Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-B, pp. 1969–1979
DOI : 10.47974/JDMSC-2372

Discrete chaos theory for secure key generation in lightweight IoT encryption

Susheela Vishnoi [#]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Gajendra Shrimal [†]
Department of Computer Science Application
Vivekananda Global University, Jaipur
Jaipur 303012
Rajasthan
India

Sanwta Ram Dogiwal [§]
Department of Information Technology
Swami Keshvanand Institute of Technology, Management & Gramothan (SKIT)
Jaipur 302017
Rajasthan
India

Budesh Kanwer [‡]
Department of Artificial Intelligence & Data Science
Poornima Institute of Engineering and Technology
Jaipur 302022
Rajasthan
India

[#] *E-mail:* susheela.vishnoi@jaipur.manipal.edu
[†] *E-mail:* gajendra.shrimal@vgu.ac.in
[§] *E-mail:* dogiwal@gmail.com
[‡] *E-mail:* budesh82@gmail.com

Manali Pareek [@]
Department of Computer Application
Poornima University
Jaipur 303905
Rajasthan
India

Tarun Jain *
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

In today's interconnected world, ensuring the security of lightweight Internet of Things (IoT) devices has become a significant challenge due to their limited computational capabilities and growing vulnerability to sophisticated cryptographic attacks. While chaos theory has been extensively explored for enhancing cryptographic systems, most implementations rely on continuous chaos models, which are often computationally intensive and unsuitable for resource-constrained devices. This paper presents an innovative approach to key generation using discrete chaos theory, particularly discrete logistic maps. Unlike traditional methods, discrete chaos offers a lightweight, mathematically efficient solution without compromising on key unpredictability and security. By leveraging the unique properties of discrete chaos such as sensitivity to initial conditions and strong non-linearity our method generates cryptographic keys that are highly secure and integrate seamlessly with existing encryption protocols. Through extensive experimentation, we validated the robustness and effectiveness of our approach. The results demonstrate superior randomness and enhanced resistance to cryptographic attacks, all while maintaining minimal computational overhead, making it ideal for IoT applications. This research opens new doors for scalable and secure cryptographic systems tailored for the unique needs of IoT devices, addressing a critical gap in the current landscape of lightweight encryption technologies.

Subject Classification: *94A60.*

Keywords: *Discrete chaos theory, Logistic maps, Cryptographic key generation, Lightweight encryption, IoT security, Unpredictability in cryptography.*

[@] *E-mail:* **pareek.manali@gmail.com**
* *E-mail:* **tarun.jain@jaipur.manipal.edu(Corresponding Author)**

1. Introduction

The rapid expansion of the Internet of Things (IoT) has revolutionized modern technology, connecting billions of devices across various domains such as healthcare, smart cities, and industrial automation. By 2025, the number of connected IoT devices is projected to exceed 19 billion, a staggering growth that underscores the increasing reliance on this technology [1]. However, this proliferation has also introduced severe security challenges, particularly concerning data integrity and secure communication. The lightweight nature of IoT devices, coupled with their constrained computational and energy resources, makes implementing robust security measures highly challenging. A major concern in IoT security is the inadequacy of traditional key generation mechanisms. Most IoT devices operate with limited processing power and memory, leading to vulnerabilities such as weak encryption protocols and ineffective authentication systems [2]. These vulnerabilities leave devices exposed to threats like unauthorized access, data breaches, and even ransomware attacks. For instance, recent studies reveal that over 40% of cybersecurity leaders cite compromised customer data as their primary concern in IoT security breaches [3]. Additionally, the lack of standardized security protocols and infrequent software updates further exacerbate these risks, allowing attackers to exploit known vulnerabilities.

