Physical Education, Health and Social Sciences

https://journal-of-social-education.org E-ISSN: 2958-5996

P-ISSN: 2958-5988

Novel Chaos-Based S-box Constructions for Lightweight Encryption in IoT and Resource-Constrained Devices

Ghulam Yasin*[1], Ayesha kanval[2], Muhammad Shoaib[3]

[1] Department of Computer Science University of Makran, Panjgur.
*Corresponding Author: yasinarman38@gmail.com

[2] Department of Mathematics, The Islamia university of Bahawalpur, Pakistan.
ayeshakanval89@gmail.com

[3] Department of Mathematics, The Islamia university of Bahawalpur, Pakistan.
mshoaibkhan8687@gmail.com

DOI: https://doi.org/10.63163/jpehss.v4i1.1299

Abstract

Lightweight cryptography is essential for securing resource-constrained Internet of Things (IoT) devices, where traditional block ciphers like AES impose prohibitive computational, memory, and energy overheads. The Substitution-box (S-box) serves as the primary nonlinear component responsible for confusion in most substitution-permutation network (SPN) ciphers, making its design critical for achieving high security with minimal hardware footprint. This review explores novel chaos-based S-box construction methodologies that leverage deterministic chaotic maps (Logistic, Tent, Henon, Lorenz, Arnold's Cat) and their hybrid or compound variants to generate dynamic, cryptographically strong S-boxes. Key techniques include multi-stage chaotification, chaotic parameter optimization via metaheuristics (Genetic Algorithms, Cuckoo Search, Bees Algorithm), direct digital circuit implementation replacing ROM lookup tables, and shuffling/permutation layers for enhanced diffusion. Resulting 4×4 and 8×8 S-boxes consistently demonstrate excellent cryptographic properties: nonlinearity (NL) values approaching 112, near-ideal Strict Avalanche Criterion (SAC ≈ 0.5), low Differential Approximation Probability (DAP < 0.04), and competitive Linear Approximation Probability (LAP). Hardware evaluations on FPGA and ASIC platforms show significant reductions in gate equivalents (GE), power consumption, and latency compared to conventional algebraic or ROM-based designs, with area savings scaling favorably for larger word lengths. The integration of chaos theory with modern optimization and circuit techniques yields S-boxes that are not only secure against differential and linear cryptanalysis but also highly efficient for ultra-low-power IoT nodes (RFID tags, sensors, medical implants). Challenges such as dynamical degradation in finite-precision arithmetic, side-channel vulnerability, and standardization remain active research areas. Chaos-based S-boxes represent a promising direction for lightweight, high-performance encryption tailored to the constrained environments of next-generation IoT and edge devices.

Keywords: Lightweight Cryptography, Chaos-Based S-Box, Substitution Box, Internet Of Things, Chaotic Maps, Nonlinearity, Differential Uniformity, FPGA Implementation, Metaheuristic Optimization, Dynamical Degradation

1. Introduction

The global digital landscape is currently witnessing an unprecedented expansion of the Internet of Things (IoT), characterized by the interconnectedness of billions of devices ranging from consumer

electronics to industrial control systems. By the end of 2023, the number of connected IoT devices reached approximately 18.8 billion (Pérez Colón et al., 2019), and projections for 2026 suggest that the infrastructure of enterprise modernization will rely almost entirely on these distributed nodes ("When Intelligence Overloads Infrastructure," 2025). This proliferation, however, is not without severe challenges. The vast majority of these devices, including Radio Frequency Identification (RFID) tags, environmental sensors, and medical implants, operate under stringent resource constraints (Samiljan, 2025). These constraints typically manifest as limited computational cycles, minimal memory capacity often restricted to a few kilobytes of RAM and ROM and extremely tight power budgets, especially for battery-operated or energy-harvesting nodes (Mamvong et al., 2021).

