Modified PRESENT Encryption algorithm based on new 5D Chaotic system

Zaid M. Jawad Kubba¹ and Haider K. Hoomod²
¹ College of Information Technology, University of Babylon
² Education college, Al-Mustansiriyah University
a) Zaidkubba1@gmail.com
b) Drhjnew@gmail.com

Abstract
Cryptography is a major concern in communication systems. IoE technology is a new trend of smart systems based on various constrained devices. Lightweight cryptographic algorithms are mainly solved the most security concern of constrained devices and IoE systems. On the other hand, most lightweight algorithms are suffering from the trade-off between complexity and performance. Moreover, the strength of the cryptosystems, including the speed of the algorithm and the complexity of the system against the cryptanalysis. A chaotic system is based on nonlinear dynamic equations that are sensitive to initial conditions and produce high randomness which is a good choice for cryptosystems. In this work, we proposed a new five-dimensional of a chaotic system for a lightweight cryptographic algorithm. The proposed new chaotic system considers as super chaos. The NIST suite of all 15th tests is examined the proposed algorithm and showed high randomness and complexity.

Introduction
In recent, the internet of everything (IoE) technology is broadly deployed especially for smart systems[1]. Smart systems are mainly based on constrained devices such as sensors and microcontrollers. IoE devices are delivering an enormous number of sensing data through the untrusted channel over the communication systems. Therefore, security concerns such as confidentiality and integrity are the main key to employing cryptography algorithms. There are a large number of conventional cryptographic algorithms based on symmetric and asymmetric keys that implement two different types of cryptosystems based on stream and block ciphers. In contrast, constraint devices involve limited resources thus conventional cryptosystems are not applicable for IoE systems. Therefore, lightweight cryptosystems are considered an effective solution for IoE applications. Moreover, different lightweight cryptographic algorithms are introduced for IoE applications. On the other hand, most lightweight cryptosystems suffer from the trade-off between computational cost and performance speed[2]. In literature studies, several lightweight cryptographic algorithms are considered applicable for IoE applications. PRESENT cipher considers as an ultra-lightweight cryptographic algorithm and broadly applied in IoE systems. In contrast, the PRESENT algorithm involves a simple design that makes it vulnerable to various cipher attacks and can be further considered with other Cryptography approach to enhance the security level[3].
On the other hand, chaotic systems have widely become the topic of many studies in the area of science and engineering. Various chaotic systems are introduced in different fields, and their use in different applications is becoming even wider. With the developments in technology, chaotic maps have started to be used in different fields such as communication systems, image processing, and optimization algorithms [8]. This attracted trend of using chaotic systems is based on the main property of chaos which has unpredictable and non-periodical and sensitive to initial conditions. Moreover, chaotic systems consider a suite choice for generating pseudo-random keys for cryptosystems[4]. However, some recent systems are considered chaotic whereas their maps didn't meet the main properties of chaos. Thus, in this study, a new five-dimensional of the chaotic system is introduced and the main properties of the proposed system would examine. In this study, the new chaotic system would be used to generate pseudo-random keys for a lightweight cipher algorithm.

2- Preliminaries

In this section, a lightweight algorithm is explored in detail.

2-1 PRESENT algorithm

Lightweight cipher algorithms are widely exploited in IoT devices to provide a suitable solution for keeping information secured through communication systems. PRESENT considers one of the most lightweight cryptographic algorithms which is designed to be appropriate for IoT systems. PRESENT cipher is based on the SPN structure and belongs to the family of block cipher algorithms [5]. The algorithm performs a 64-bit block and optionally can use 80- or 128-bit keys. The algorithm manipulates the plaintext through different operations of the S-box layer, P-layer, and XORed with generated Keys of 31 Rounds to produce ciphertext that XORed with last generated key at the end of the algorithm operations. Figure (1) shows the outline of the PRESENT cipher algorithm processes.