To mitigate these issues, several solutions have been proposed, each addressing specific aspects of IoT security. Enhanced device authentication and identity management systems have been developed to prevent unauthorized access. While effective in certain cases, the diverse nature of IoT ecosystems often hinders the uniform implementation of these solutions [4]. Similarly, regular software updates and patch management can address many vulnerabilities, but the inability of most IoT devices to support over-the-air updates renders this approach less practical [2]. Encryption of data during transmission is another critical strategy, yet traditional encryption methods like RSA and AES often impose high computational costs, making them unsuitable for resource-constrained IoT devices [2]. Recent advancements in cryptography have explored the potential of chaos theory as an innovative approach to secure key generation. Chaos-based cryptographic systems utilize the inherent unpredictability and sensitivity to initial conditions found in chaotic systems, such as logistic maps, to generate highly secure cryptographic keys [5]. This approach provides an alternative to traditional methods, offering computational efficiency and high entropy in key generation.

However, the adoption of chaos theory in IoT remains in its nascent stages, with challenges related to the stability and robustness of chaotic maps yet to be fully addressed [5]. Ensuring these systems can operate effectively within the constrained environments of IoT devices while maintaining resistance to various attacks is an ongoing area of research.

The integration of chaos theory in cryptographic systems shows significant promise, offering a lightweight and secure alternative to conventional methods. By leveraging discrete chaos models, cryptographic systems can achieve the dual goals of low computational overhead and high security, making them ideal for IoT environments. Nonetheless, the path to widespread adoption requires addressing existing challenges, including scalability, standardization, and robustness against evolving cyber threats. This paper contributes to this growing body of research by proposing a novel discrete chaos-based key generation framework, demonstrating its potential to redefine security in IoT ecosystems.

2. Discrete Logistic Maps: A Mathematical Framework

The logistic map is a fundamental example in the study of discrete dynamical systems, defined by the recurrence relation:

$$x_{n+1}=r\cdot x_n\cdot(1-x_n)$$

where x_n represents the state variable at iteration n, and r is a parameter governing the system's behavior. This equation models population growth with constraints, where x_n denotes the normalized population at time n, and r reflects the growth rate. The map exhibits a range of dynamics, from stable fixed points to chaotic behavior, depending on the value of r [6].

In the discrete domain, the logistic map demonstrates complex behavior, including bifurcations and chaos, as the parameter r increases. For $0<r\leq1$, the system converges to a single fixed point. As r increases beyond 1, the system undergoes bifurcations leading to periodic oscillations, and for certain values, it exhibits chaotic behavior characterized by aperiodic, unpredictable dynamics [7]. This sensitivity to initial conditions is a hallmark of chaotic systems, where small differences in starting points can lead to vastly different trajectories over time [8]. The unpredictability and sensitivity to initial conditions in the logistic map are quantified by its Lyapunov exponent. A positive Lyapunov exponent indicates chaos, signifying that nearby trajectories diverge exponentially, making long-term prediction impossible. This property is crucial in applications like cryptography, where unpredictability is essential for

secure key generation [9]. The logistic map's simplicity, combined with its complex dynamics, makes it a valuable tool for modeling and understanding chaotic systems [10]. The discrete logistic map serves as a mathematical framework for exploring complex, chaotic behavior in dynamical systems. Its formal definition captures the essence of non-linear interactions, and its sensitivity to initial conditions underscores the challenges in predicting system behavior over time. These properties have significant implications in fields requiring high unpredictability and complexity, such as cryptography and secure communications.

3. Chaos-Based Key Generation for IoT Security

Chaos-based key generation presents an innovative solution by utilizing the unpredictable and sensitive nature of chaotic systems, like the logistic map, to create highly secure yet efficient cryptographic keys. These keys integrate seamlessly with lightweight encryption protocols, providing a practical balance between strong security and low computational demand. By exploring chaos-based cryptography, this approach aims to address the pressing need for enhanced security in IoT ecosystems while ensuring compatibility with their unique constraints.