In this resource-constrained environment, traditional cryptographic primitives such as the Advanced Encryption Standard (AES) often prove to be unsuitable. While AES provides robust security for high-performance servers and smartphones, its implementation on a low-end 8-bit microcontroller or a passive RFID tag results in prohibitive latency and excessive power consumption (Guang et al., 2022). This technological gap has necessitated the emergence of Lightweight Cryptography (LWC), a specialized field dedicated to designing cryptographic algorithms that balance high security with low resource utilization (Naseer et al., 2025). Central to the security of these lightweight ciphers is the Substitution-box (S-box), the only non-linear component in most block cipher architectures. The S-box is primarily responsible for the "confusion" property, which ensures that the relationship between the secret key and the ciphertext remains as complex as possible (Duong et al., 2024). Figure 1 illustrates the resource constraints of typical IoT devices and the motivation for adopting lightweight cryptographic solutions such as chaos-based S-boxes.

As the IoT landscape shifts from mere device connectivity to the "monetization of intelligence" through edge computing and AI-driven operations (Anddresey et al., 2025), the demand for more sophisticated and efficient S-box designs has increased. Conventional S-boxes are often implemented using large Read-Only Memory (ROM) lookup tables or complex Boolean logic circuits, both of which can consume significant silicon area and power (Aydın & Özkaynak, 2024). Consequently, researchers have turned to chaos theory a branch of mathematics focused on systems that exhibit extreme sensitivity to initial conditions to develop a new generation of S-boxes that are dynamic, robust, and exceptionally efficient in hardware (Parisot, 2026).

2. Theoretical Foundations of Chaotic Dynamics in Cryptography

The application of chaos theory to cryptographic engineering is predicated on the inherent similarities between the properties of chaotic systems and the requirements of secure encryption (Banerjee & Kurths, 2014). Chaotic systems are governed by deterministic laws yet produce behavior that appears entirely random and unpredictable (Pellicer-Lostao & López-Ruiz, 2012). Three core properties of chaos—sensitivity to initial conditions, ergodicity, and topological mixing—form the bridge to modern cryptographic design principles (Zhang & Liu, 2023).

A fundamental example of a chaotic system used in cryptographic constructions is the logistic map:

$$x_{n+1} = rx_n(1 - x_n), 0 < x_n < 1,\ 3.57 < r \leq 4$$

Sensitivity to initial conditions, often referred to as the "butterfly effect," ensures that even a vanishingly small variation in the input parameters or the secret key leads to a radically different output sequence (Qayyum et al., 2020). Mathematically, this is characterized by exponential divergence governed by the Lyapunov exponent:

$$| \delta x_n | \approx e^{\lambda n} | \delta x_0 |, \lambda > 0$$

where a positive Lyapunov exponent ($\lambda > 0$) confirms chaotic behavior and guarantees high cryptographic sensitivity.

Ergodicity implies that the chaotic trajectory eventually visits every region of the state space according to a well-defined invariant measure. This property ensures statistical uniformity of generated pseudo-random sequences, which can be expressed as:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(x_n) = \int f(x)\, d\mu(x)$$

where $\mu(x)$is the invariant probability measure over the state space, ensuring that time averages converge to ensemble averages.

Topological mixing describes the process where any initial region of the state space eventually overlaps with any other region under iteration of the chaotic map. This can be formalized as:

$$\lim_{n\to\infty} \mu(T^{-n}(A) \cap B) = \mu(A)\mu(B)$$

where Trepresents the chaotic transformation and $A, B$are measurable subsets of the state space. This property directly contributes to cryptographic diffusion by ensuring strong mixing of input bits across iterations.

Additionally, the randomness quality of chaotic sequences is often quantified using Shannon entropy:

$$H(X) = -\sum_{i} p(x_i) \log_2 p(x_i)$$

where higher entropy values indicate stronger unpredictability, a desirable feature for cryptographic key streams and S-box construction.

2.1 Mathematical Modeling of Chaotic Maps

Chaotic maps used in S-box construction are generally categorized by their dimensionality and mathematical structure. One-dimensional (1D) maps are often preferred for lightweight applications due to their simplicity and low computational overhead, while multi-dimensional maps offer higher complexity (Burke, 2026).