![Figure.1 Block Diagram of PRESENT Algorithm](image)

The first step of the PRESENT algorithm is generating rounds keys and implements Add Round Key (RK) for each of the 31 rounds via XOR operation into the plaintext (state). The second operation is concluded as an S-box layer which takes each four bits and XORed them with the bits of round key and the output preceding to passing it into the next operation of P-layer and then mixing the whole state into 64-bit block. The last stage of the algorithm is to XOR the 64-bit block with the update key in the last round of the algorithm to produce ciphertext. Due to the simple construction of the PRESENT algorithm which is vulnerable to different cipher attacks thus, it can be further combined with other cryptography
algorithms to enhance the security of the algorithm [3]. Hence, the PRESENT structure requires development in complexity to be more efficient to secure the data of IoE applications. In the study of a lightweight cryptosystem, the execution time and computational complexity are the main concern when designing and applying such cipher algorithms for constrained devices.

3- Methodology
3-1 The proposed new chaotic system
In this work, a new chaotic system is proposed based on five novel equations. The equations of the proposed system are presented as follow:

\[
\begin{align*}
    x &= x + (-s \cdot x + y \cdot k - r \cdot p) \\
    y &= y + (-y - x \cdot z + r \cdot x - u \cdot p) \\
    z &= z + (z \cdot x \cdot y - 1.5 \cdot s \cdot p - k) \\
    k &= k + (s \cdot x + (u \cdot y - r \cdot k)) \\
    p &= p + (b \cdot ((x + k) / z) + y)
\end{align*}
\]

where \(x, y, z, k,\) and \(p\) are the vectors that represent the behavior of the system. The behavior shows chaotic system for \(s = 0.95, r = 0.5, b = 0.01, u = 1.1\). The attractors of the chaotic system are plotted on a plane as shown in figure1. The significance of the proposed system is that it produces a new 4D chaotic system that is more complex and sensitive to initial conditions.

3-2 The modified PRESENT algorithm based on new 5D Chaotic
In this section, a lightweight PRESENT cipher algorithm is modified based on the proposed new chaotic system. The new chaotic system is used for generating pseudorandom keys to improve complexity and randomness. The proposed algorithm is modified based on five-dimensional equations of a chaotic system. The new trend of using a novel chaotic system with the developed lightweight algorithm is suggested to enhance the complexity and preserve the high performance. The diagram of the proposed algorithm is shown in Figure (2).

![Diagram of the proposed algorithm](image)
3-3-1 Encryption Process

Encryption is the process of converting the plaintext into a cryptograph form to secure data transmission through the network channels. This operation forbids unauthenticated persons to access and modified the original text transmitted by the sender through the network. The encryption operation of the modified algorithm is depicted as follows.

Algorithm 1. Encryption Algorithm

INPUT:
Plaintext

OUTPUT:
Ciphertext

Step
1. Generate Chaotic Keys ()
2. for i = 1 to 31 do
3. Padding (STATE, Key)
4. add Round Key (STATE, Ki)
5. S-box Layer (STATE)
6. P-Layer (STATE)
7. end for
8. The update adds chaotic Key (state, K32)
9. end

Firstly, the input message of size 64 bits is padding into 128 bits using the first chaotic key. The generated state of 128 bits then split into two block sizes of 64-bit and each block will be processed through the next functions. Then, the plaintext is encrypted via XORed operation through the add round key. Then S-box operation is applied to substitute each block of 64-bit size using the binary sequence of the state based on the PRESENT S-box table. In the next operation, the P-layer is processed based on the permutation table of the PRESENT algorithm[6]. In the entire operation for the above opera, there was a loop of 31 rounds until the last stage. In the last operation, a new chaotic key is XORed with the last rounds of the state to produce the ciphertext.

3-3-2 Decryption Process

Decryption considers as the operation of translating the ciphertext into the original plaintext, which is received by the end-user. It is the inverse operations of the encryption process, in which it uses the inverse operations, such as S-box and P-layer operations. The decryption operations of the modified algorithm are described as follows.