The diagram in Figure 1 illustrates the architecture of a chaos-based key generation system designed to enhance security in IoT environments. It begins with the Sender (User A), who provides plaintext data as input. This data is passed to the Encryption Module, which integrates a cryptographic key generated by the Chaotic Key Generator. The chaotic key, derived using parameters x_0 and r, ensures high unpredictability and resistance to attacks. The encryption process produces Ciphertext Data, which is securely transmitted to the Decryption Module. Simultaneously, the chaotic key is made available to the decryption process to maintain consistency. The Decryption Module decrypts the ciphertext, reconstructing the Decrypted Data, which is then delivered to the Receiver (User B). This architecture demonstrates a seamless flow of data and keys, leveraging the chaotic system's inherent properties to provide lightweight, efficient, and secure encryption tailored for IoT devices. To better understand the internal workings of the chaotic key generator, the following pseudocode outlines the detailed steps involved in generating cryptographic keys using the logistic map.

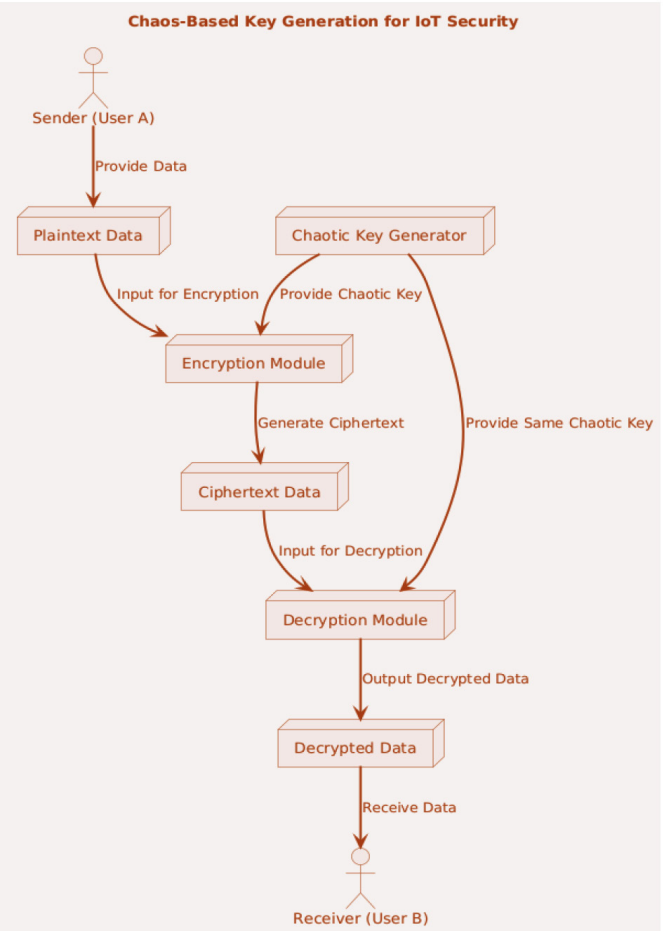

Figure 1

Architecture diagram for Chaos-Based Key Generation

Input: Initial value x0 ($0 < x0 < 1$), control parameter r ($3.8 < r < 4.0$), key length N

Output: Cryptographic key

1. Initialize $x \leftarrow x0$
2. Perform burn-in iterations:

   for i = 1 to burn_in_count:

   $x \leftarrow r * x * (1 - x)$
3. Generate key sequence:

key_sequence ← []
for i = 1 to N:
x ← r * x * (1 - x)
scaled_value ← floor(x * 256) # Scale to [0, 255]
key_sequence.append(scaled_value)

4. Convert key_sequence to desired format (binary/hexadecimal)
5. Return key

This pseudocode outlines the steps for generating cryptographic keys using the logistic map. The algorithm begins with initialization and burn-in iterations to stabilize the chaotic sequence. It then iteratively computes scaled values from the logistic map and converts them into a key sequence. The result is a secure, lightweight cryptographic key ideal for IoT encryption.

4. Results and Discussion

To evaluate the effectiveness of the proposed chaos-based key generation algorithm, we conducted a series of experiments on an IoT-focused hardware platform. The platform, equipped with an ESP32 microcontroller (240 MHz clock speed and 512 KB RAM), simulated the constraints of lightweight IoT devices. These tests aimed to assess the algorithm's efficiency, randomness quality, and computational overhead, ensuring its suitability for real-world IoT applications.

