Mustansiriyah Journal of Pure and Applied Sciences, Print ISSN: 2957-9910. Online ISSN: 2957-9929, Vol. 3, No. 3, 2025, Pages 89-99
DOI: 10.47831/mjpas.v3i3.236

MJPAS

MUSTANSIRIYAH JOURNAL OF PURE AND APPLIED SCIENCES

Journal homepage*:*
https://mjpas.uomustansiriyah.edu.iq/index.php/mjpas

RESEARCH ARTICLE – COMPUTER SCIENCE

A Hybrid Lightweight Cryptographic Algorithm for Text Encryption in Web of Things

Suhaila B. Abdul Abbas [1] , Haider K. Hoomod [2]

Department of Computer Science, College of Education, Mustansiriyah University, Iraq suhailabasim1993@gmail.com , 2 Department of Computer Science, College of Education, Mustansiriyah University, Iraq drhjnew@gmail.com

Article Info.

Article history:

Received
9 June 2024

Accepted
18 July 2024

Publishing
30 June 2025

Abstract

The increasing importance of securing digital data in diverse applications requires the development of advanced encryption algorithms. This paper presents a hybrid encryption algorithm that combines the lightweight encryption algorithms Speck and PRESENT, specifically designed for limited devices in the Web of Things (WoT) environment. The proposed method is based on a chaotic key generation system to enhance security and performance. The algorithm aims for high-speed encryption, increasing complexity to protect data transmission in WoT. The hybrid model is implemented and tested in the Python programming language, focusing on textual data collected by sensors. Randomness was evaluated using the NIST statistical test suite, where the proposed method was compared to the Speck and PRESENT algorithms. The results showed superior performance in most NIST tests, indicating higher safety. In addition, the proposed algorithm showed significantly faster execution times across different file sizes compared to the individual SPECK and PRESENT algorithms.

The official journal published by the College of Education at Mustansiriya University

Keywords: Hybrid Encryption, IoT security, WOT, PRESENT, PRESENT-Speck

1. Introduction

These days, because to advancements in technology, real objects can connect to the Internet and offer their services as resources on the Web. We refer to that as the Web of Things (WoT)[1]. Within the WoT, which is a subset of the IoT, physical items are easily integrated and connected through the usage of web standards[2]. The primary objective of the Web of Things is to expand the range of methods and resources available on the Internet to include IoT network creation. By doing this, the WoT will be able to interact via the already-existing Web protocols (http, https, WebSocket, etc) without having to develop new, complicated protocols that might not help with IoT interoperability. However, privacy and security needs are crucial in order to overcome the problems posed by WoT. Data integrity, privacy, dependability, access control, and authentication inside the WoT network are some of these criteria. [2]. Managing unwanted access is regarded as a serious risk to devices connected to the Internet of Things. More emphasis was placed on the security mechanisms, including access control, identity management, confidentiality, integration, authorization, and authentication, to ensure secure WoT communication

between various devices. Authors have used tools like threat analysis and attack modeling to inform users about defensive tactics and prevent security threats from taking advantage of holes in systems. The writers have provided the necessary understanding of how different existing procedures and algorithms might be utilized to improve security)[3]To mitigate the inherent security risks, encryption emerges as a pivotal strategy to ensure the confidentiality and integrity of transmitted information. Encryption involves encrypting data in a validated format, rendering it comprehensible only to an intended recipient [4,5]. Cryptography, as the cornerstone of secure data transmission and storage, plays a pivotal role in this process. Symmetric key algorithms, characterized by efficiency and simplicity, have garnered widespread adoption, exemplified by algorithms like Present and Speck [6,7]. The Present algorithm, introduced as a lightweight cryptographic solution, focuses on efficiency and adaptability, making it particularly suitable for resource-constrained environments. Its design, featuring a substitution-permutation network (SPN), underscores its effectiveness in secure data processing [8,9]. Speck, conceived by the US National Security Agency (NSA), is renowned for its prowess in software implementations. With add-rotate-XOR (ARX) ciphering, The design of Speck places equal emphasis on computing efficiency and security. making it an exemplary choice for encryption in diverse applications [9, 10] This paper introduces a comprehensive approach to data security through encryption, leveraging the unique attributes of the Present and Speck algorithms. The synthesis of these algorithms aims to fortify the encryption process, ensuring robust protection for sensitive information in a variety of text-centric applications.