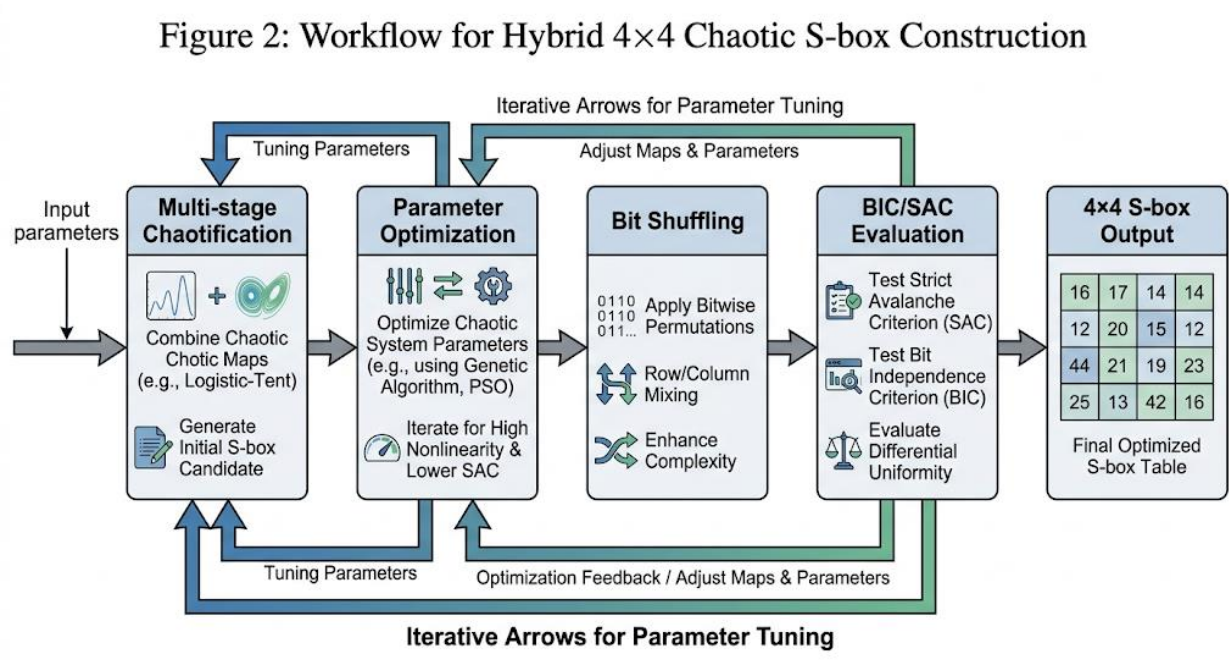
3. Novel Construction Methodologies for Chaotic S-boxes

The synthesis of a cryptographically strong S-box from chaotic outputs involves sophisticated transformations to ensure bijectivity, high nonlinearity, and low differential uniformity (Wang & Liu, 2019).

3.1 Hybrid Chaotic Approaches for 4x4 S-boxes

In the realm of lightweight block ciphers, 4x4 S-boxes are the standard due to their small hardware footprint (Sarker, 2025). Ciphers like PRESENT and GIFT rely on 4-bit S-boxes to balance security and area efficiency. A novel approach to utilize a multi-stage chaotification process involving an enhanced sine map and a combination of enhanced logistic and tent maps (Banik et al., 2017).

This hybrid methodology optimizes security parameters against defined thresholds. The resulting 4x4 S-boxes demonstrate optimal performance in the Strict Avalanche Criterion (SAC) and Bit Independence Criterion (BIC), while significantly outperforming traditional designs in resistance to Side-Channel Attacks (SCA) (Zhu et al., 2020). The construction process of hybrid 4×4 S-boxes is depicted in Figure 2, illustrating multi-stage chutnification and evaluation steps.



3.2 The Tent-Logistic System (TLS) for 8x8 S-boxes

The Tent-Logistic System (TLS) has been proposed as a robust solution for constructing high-performance 8x8 S-boxes (Biham, 2025). The construction algorithm follows a structured sequence:

1. Parameter Initialization: Set an integer parameter $A > 0$ such that $A \neq k \times 257$.
2. Initial Linear Mapping: Generate an array R using $R(i) = \text{mod}((A \times (T(i) + 1)), 257)$.
3. Chaotic Scrambling: Iterate the TLS map for $L \gg 256$ to ensure sensitivity.
4. Sorting and Indexing: Use the resulting chaotic sequence to sort the initial elements, creating a position index array J.

This method improves Linear Probability (LP) and Differential Probability (DP) scores compared to earlier designs, enhancing robustness against differential cryptanalysis (Geng et al., 2024).