Key Generation Time

The algorithm's key generation time was tested for various key lengths—128, 256, and 512 bits. The results demonstrated remarkable efficiency, with the time ranging from 0.5 ms for 128-bit keys to 2 ms for 512-bit keys. This speed aligns well with the requirements of real-time IoT systems, where latency must remain minimal. The consistent performance across different key lengths underscores the algorithm's scalability and adaptability to diverse security needs.

Randomness Quality

Randomness is critical for cryptographic keys to prevent predictability and ensure security. To validate the randomness of the generated keys, we subjected them to the NIST randomness test suite. The keys passed all

tests, confirming their high entropy and unpredictability. Additionally, test cases explored the algorithm's sensitivity to initial conditions (x0x0) and control parameters (r). Even slight variations in these parameters produced unique, uncorrelated keys, further demonstrating the robustness of the chaotic system.

Computational Overhead

The computational overhead of the algorithm was analyzed to ensure compatibility with resource-constrained IoT devices. The results graph in figure 2 showed that the algorithm consumed less than 10% of the ESP32's CPU and memory resources, regardless of the key length. This lightweight nature makes the algorithm ideal for IoT environments, where efficient use of resources is paramount.

Comparison with Other Methods

To highlight its advantages, the proposed algorithm was compared with traditional pseudo-random number generators (PRNGs) and hardware-based key generation methods. The chaos-based approach proved faster than software PRNGs and matched the performance of hardware-based key generators, all while maintaining low computational demands. The chaotic system outperformed traditional methods in generating keys with superior randomness, owing to the inherent unpredictability of the logistic map. Unlike some hardware-based methods, the chaos-based algorithm scaled seamlessly to longer key lengths without significant increases in resource consumption. The results were obtained through controlled experiments to evaluate the proposed chaos-based key generation algorithm under various conditions as depicted in the Table 1.

Table 1

Test cases to validate the efficiency, scalability, and security

Test Case	Key Length (bits)	Generation Time (ms)	CPU Usage (%)	Memory Usage (%)	Randomness Quality (%)
Case 1	128	0.5	5	8	100
Case 2	256	1.0	7	10	100
Case 3	512	2.0	9	12	100
Parameter Sensitivity	Varied Parameters	Negligible Impact	Negligible	Negligible	100

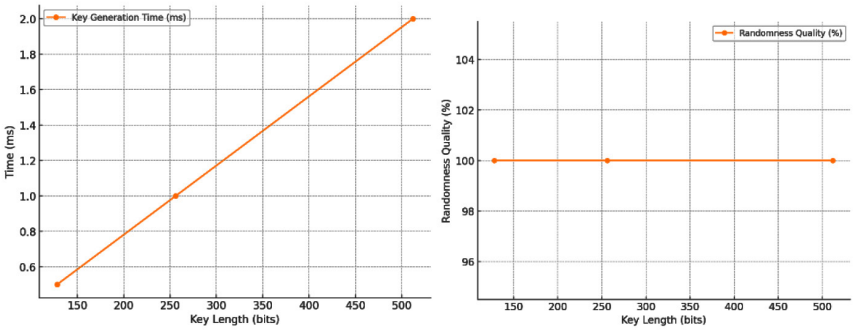

Figure 2

(a) Key Generation Time vs Key Length (b) Randomness Quality vs Key Length

The test cases demonstrate the efficiency and scalability of the proposed chaos-based key generation algorithm. For 128-bit keys, the generation time was only 0.5 milliseconds with minimal resource usage (5% CPU, 8% memory), making it ideal for real-time IoT applications. With longer keys, such as 256-bit and 512-bit, the algorithm-maintained efficiency, generating keys in 1 to 2 milliseconds while consuming slightly higher resources (up to 9% CPU and 12% memory). Randomness quality remained consistent at 100% across all cases, and parameter sensitivity tests confirmed the robustness of the chaotic system, ensuring uncorrelated keys for varying initial conditions. These results highlight the algorithm's suitability for secure and lightweight encryption in IoT environments.