Algorithm 2. Decryption Algorithm

INPUT:
Ciphertext

OUTPUT:
Plaintext

Step
1. Generate Chaotic Keys ()
2. XOR (STATE, Key32)
3. for i = 1 to 31 do
4. XOR (STATE, Ki)
5. Inverse S-box Layer (STATE)
6. Inverse P-Layer (STATE)
Firstly, a new chaotic key is generated and XORed with the received ciphertext. Then, the new state of ciphertext is decrypted via XOR operation through chaotic round keys. The next layer is the inverse S-box technique used to substitute the block of cipher block of 64-bit size using the binary sequence based on the PRESENT inverse S-box table. The next operation of the inverse P-layer is processed based on the inverse permutation table of the PRESENT algorithm[6]. The entire operations for the above layers, there are 31 rounds of chaotic keys until the last stage. The last operation is unpadded to the last state to produce the plaintext.

4- Results and Security Analysis of modified algorithm based on Chaotic Implementation

This section examines the behavior and properties of the new chaotic system and shows the security analysis of the modified PRESENT lightweight cipher algorithm. The results experimented on PC-Intel using Core i7 processor and executing in PyCharm environment which encoded by python programming language. The execution time is calculated by using a text file of size 28 kb for both PRESENT cipher and modified algorithm. The execution time of the PRESENT cipher was 42.45923 seconds for the encryption process while the modified algorithm was 1.89193 seconds for the encryption process. Thus, the modified algorithm is suitable for IoE applications that operate low execution time than the PRESENT algorithm.

4-1 Lyapunov exponent

The Lyapunov exponent is a metric of sensitive dependence on initial states. It is the main approach to examine if a dynamic system behaves during time as a chaotic scheme by calculating the largest number of Lyapunov exponents. A Lyapunov exponent can be defined as a number that illustrates the dynamic movement of trajectory evolution. It examines the rate of convergence or divergence of two adjacent trajectories in the phase domain[7]. The exponential separation of trajectories as follows:

\[ \ln \| \delta z(t) \| \approx \ln \| \delta z(0) \| e^{\lambda t} \]  \hspace{1cm} (4.1)\]

where \( \lambda \) is the average rate of the trajectories separation, \( \delta z(0) \) is the preliminary separation, and \( \delta z(t) \) is the separation after time \( t \). The Lyapunov exponent for certain trajectories can be negative, zero, or positive value. The negative value refer that the two trajectories attract closer to one another. A positive value means that the two trajectories divergence from one another and appear only within the chaotic domain. Hence, a positive Lyapunov exponent considers one of the most significant indicators of chaos. Recently Lyapunov exponent commonly calculates by using the variational methods. A positive value of Lyapunov exponent computes sensitive dependence on initial points by showing the mean at which two close points separate with time[8]. In recent studies, they consider the multi-dimension of dynamic systems that result in at least one positive Lyapunov exponent is considered as chaos. In this work, the new five-dimensional system results with five positive Lyapunov exponents which are 0.0199, 0.017, 1.496, 0.015, and 0.016 as the order of the system maps. Figure (3) shows the five positive Lyapunov exponents of the new chaotic maps. Thus, the proposed new chaotic system is considered a super chaotic system, and all its Lyapunov exponents are positives.
4-2 Chaotic properties
The new five chaotic maps demonstrate the main property of chaos theory which is the sensitive dependence on initial seeds. This property refers to the slight difference between the two pairs of initial conditions. Which initially begin as adjacent together as desired, then eventually change apart. Table 1 shows the maxim value of five maps that reached for two separate orbits whose begin with conditions differ by .0001.

| Chaotic Maps | Max. value of the First orbit | Max. value of the Second orbit |
|--------------|-------------------------------|-------------------------------|
| Eq1          | 0.07595                       | 0.10024                       |
| Eq2          | 0.20251                       | 0.26802                       |
| Eq3          | 0.27836                       | 0.34676                       |
| Eq4          | 0.26492                       | 0.35985                       |
| Eq5          | 0.06485                       | 0.08287                       |