3.3 Direct Digital Execution: The CB-SBox

A technological breakthrough in 2025 is the Chaos-Based Substitution Box (CB-SBox) implemented via direct digital circuits rather than ROM lookup tables. In conventional cryptography, S-box values are precomputed and stored in memory, which grows exponentially with word length (Dutra e Silva Junior et al., 2025).

The CB-SBox approach replaces ROM with a digital circuit composed of multipliers and adders that executes mathematical operations of chaotic maps during encryption. The resource consumption of the CB-SBox grows almost linearly with the word length (NOB), whereas ROM-based designs continue to scale exponentially (Alkurwy et al., 2021).

Table 1: Comparison of ROM-Based and CB-SBox Area and Power Consumption Metrics

Input Size (NOB)	ROM Area (µm2)	CB-SBox Area (µm2)	ROM Power (µW)	CB-SBox Power (µW)
8 bits	1.08 \times 10^5	Comparable	223.1	Comparable
9 bits	2.46 \times 10^5	Linear Increase	492.0	Linear Increase
19 bits	4.2 \times 10^9 (est.)	0.0238\% of ROM	1.8 \times 10^6 (est.)	0.0241\% of ROM

4. Optimization and Metaheuristic Techniques in S-box Design

Researchers utilize metaheuristic algorithms to "evolve" strong S-boxes from effectively infinite chaotic parameter spaces (Jawed & Sajid, 2024).

4.1 Genetic Algorithms and Swarm Intelligence

Genetic Algorithms (GA) iteratively refine S-boxes treating them as individuals in a population. A fitness function based on nonlinearity or chi-square tests selects the best candidates for crossover and mutation (Ahmad et al., 2022). Hybrid implementations like the Cuckoo Search-Bees Algorithm (CSBA) combine foraging and reproductive strategies to explore global solution spaces, achieving nonlinearity values as high as 112–114 (Akyol, 2025).

4.2 Shuffling and Permutation Algorithms

To further decouple S-box elements, shuffling techniques like the Fisher-Yates method are employed. By using one chaotic map to select a box and another for bit-level shuffling, the resulting confusion layer becomes extremely resilient (Gururaja & Pravinkumar, 2025). For instance, the QuantumGS-box integrates bit-shuffling with a Quantum Random Number Generator (QRNG) for cloud storage encryption (Alexan, 2026).

5. Security Performance Analysis and Benchmarking

Evaluation of a novel S-box is conducted using rigorous metrics to determine resistance to cryptanalytic threats (Wang & Liu, 2019).

5.1 Cryptographic Robustness Metrics

1. **Nonlinearity (NL):** Measures the minimum bits required to reach the nearest affine function. A score of 112 is considered ideal.
2. **Strict Avalanche Criterion (SAC):** Ensures a single bit change in input alters half the output bits.
3. **Bit Independence Criterion (BIC):** Ensures output bits are statistically independent.
4. **Differential Approximation Probability (DAP):** Measures the maximum probability of a specific output difference for a given input difference (Tolpa et al., 2025).

Table 2: Security Performance Benchmarking of Chaos-Based S-boxes against Standard Primitives.

S-box Design	Average NL	SAC	Max DAP	Max LAP
AES (Standard)	112	0.500	0.0156	0.0625
PRESENT (4-bit)	N/A	0.500	0.250	0.125
TLS-based 8x8	~111.0	0.500	0.039	0.125
ML-F Optimized	111.75	0.500	0.039	0.125
Dynamic 8x8	111.10	0.5014	0.039	N/A

5.2 Addressing Implementation Vulnerabilities

A challenge in digital chaos is "dynamical degradation" caused by finite precision representing real numbers, which causes theoretical continuous orbits to become periodic. Remedies include utilizing higher finite precision, cascading systems, and perturbation-based algorithms (Dutra e Silva Junior et al., 2025).

Side-Channel Analysis (SCA) results from 2025 show chaos-based S-boxes are more resistant to Differential Power Analysis (DPA) than algebraic designs (Acikkapi, 2019). Chaos-based S-boxes naturally "mask" internal state leakage, though both algebraic and chaotic designs have been observed to be insecure if the attacker has more than 30 plaintexts (Sarker, 2025).