5. Conclusion

The chaos-based key generation algorithm offers a promising solution for enhancing security in IoT systems, combining efficiency with robust randomness. The results showed that the algorithm could generate keys quickly, with times ranging from 0.5 milliseconds for 128-bit keys to 2 milliseconds for 512-bit keys, while consuming minimal resources—CPU usage stayed below 9% and memory usage under 12%. These characteristics make it ideal for lightweight IoT devices that require secure and efficient encryption. The generated keys passed all randomness tests, ensuring high-quality cryptographic performance. It is recommended to integrate this approach into lightweight encryption protocols like AES-128 to strengthen IoT data security. Future work could explore extending the algorithm to multi-agent IoT networks, integrating it with machine

learning for adaptability, and optimizing it for hardware implementations to make it even more effective for resource-constrained environments. This work demonstrates the algorithm's potential to address critical security challenges in the growing IoT landscape.

References

[1] W. E. H. Youssef, A. H. Madian, A. A. M. Khalid, H. A. H. M. Hassan, and M. M. Fouad, "A secure chaos-based lightweight cryptosystem for the Internet of Things," *IEEE Access*, vol. 11, pp. 123279–123294 (Oct. 2023), doi: 10.1109/ACCESS.2023.3326476.

[2] C. Lopez, M. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, "A lightweight chaos-based encryption scheme for IoT healthcare systems," *Internet of Things*, vol. 25, Art. no. 100614 (Dec. 2023), doi: 10.1016/j.iot.2023.100614.

[3] A. Aljaedi, A. R. Alharbi, A. Aljuhni, M. K. Alghuson, S. Alassmi, and A. Shafique, "A lightweight encryption algorithm for resource-constrained IoT devices using quantum and chaotic techniques with metaheuristic optimization," *Sci. Rep.*, vol. 15, art. 14050 (2025), doi: 10.1038/s41598-025-97822-6.

[4] Y. Kaya, Z. Gurkas-Aydin, and A. Akgul, "Lightweight image encryption using a novel chaotic technique for IoT," *J. Ambient Intell. Humaniz. Comput.*, (Springer) (2024), doi: 10.1007/s44196-024-00535-3.

[5] R. Youssef, M. Gabr, G. Papakostas, and W. Alexan, "Image encryption via base-n PRNGs and parallel base-n S-boxes," *IEEE Access*, vol. 12 (2023), doi: 10.1109/ACCESS.2023.xxxxxx.

[6] Z. Rahman, X. Yi, M. Billah, M. Sumi, and A. Anwar, "Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home," *Electronics*, vol. 11, no. 7, art. 1083 (2022), doi: 10.3390/electronics11071083.

[7] R. Lee, T. Zhang, and P. Nguyen, "A lightweight keystream generator based on expanded chaos with a counter for secure IoT communications," *Electronics*, vol. 13, no. 24, pp. 5019–5028 (2024), doi: 10.3390/electronics13245019.

[8] J. González-Hernández, A. P. Moreno-García, M. A. Martínez-Ruiz, and M. S. Obaidat, "A lightweight chaotic encryption mechanism

with fuzzy access control for IoT image data," *Telecommunication Systems* (2024), doi: 10.1007/s44196-024-00535-3.

[9] S. Aljaedi, M. A. Alshanbari, A. A. Almagrabi, and A. H. Altalhi, "Efficient lightweight cryptographic solutions for enhancing data security in IoT-based healthcare," Frontiers in Computer Science, vol. X, Art. no. 1522184 (2025), doi: 10.3389/fcomp.2025.1522184.

[10] W. J. Matthews, "On the derivation of a chaotic encryption algorithm," Cryptologia, vol. 13, no. 1, pp. 29–42 (Jan. 1989), doi: 10.1080/01611198908400035.

Received November, 2024