2. Related Work

In this section, the investigation centres on the examination and refinement of encryption methodologies, specifically directed towards the PRESENT and SPECK encryption algorithms. The research endeavours to enhance the encryption and decryption processes applied to text, image data through the different algorithm. Hoomod, H.K. et al[9] This study provides novel encryption methods (including hybrid encryption and two modified encryption algorithms) regulated by fuzzy rules, as well as an encryption algorithm based on the new 5-D comprehensive chaotic system. A novel five-dimensional chaotic system is integrated with the encryption mechanism through the use of the PRESENT and SPECK algorithm architecture. Additionally, the PRESENT method by SPEECK, which has been implemented in the transmission of data from IoT sensors, will employ modified circular step mechanisms for encryption. M.N. Dhuha et al. [10] This study proposes the Henon and Arnold-cat map, a hybrid key generation technique for sequences, along with an efficient picture encryption solution based on PRESENT-SPECK algorithms. The suggested technique included the picture data to the encryption block. After connecting the aggregate blocks, an encrypted image is created. Numerous types of tests have been conducted with the suggested procedure, and the generated key has passed all of them. This work is by Abdulraheem and Nema. M [11]developed a new method that compares the two approaches' performance evaluation findings, employs the 2D-chaos system in key generation, and combines it with the block cipher PRESENT to improve security and offer a high degree of encryption for data transmission in IoT devices. In their work on the lightweight modified-Provide system, Kubba and Hoomod [5]present a new 5-dimensional chaotic system. In comparison to most other systems in existence, the chaotic system that has been given is superior. Its positive Lyapunov value will introduce unpredictability and complexity into the system's behavior, making it unpredictable[12]This paper discusses lightweight cryptographic algorithms specifically designed to meet security requirements in IoT environments, where constraints on power, memory, and data processing are stringent. The focus is on developing algorithms that use minimal

resources without compromising security. [13] This research introduces the concept of using ARX (Add-Rotate-XOR) cryptographic algorithms, which are characterized by simplicity and efficiency, making them suitable for resource-constrained devices such as those used in the IoT. The paper evaluates the performance and security of these algorithms[14]This paper provides a comprehensive survey of lightweight cryptographic algorithms specifically designed for IoT devices. It compares various algorithms in terms of performance, efficiency, security level, and ease of implementation . [15]This paper addresses energy-efficient cryptographic solutions suitable for IoT devices. The focus is on developing cryptographic algorithms that consume less energy while maintaining a high level of security.[16] This paper proposes a lightweight encryption scheme tailored for networked sensors in IoT applications. The scheme is designed to provide robust security while minimizing computational overhead and power consumption, making it ideal for sensor nodes with limited resources[17] This survey reviews the state-of-the-art lightweight cryptographic algorithms developed for IoT applications. It highlights the key challenges in designing these algorithms, such as limited processing power and memory, and discusses various solutions to address these challenges.[18]This paper is an image encryption method with relatively simple structure, low cost and good encryption effect. The proposed method combines chaotic system and 3D nonlinear iterative systems for image encryption Table 1 summarizes related work