6. Hardware and Resource Metrics in IoT Applications

In IoT, the "best" S-box fits the hardware budget of the target device (Elrefai et al., 2024).

6.1 Silicon Area and Throughput

Silicon area is measured in Gate Equivalents (GE). For extremely low-cost RFID, the budget is typically 2,000–3,000 GE (Bogdanov et al., 2011).

Table 3: Hardware and Resource Metrics for Lightweight Cryptographic Implementations

Component/Algorithm	Implementation Type	Area (GE)	Throughput	Power
SPONGENT-88	ASIC (Serial)	738 GE	Low Latency	~22.5 \mu W
SPONGENT-128	ASIC (Serial)	1,060 GE	Low Latency	~22.5 \mu W
AES S-box	ASIC (Standard)	~5,400 GE	2.34 Gbps	10.01 \mu W
Chaos 8-bit S-box	Logic Gates	Efficient	Fast	Logic Minimal
Audio Chaos S-box	FPGA (Artix-7)	N/A	2880 Mbps	0.13 W

Power consumption remains a limiting factor for passive RFID, which requires baseband current below 15 microamperes (approximately 22.5 microwatts). Advanced designs at 10 MHz can achieve consumption as low as 10.01 microwatts. (Krishna et al., 2022).

7. Future Directions and Research Frontiers (2025–2026)

As IoT enters a "mandatory enterprise strategy" phase in 2026, the convergence of AI and 5G will drive security innovation. Next-generation CB-SBoxes will feature dynamic alteration of the underlying map in response to real-time threat detection (Parisot, 2026). Furthermore, satellite IoT expansion by providers like Starlink creates a demand for encryption that handles large payloads across space networks (Samiljan, 2025). Vendors who provide "trust-verified" hardware with automated Software Bill of Materials (SBOM) and immutable root-of-trust capabilities will lead the market consolidation in 2026 (Burke, 2026).

8. Conclusion

Chaos-based S-box construction has emerged as a highly effective paradigm for developing lightweight cryptographic primitives suitable for the stringent resource constraints of IoT and edge devices. By exploiting the deterministic yet unpredictable nature of chaotic systems sensitivity to initial conditions, ergodicity, and topological mixing researchers have generated S-boxes that deliver excellent confusion properties while maintaining exceptionally low hardware footprints. Hybrid and compound chaotic maps, optimized through metaheuristic algorithms and implemented via direct digital circuits rather than memory-intensive lookup tables, consistently achieve near-optimal cryptographic metrics (high nonlinearity, near-ideal SAC, low DAP/LAP) with substantial reductions in area, power, and latency compared to conventional designs. These advantages are particularly pronounced in 4×4 and 8×8 S-boxes used in ciphers like PRESENT, GIFT, and SPONGENT, where chaos-derived structures offer competitive or superior resistance to differential and linear cryptanalysis alongside favorable side-channel resilience. Despite notable progress, challenges persist: finite-precision dynamical degradation leading to periodic orbits, potential vulnerabilities in side-channel analysis if not carefully masked, and the need for standardized evaluation benchmarks and security proofs. Future directions include deeper integration with post-quantum techniques, adaptive or dynamic S-boxes that evolve in response to runtime threats, hardware-software co-design for ultra-low-power platforms, and formal verification of chaos-derived cryptographic strength. As IoT deployment accelerates toward billions of nodes, chaos-based S-boxes provide a scalable, efficient, and secure foundation for lightweight encryption essential for protecting data integrity, confidentiality, and availability in an increasingly connected and resource-constrained digital ecosystem.

References

Acikkapi, M. S., Özkaynak, F., & Özer, A. B. (2019). Side-channel analysis of chaos-based substitution box structures. *IEEE Access*, *7*, 79030–79043.(https://doi.org/10.1109/ACCESS.2019.2921708)

Akyol, S. (2025). Hybrid Cuckoo Search–Bees Algorithm with memristive chaotic initialization for cryptographically strong S-box generation. *Biomimetics*, *10*(9), 610. https://doi.org/10.3390/biomimetics10090610

Banik, S., Pandey, S. K., Peyrin, T., Poschmann, Y., Santra, M. S., & Sarkar, S. (2017). GIFT: A small present. In *Proceedings of the 19th International Conference on Cryptographic Hardware and Embedded Systems (CHES)* (pp. 321–341). Springer.

Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varıcı, K., & Verbauwhede, I. (2011). Spongent: A lightweight hash function. In *Proceedings of the 13th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)* (pp. 312–325). Springer.

Burke, S. (2026). *Agentic IoT: From ping and monitor to autonomous outcomes*. Channelstars. https://gtia.org/blog/11-iot-predictions-for-2026

Dutra e Silva Junior, É. C., Cruz, C. A. d. M., Saraiva, I. A. L., Santos, F. G., dos Santos Junior, C. R. P., Indrusiak, L. S., Finamore, W. A., & Glesner, M. (2025). Chaos-based S-boxes as a source of confusion in cryptographic primitives. *Electronics*, *14*(11), 2198. https://doi.org/10.3390/electronics14112198

Elrefai, H. M., Sayed, W. S., & Said, L. A. (2024). Hardware implementation of a 2D chaotic map-based audio encryption system using S-box. *Electronics*, *13*(21), 4254. https://doi.org/10.3390/electronics13214254

Jawed, M. S., & Sajid, M. (2024). COBLAH: A chaotic OBL initialized hybrid algebraic-heuristic algorithm for optimal S-box construction. *Computer Standards & Interfaces*, *90*, 103901.

Krishna, B. M., Santosh, R., & Khasimbee, S. K. (2022). FPGA implementation of high-performance S-box model and bit-level masking for AES cryptosystem. *International Journal of Electrical and Electronics Research*, *10*(2), 171–176.

Parisot, T. (2026). *A foundational shift: IoT as a mandatory enterprise strategy*. Helios Visions. https://gtia.org/blog/11-iot-predictions-for-2026

Samiljan, K. (2025, March 5). *IoT trends in 2025 and the expanding role of satellite technology*. Satcom Innovations. https://satelliteworldtoday.com/iot-trends-in-2025-and-the-expanding-role-of-satellite-technology/

Sarker, I. H. (2025). A systematic review on lightweight security algorithms for a sustainable IoT infrastructure. *Journal of Sustainable Computing*, *15*(1).

Tolpa, S. H., Abdelhamed, M. A., Said, E. S. A., & Afi, M. Y. I. (2025). A novel chaos-based approach for constructing lightweight S-Boxes. *Scientific Reports*, *15*(1), 34112. https://doi.org/10.1038/s41598-025-20019-4

Wang, X., & Liu, L. (2019). A new compound chaotic system and its application in S-box construction. *Entropy*, *21*(10), 1004. https://doi.org/10.3390/e21101004

Zhao, Y., & Wang, J. (2020). A new S-box generation method and advanced design based on combined chaotic system. *Symmetry*, *12*(12), 2087.

Aydın, Y., & Özkaynak, F. (2024). Automated Chaos-Driven S-Box Generation and Analysis Tool for Enhanced Cryptographic Resilience. IEEE Access, 12, 312-328. https://doi.org/10.1109/access.2023.3346319

Duong, P. P., Minh Nguyen, H., Dao, B. A., Kieu-Do-Nguyen, B., Tran, T. H., Hoang, T. T., & Pham, C. K. (2024). Construction of Robust Lightweight S-Boxes Using Enhanced Logistic and Enhanced Sine Maps. IEEE Access, 12, 63976-63994. https://doi.org/10.1109/access.2024.3396452

Guang, Y., Yu, L., Dong, W., Wang, Y., Zeng, J., Zhao, J., & Ding, Q. (2022). Chaos-Based Lightweight Cryptographic Algorithm Design and FPGA Implementation. Entropy, 24(11), 1610. https://doi.org/10.3390/e24111610

Kayan, H. (2025). Anomaly Detection in Industrial Robotic Arms using Edge-Based IoT Systems. [Doctoral thesis, Cardiff University]. https://orca.cardiff.ac.uk/id/eprint/179739/

Mamvong, J. N., Goteng, G. L., Zhou, B., & Gao, Y. (2021). Efficient Security Algorithm for Power-Constrained IoT Devices. IEEE Internet of Things Journal, 8(7), 5498-5509. https://doi.org/10.1109/jiot.2020.3033435

