for Standardization, 2012.
- [40] M. El-Hajj, “Lightweight post-quantum cryptographic solutions for IoT: A practical approach,” *Proc. 2025 5th Intelligent Cybersecurity Conference (ICSC)*, Tampa, FL, USA, 2025, pp. 17–26. <https://doi.org/10.1109/ICSC65596.2025.11139871>
- [41] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, “Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities,” *IEEE Access*, vol. 9, pp. 28177–28193, 2021. <https://doi.org/10.1109/ACCESS.2021.3052867>
- [42] P. S. Suryateja and K. Venkata Rao, “A Survey on Lightweight Cryptographic Algorithms in IoT,” *Cybernetics and Information Technologies*, vol. 24, no. 1, pp. 65–86, 2024. <https://doi.org/10.2478/cait-2024-0002>
- [43] A. Amrita, C. P. Ekwueme, I. H. Adam, and A. Dwivedi, “Lightweight Cryptography for Internet of Things: A Review,” *EAI Endorsed Transactions on Internet of Things*, vol. 10, 2024. <https://doi.org/10.4108/eetiot.5565>
- [44] T. M. Fernandez-Carames, “From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things,” 2024.
- [45] T. Liu, G. Ramachandran, and R. Jurdak, “Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization,” 2024.
- [46] J. Rubia, B. L. Rincy, E. E. Nithila, S. S. C., and R. A., “A Survey about Post Quantum Cryptography Methods,” *EAI Endorsed Transactions on Internet of Things*, vol. 10, 2024. <https://doi.org/10.4108/eetiot.5099>
- [47] A. Babu, S. A. P. Kumar, A. G. Reddy, and A. K. Das, “Quantum Secure Authentication and Key Agreement Protocols for IoT-Enabled Applications: A Comprehensive Survey and Open Challenges,” *Computer Science Review*, vol. 54, article 100676, 2024. <https://doi.org/10.1016/j.cosrev.2024.100676>
- [48] A. Alomari, and S. A. P. Kumar, “Securing IoT Systems in a Post-Quantum Environment: Vulnerabilities, Attacks, and Possible Solutions,” *Internet of Things*, vol. 25, article 101132, 2024. <https://doi.org/10.1016/j.iot.2024.101132>
- [49] S. Afzal, M. U. Bokhari, S. Alam, I. Khan, M. Shuaib, and M. Ullah, “Lightweight deep learning-driven secure communication architecture for Internet of Things enabled government applications,” *Discover Computing*, vol. 29, no. 1, Art. no. 112, 2026. <https://doi.org/10.1007/s10791-026-10002-6>
- [50] V. Bhandiwad and L. K. Ragha, “Enhancing the security of IoT enabled systems using lightweight hybrid cryptography models,” *Cluster Computing*, vol. 28, Art. no. 189, 2025. <https://doi.org/10.1007/s10586-024-04897-3>
- [51] A. Alshammari, “Energy-efficient cryptographic protocols for sustainable IoT security: A federated learning-enhanced lightweight framework with post-quantum resilience,” *Sensors*, vol. 26, no. 12, Art. no. 3656, 2026. <https://doi.org/10.3390/s26123656>
- [52] F. Nujumudeen, M. N. Mubarak, and Y. K. Sharma, “A hybrid chaos-based cryptographic framework for lightweight IoT security: Enhancing efficiency and security in low-power devices,” *Peer-to-Peer Networking and Applications*, vol. 19, Art. no. 53, 2026. <https://doi.org/10.1007/s12083-025-02188-1>

BIOGRAPHIES OF AUTHORS



Mircea Țălu    obtained his Bachelor's degree in Computer Science from the Technical University of Cluj-Napoca, Romania. He is currently pursuing a Master's degree in Cybersecurity at the same institution, specializing in information security, cryptographic protocols, and secure communication architectures, with a focus on enhancing the resilience of modern digital infrastructures. Professionally, Mircea Țălu is a Software System Engineer at SC ACCESA IT SYSTEMS SRL, Cluj-Napoca, Romania, where he is involved in the research, development, and optimization of scalable, high-performance software solutions. His work focuses on designing secure and efficient computing architectures, including low-latency and high-throughput systems, contributing to the advancement of modern digital technologies and performance-driven computational models for complex software environments. His primary research interests include WebAssembly, the Extended Berkeley Packet Filter (eBPF), eXpress Data Path (XDP), Cloud and Edge Computing, the Internet of Things (IoT), Artificial Intelligence (AI), Blockchain Technology, Digital Forensics, AI-Driven Threat Intelligence, Cryptography, and Cybersecurity. In addition to his academic and professional work, Mircea Țălu is a FIDE Master in chess, reflecting robust analytical and strategic abilities at an international level and reinforcing his capacity for precise, creative problem-solving. He can be contacted at email: talus.mircea@gmail.com; mircea.talu@accesa.eu.