Table 1. summarizes related work

no	Reference	Findings	Research Summary
1	Hoomod, H.K. et al., [9]	Improved encryption and decryption processes for text and image data using a 5-D chaotic system to increase security and complexity..	This research presents novel encryption methods (including hybrid encryption and two modified encryption algorithms) regulated by fuzzy rules and an encryption algorithm based on a new 5-D comprehensive chaotic system. The chaotic system is integrated with the encryption mechanism through the PRESENT and SPECK algorithm architecture.
2	M.N. Dhuha et al., [10]	The generated keys passed all tests, and an encrypted image was created using the proposed technique.	This study proposes the Henon and Arnold-cat map, a hybrid key generation technique for sequences, along with an efficient image encryption solution based on PRESENT-SPECK algorithms. The technique includes the image data in the encryption block, and an encrypted image is created after connecting the aggregate blocks.
3	Abdulraheem and Nema, M [11]	Improved encryption security and provided high-level encryption using a 2D-chaos system and PRESENT block	This work develops a new method comparing the performance evaluation findings of two approaches, using a 2D-chaos system in key generation and combining it with the PRESENT block

		cipher.	cipher to improve security and offer high-level encryption for data transmission in IoT devices
4	Kubba and Hoomod [5]	Introduced a new chaotic system that increases system complexity and unpredictability, enhancing security..	This work presents a new 5-dimensional chaotic system. Compared to most other existing systems, the proposed chaotic system is superior. Its positive Lyapunov value introduces unpredictability and complexity into the system's behavior, making it unpredictable
5	S. S. Dhanda et,al., [17]	Analyzed the key challenges in designing lightweight algorithms and provided solutions to address these challenges in IoT applications.	This survey reviews the state-of-the-art lightweight cryptographic algorithms developed for IoT applications. It highlights the key challenges in designing these algorithms, such as limited processing power and memory, and discusses various solutions to address these challenges.
6	K. M. Hosny .et.al. [16]	Achieved robust security while minimizing computational overhead and power consumption, making it ideal for networked sensors.	This study proposes a lightweight encryption scheme tailored for networked sensors in IoT applications. The scheme is designed to provide robust security while minimizing computational overhead and power consumption, making it ideal for sensor nodes with limited resources.

3. Research Methods

Web of Things (WoT) encryption involves securing data communication between interconnected devices on the web. This encryption ensures that data exchanged between devices, such as sensors and controllers, is protected from unauthorized access and tampering, enhancing the overall security and integrity of the IoT ecosystem. Both the Speck and Present algorithms were merged together. This merging aims to achieve a more efficient and powerful algorithm, which enhances its ability to confront various challenges and threats.

3.1 Present algorithm

The PRESENT block The cipher is a thin cryptography method intended to offer effective and secure encryption in resource-constrained environments[19 , [20] Introduced in 2007 by Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe, PRESENT has found applications in scenarios where computational and memory

resources are limited, RFID(Radio-Frequency Identification) tags, sensor nodes , and other embedded systems[5 ,8] PRESENT [9, 10] is a 64-bit block cipher with 80- and 128-bit key lengths that is lightweight. 31 rounds make up the PRESENT block cipher, which was specified by ISO(International Organization for Standardization)/IEC(International Electrotechnical Commission) 29192-2 [21]. This cipher's add round key, substitution layer (S-box), and permutation layer are its essential parts. Lightweight block cipher families with 64–256 bits of key length and block sizes ranging from 32–128 bits are known as SIMON[10]. The National Security Agency [22] created this block cipher to offer security and flexibility in lightweight applications. With a straightforward structure, SIMON has 32 to 72 rounds, depending on the key and block sizes. It makes use of rotation operations, bit-wise AND, and bit-wise XOR. A 64-bit block cipher built on a substitution-permutation network is called LED(Lightweight Encryption Device) [11]. Its relatively basic key scheduling allows it to support any key length between 64 and 128 bits. There are 32 rounds for 64-bit keys and 48 rounds for 128-bit keys, depending on the size of the key. This encryption involves inserting constants, S-box layer, Mix-columns, and Shift-rows in each round. Algorithm 1 Pseudocode of Present block cipher [22].

Algorithm 1 Pseudocode of Present block cipher.

$generateRoundKeys()$

for i=1 i=1to 31 do

a. $addRoundKey(STATE,Ki)$

b. $sBoxLayer(STATE)$

c. $pLayer(STATE)$

d. end for.