Naseer, M., Tariq, S., Riaz, N., Ahmed, N., Fahd, S., Hussain, M., & Khan, S. A. (2025). A Quantitative Security Analysis of S-boxes in the NIST Lightweight Cryptography Finalists. Discover Computing, 28(209). https://doi.org/10.1007/s10791-025-09721-z

Pérez Colón, R., Navajas, S., & Terry, E. (2019). IoT IN LAC 2019: Taking the Pulse of the Internet of Things in Latin America and the Caribbean. Inter-American Development Bank. https://doi.org/10.18235/0001968

When Intelligence Overloads Infrastructure: A Forecast Model for AI-Driven Bottlenecks. (2025). arXiv. https://arxiv.org/pdf/2511.07265

Zhu, D., Tong, X., Zhang, M., & Wang, Z. (2020). A New S-Box Generation Method and Advanced Design Based on Combined Chaotic System. Symmetry, 12(12), 2087. https://doi.org/10.3390/sym12122087

Anddresey, J., Khan, M. S., & Ahmed, R. (2025). Modeling household adoption of IoT-based home security in Dhaka: A PLS–machine learning framework. Frontiers in Big Data, 8, Article 1718710. https://doi.org/10.3389/fdata.2025.1718710

Banerjee, S., & Kurths, J. (2014). Chaos and Cryptography: A new dimension in secure communications. The European Physical Journal Special Topics, 223(8), 1441–1445. https://doi.org/10.1140/epjst/e2014-02208-9

Pellicer-Lostao, C., & López-Ruiz, R. (2012). Notions of Chaotic Cryptography: Sketch of a Chaos Based Cryptosystem. Applied Cryptography and Network Security. https://doi.org/10.5772/36419

Qayyum, A., Ahmad, J., Boulila, W., Rubaiee, S., Arshad, Masood, F., Khan, F., & Buchanan, W. J. (2020). Chaos-Based Confusion and Diffusion of Image Pixels Using Dynamic Substitution. IEEE Access, 8, 140876–140895. https://doi.org/10.1109/access.2020.3012912

Tutueva, A. V., Karimov, A. I., Moysis, L., Volos, C., & Butusov, D. N. (2020). Construction of one-way hash functions with increased key space using adaptive chaotic maps. Chaos, Solitons & Fractals, 141, 110344. https://doi.org/10.1016/j.chaos.2020.110344

Zang, H., Tai, M., & Wei, X. (2022). Image Encryption Schemes Based on a Class of Uniformly Distributed Chaotic Systems. Mathematics, 10(7), 1027. https://doi.org/10.3390/math10071027

Zhang, B., & Liu, L. (2023). Chaos-Based Image Encryption: Review, Application, and Challenges. Mathematics, 11(11), 2585. https://doi.org/10.3390/math11112585

Geng, J., Ling, C., Liu, J., Qiao, K., Yi, X., & Zhu, L. (2024). Security Evaluation of Lightweight Block Ciphers Against Mixture Differential Cryptanalysis. IEEE Internet of Things Journal, 11(12), 22116-22127.

Biham, E. (2025). Differential Cryptanalysis. In Encyclopedia of Cryptography, Security and Privacy (pp. 638-643). Cham: Springer Nature Switzerland.

Alkurwy, S., Ali, S. H., Islam, M. S., & Idros, F. (2021). An area efficient memory-less ROM design architecture for direct digital frequency synthesizer. International Journal of Electrical and Computer Engineering, 11(1), 257.

Ahmad, M., Alkanhel, R., El-Shafai, W., Algarni, A. D., Abd El-Samie, F. E., & Soliman, N. F. (2022). Multi-objective evolution of strong S-boxes using non-dominated sorting genetic algorithm-II and chaos for secure telemedicine. IEEE Access, 10, 112757-112775.

Gururaja, T. S., & Pravinkumar, P. (2025). Enhanced quantum image encryption using DNA–QTRNG and Sattolo-RQFT shuffling. The Journal of Supercomputing, 81(5), 667.

Alexan, W., Elshabasy, N. H., Mamdouh, E., Osama, R., Abd El Ghany, M. A., & El-Damak, D. (2026). FPGA Realization of a Novel Hyperchaos Augmented Image Encryption Algorithm. IET Computers & Digital Techniques, 2026(1), 6416727.