$addRoundKey\ (STATE, K32)$

3.2 The Speck Algorithm

In June 2013, a group of academics connected to the Science Directorate of the US National Security Agency publicly unveiled the Speck algorithm[23]. The imperative driving the development of Speck was its requisite adaptability across a spectrum of constrained systems. Consequently, an intentional pursuit of simplicity in algorithmic components was undertaken to ensure versatility[24,25]. Paradoxically, This effort produced a cipher that functions well on both powerful and budget computers. Notably, Among block ciphers intended for 64-bit processing in software applications, Speck has the highest throughput. [10] The design philosophy of Speck was guided by a deliberate selection of operations within a constrained set. To foster stability through simplicity the approach is based on basic operations that represent modular addition and subtraction, including bitwise XOR, bitwise AND, left circular shift (Sj), by j bits, and right circular shift (S-j), by j bits. [23,10,22]. The National Security Agency (NSA) made Speck, a family of lightweight block ciphers, available to the public in June 2013. Noteworthy is its optimization for software implementations, while its counterpart, Simon, is tailored for hardware environments. arranged as an add-rotate-XOR (ARX) encryption , the inception of Speck was rooted in the NSA's anticipation of the need for a cipher accommodating diverse Internet of Things (IoT) devices within the ambit of the US federal government, all the while upholding a commendable level of security[10,24,25].The versatility of Speck is evident in its support for an array of block and key sizes.

The block, a constant two words, accommodates words of varying sizes: 16, 24, 32, 48, or 64 bits. Correspondingly, the key, spanning 2, 3, or 4 words, adjusts to the specified block size. Two rotations are included in Speck's round function. the process of combining the right and left words, XORing the key into the left word, and then XORing the left and right words together . The determination of the optimal number of rounds is contingent upon the specific parameters selected for the algorithm[22,25].

4. Proposed Hybrid Data Encryption

The hybrid cryptographic model here assumes a combination of the distinct binary operations of the Speck algorithm with the PRESENT algorithm. These operations are designed with the clear goal of increasing the security posture of the encryption process. Figure 1 shows the diagram of the hybrid encryption algorithm.

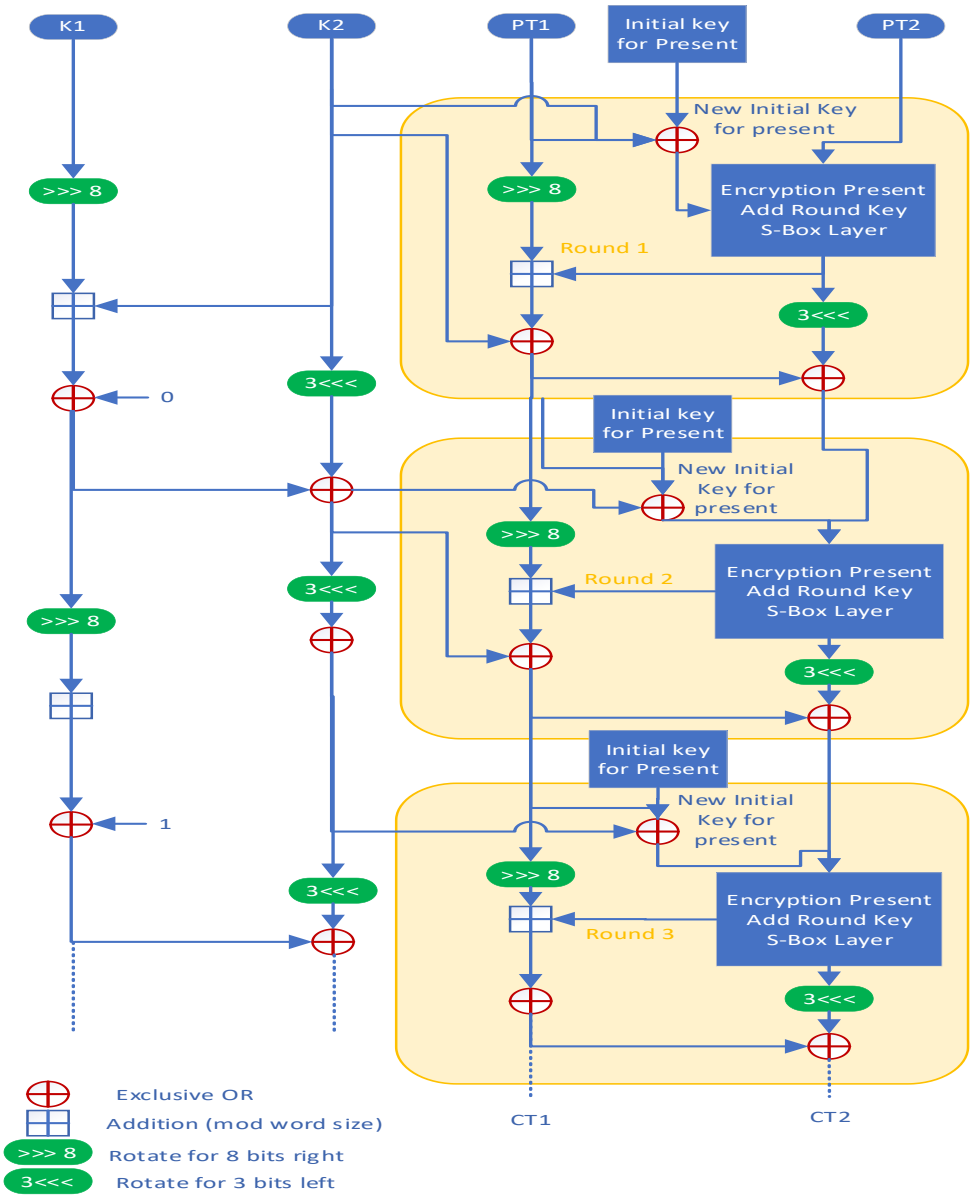

Figure. 1 Block diagram of proposed method steps.

Encryption Stage:
Input: the plain text block, chaotic system initial and parameter.
Output: Ciphered blocks.

1. Key Generation: Used logistic chaos equation to generate key sequence.
2. Key Expansion: Split the generated chaos key to generate a set of round subkeys with size(256 bits).
3. Split: Divide the plain block (128 bits) into two halves (each halve with size 64), typically referred to as the "left" and "right" halves.
4. Encryption Rounds: Iterate a specified number of rounds (20 rounds at max), applying the following operations in each round:
    a. Key Setup for Present and encrypt the right half:
        i. Input the secret encryption key, which is typically an 80-bit or 128-bit value.
        ii. The left half of the plain text is taken and an XOR operation is performed with the encryption subkey of the Speck (k2) algorithm and the master key of the Present algorithm.
        Present Key = left half XOR K2 XOR master key.
        iii. Expand the key into a set of round subkeys. This is achieved through a key scheduling process, where each round key is derived from the original key using bitwise operations.
        iv. Encrypt the right half of the plain text using the Present algorithm.
    b. Perform a bitwise rotation of the right half.
    c. XOR the right half with the left half.
    d. Apply a substitution operation to the left half.
    e. XOR the result of the substitution operation with the round subkey.
    f. Swap the left and right halves.
5. Final Round: After completing the encryption rounds, the resulting values of The encrypted text block is represented by the left and right halves.

5. The Proposed System

The proposed security method used chaotic system to generate encryption key instead the key scheduling operation and exploiting the characteristics of chaotic system and the main objectives of the proposed method is:

1. To protect the privacy of information in the WoT environment during transmission and not allow unauthorized individuals to access and exploit this information.
2. Highest speed (processing time) in the encryption and decryption.
3. To increase complexity (performance measurements).

The suggested Hybrid Encryption approach involves multiple stages, beginning with the utilization of a chaotic system to generate an extensive key. Additionally, a pseudo random key is generated by using the distinctive properties of the chaotic system. Secondly, in order to ensure confidentiality and prevent unauthorized access to information in the WoT environment during transmission, we propose the use of a hybrid encryption algorithm that offers the fastest processing time for encryption and decryption. Furthermore, the SHA3 hash function is employed to ensure both the integrity and authentication. The block diagram of the suggested encryption method is depicted in Figure 2.

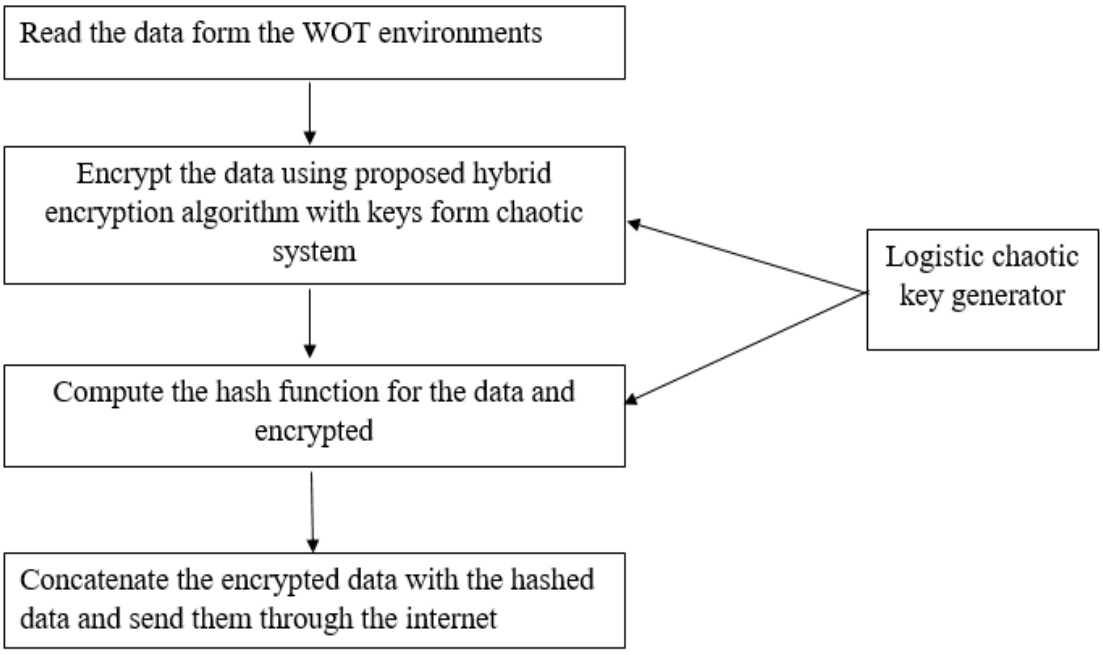

Figure. 2 The block diagram of the proposed system

6. Results and Discussions

The recommended algorithm was developed and programmed in Python. The type of data indicated for this proposed solution is text data collected by sensors. Numerous statistical tests are available for examining the randomness properties of cryptography methods. Using the well-known NIST statistical test suite, the recommended method's randomness was compared against the Speck and present encryption algorithms. Data blocks and various keys have been tried in . Table 1 shows the outcomes of the NIST statistical tests.

Table 1: statistical tests of NIST

NIST Tests	Speck	PRESENT	Proposed Algorithm
Frequency test	0.412	0.341	0.622
Block Frequency	0.256	0.477	0.690
Cumulative Sums	0.341	0.387	0.447
Runs	0.178	0.558	0.620
Longest Run	0.612	0.638	0.708
Rank	0.541	0.317	0.644
Non-Overlapping	0.374	0.001	0.410
Overlapping Template	0.311	0.055	0.419
Universal test	0.210	0.671	0.712
Approximate Entropy	0.389	0.457	0.558

Random Excursions	0.247	0.447	0.688
Random Excursions Variant	0.335	0.001	0.573
Serial test	0.546	0.333	0.627
Linear Complexity	0.318	0.175	0.337

The NIST tests determine the randomness of a specific segment of a sequence by evaluating its significance value (α), which has a default value of 0.01. Thus, a sequence would be deemed random if the P-value is less than 0.01, while if the P-value is more than 0.01 it would not be considered random. The suggested approach and the current encryption algorithm have successfully passed all NIST tests. The results for each test may be found in Table 2. The results indicate that, in the majority of the NIST tests, the P-values obtained from the suggested approach are higher than those obtained from the Speck and Present algorithms. Consequently, the suggested approach leads to a sequence that is rather uncertain. According to the data in table 2, the suggested approach balances a reduced computing speed with an elevated level of complexity.

Table 2. Execution Time comparison

File size (byte)	Speck Algorithm (sec)	PRESENT Algorithm (sec)	Proposed Algorithm (sec)
128	0.045	0.064	0.0052
1 k	0.211	0.189	0.0111
10 k	1.756	1.375	0.9472
100 k	11.145	10.418	8.8845
500 k	52.998	51.202	35.1187
1M	145.441	190.743	98.7289

7. Conclusions

This paper introduces a hybrid encryption algorithm from Speck-Present encryption lightweight algorithms. Proposed hybrid algorithm designed specifically for limited devices characterized by low power and limited resources and useful in WoT environment. The hybrid cipher has emerged as a highly popular concept in the realm of lightweight cryptography. This study introduces the hybrid lightweight cryptographic approach, which aims to safeguard sensor data from WoT/IoT devices during network transitions with strong security and high speed encryption. This technology is designed to maintain connectivity for devices connected to the Internet. Result og implementation our proposed hybrid encryption get a best security NIST tests and high encryption time operation comparing with the Speck and Present algorithms. The frequency test: The proposed algorithm achieved a success rate of 62.2%, compared to 41.2% for the Speck algorithm and 34.1% for the PRESENT algorithm. Block repetition test: The proposed algorithm achieved a success rate of 69.0%, compared to 25.6% for the Speck algorithm and 47.7% for the PRESENT algorithm. The proposed algorithm showed significantly lower execution times across different file sizes compared to the Speck and PRESENT algorithms, reflecting a balance between lower execution speed and increased complexity. Lightweight cryptographic methods are commonly used and provide greater benefits in IoT applications. The main form of communication in the

information security industry is cryptography. It is essential to have interaction between multiple devices through the internet. On the contrary, limiting devices are unable to utilize regular cryptography due to their restricted availability of resources. Constraint devices commonly employ symmetric key cryptography, a cryptographic technique that utilizes a single key for both encryption and decryption. On the contrary, rapid cryptographic methods can be employed to address limited devices.

Reference

[1] M. R. Faheem, T. Anees, and M. Hussain, "The web of things: findability taxonomy and challenges," *IEEE Access*, vol. 7, pp. 185028–185041, 2019.

[2] S. El Jaouhari, A. Bouabdallah, and J.-M. Bonnin, "Security issues of the web of things," in *Managing the web of things*, Elsevier, 2017, pp. 389–424.

[3] R. Sardar and T. Anees, "Web of things: security challenges and mechanisms," *IEEE Access*, vol. 9, pp. 31695–31711, 2021.

[4] A. A. Rashid and K. A. Hussein, "Image encryption algorithm based on the density and 6D logistic map.," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, 2023.

[5] Z. M. J. Kubba and H. K. Hoomod, "Modified PRESENT Encryption algorithm based on new 5D Chaotic system," in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 928, no. 3, p. 32023.

[6] A. T. Hashim, J. A. Mahdi, and S. H. Abdullah, "A proposed 512 bits RC6 encryption algorithm," *IJCCCE*, vol. 10, no. 1, pp. 12–25, 2010.

[7] I. Alshawi and L. Muhalhal, "Improved Salsa20 stream cipher diffusion based on random chaotic maps," *Informatica*, vol. 46, no. 7, 2022.

[8] N. Bagheri, R. Ebrahimpour, and N. Ghaedi, "New differential fault analysis on PRESENT," *EURASIP J. Adv. Signal Process.*, vol. 2013, pp. 1–10, 2013.

[9] H. K. Hoomod, J. R. Naif, and I. S. Ahmed, "Modify Speck-SHA3 (SSHA) for data integrity in WoT networking based on 4-D chaotic system," *Period. Eng. Nat. Sci.*, vol. 8, no. 4, pp. 2379–2388, 2020.

[10] D. M. Noori, H. K. Hoomod, and I. A. Yousif, "An image encryption based on hybrid PRESENT-SPECK algorithm," *Mater. Today Proc.*, vol. 80, pp. 2668–2677, 2023.

[11] A. N. Abdulraheem and B. M. Nema, "Secure iot model based on present lightweight modified and chaotic key generator," in *2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA*, 2020, pp. 12–18.

[12] M. Katagi and S. Moriai, "Lightweight cryptography for the internet of things," *sony Corp.*, vol. 2008, pp. 7–10, 2008.

[13] S. An, Y. Kim, H. Kwon, H. Seo, and S. C. Seo, "Parallel implementations of ARX-based block ciphers on graphic processing units," *Mathematics*, vol. 8, no. 11, p. 1894, 2020.

[14] A. Thakur, P. Kumar, and N. Chaurasia, "A Lightweight Trust Based Secure Authentication Mechanism for IoT Devices," 2023.

[15] I. Batra *et al.*, "Hybrid logical security framework for privacy preservation in the green internet of things," *Sustainability*, vol. 12, no. 14, p. 5542, 2020.

[16] K. M. Hosny, M. A. Zaki, N. A. Lashin, M. M. Fouda, and H. M. Hamza, "Multimedia security using encryption: A survey," *IEEE Access*, vol. 11, pp. 63027–63056, 2023.

[17] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight cryptography: a solution to secure IoT," *Wirel. Pers. Commun.*, vol. 112, no. 3, pp. 1947–1980, 2020.

[18] Y. Wanbo, Z. Qinwu, and Z. Qingjian, "chaotic image encryption method based on three-dimensional nonlinear system," *Mustansiriyah J. Pure Appl. Sci.*, vol. 1, no. 3, pp. 1–27, 2023.

[19] M. Imdad, S. N. Ramli, and H. Mahdin, "An enhanced key schedule algorithm of PRESENT-128 block cipher for random and non-random secret keys," *Symmetry (Basel).*, vol. 14, no. 3, p. 604, 2022.

[20] Z. Tang, J. Cui, H. Zhong, and M. Yu, "A random PRESENT encryption algorithm based on dynamic S-box," *Int. J. Secur. its Appl.*, vol. 10, no. 3, pp. 383–392, 2016.

[21] Z. M. J. Kubba and H. K. Hoomod, "A hybrid modified lightweight algorithm combined of two cryptography algorithms PRESENT and Salsa20 using chaotic system," in *2019 First International Conference of Computer and Applied Sciences (CAS)*, 2019, pp. 199–203.

[22] H. K. Hoomod, J. R. Naif, and I. S. Ahmed, "A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and novel 5D chaotic system," *Period. Eng. Nat. Sci.*, vol. 8, no. 4, pp. 2333–2345, 2020.

[23] R. A. F. Lustro, A. M. Sison, and R. P. Medina, "Performance analysis of enhanced SPECK algorithm," in *Proceedings of the 4th International Conference on Industrial and Business Engineering*, 2018, pp. 256–264.

[24] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "Implementation and performance of the Simon and Speck lightweight block ciphers on ASICs," *Unpubl. Work*, 2013.

[25] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK lightweight block ciphers," in *Proceedings of the 52nd annual design automation conference*, 2015, pp. 1–6.