4-3 NIST Suite
There are various tests are used for examining the randomness and statistical properties of cryptography algorithms [9]. The NIST Suite consider as realistic tests that have been used for measuring the randomness of cryptosystems. Thus, in this study NIST tests are implemented as a metric for comparing the randomness of the modified algorithm based new chaotic system with the PRESENT algorithm. NIST tests have experimented with $10^6$ bits that were obtained from converting the ciphertext file of both algorithms PRESENT and the proposed algorithm for a specific period. Table 1 demonstrates the results of the 15f tests of the NIST suite. The highest value $(P)$ designated that the sequence of bits is random or
otherwise is not random, the default value of $p$ is (0.01). If $P$-value $\geq 0.01$, then, the sequence of bits is considered random. In contrast, if $P$-value $< 0.01$, it indicates that the sequence of bits is non-random. Thus, as shown in table 1 the developed algorithms had passed all of the 15$^{th}$ tests of NIST which indicate that the proposed algorithm is secure and applicable for cryptosystems. Moreover, the $P$-values of NIST tests for the proposed algorithm is higher than the result of $P$-values for the PRESENT algorithm. Therefore, the sequence of bits generated by the proposed algorithm has the highest level of randomness.

| NIST Tests            | PRESENT  | Proposed algorithm |
|-----------------------|----------|--------------------|
| Frequency             | 0.28229  | 0.52708            |
| Block Frequency       | 0.012400 | 0.55441            |
| Cumulative Sums       | 0.470681 | 0.4729459          |
| Runs                  | 0.731362 | 0.621650           |
| Longest Run           | 0.231373 | 0.418841           |
| Rank                  | 0.28878  | 0.8624572          |
| FFT                   | 0.000708 | 0.258568           |
| Non-Overlapping       | 0.82787  | 0.80991            |
| Overlapping Template  | 0.008551 | 0.15140            |
| Universal             | 0.5280793| 0.55039            |
| Approximate Entropy   | 0.02096  | 0.93537            |
| Random Excursions     | 0.10079  | 0.501099           |
| Random Excursions     | 0.039591 | 0.643429           |
| Serial                | 0.040977 | 0.208385           |
| Linear Complexity     | 0.919688 | 0.808833           |

5- Conclusion
In this paper, a new five-dimensional chaotic system is introduced for a modified PRESENT lightweight cryptographic algorithm. The new chaotic system is superior to most of the current systems that all the five maps are examined positive values of Lyapunov exponents. This property presents more randomness and complexity to make the system behavior unpredictable. Thus, such a system is more applicable to cryptosystems to produce pseudorandom keys that are difficult to analyze. Also, conventional cartography algorithms do not apply to constrained devices. In contrast, lightweight cryptographic algorithms are more applicable and applied widely with IoE applications. Moreover, lightweight cryptography suffers from a tradeoff between complexity and performance. Thus, in this work, we suggested a modified lightweight cryptographic algorithm based on the new five-dimensional of the chaotic system presented in this study.

References
1. Kubba, Z.M.J. and H.K. Hoomod. *The Internet of Everything Based Smart Systems: Applications and Challenges*. in *2019 1st AL-Noor International Conference for Science and Technology (NICST)*. 2019. IEEE.

2. Usman, M., et al., *SIT: a lightweight encryption algorithm for secure internet of things*. arXiv preprint arXiv:1704.08688, 2017.

3. Azari, H.D. and P.V. Joshi, *An efficient implementation of present cipher model with 80 bit and 128 bit key over fpga based hardware architecture*. International Journal of Pure and Applied Mathematics, 2018. 119(14): p. 1825-1832.

4. Kubba, Z.M.J. 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. IEEE.

5. Gómez, E.J., F.M. Sarmiento, and H.M. Ariza, *Functional Comparison of the Present Algorithm on Hardware and Software Embedded Platforms*. 2017.

6. Bogdanov, A., et al. *PRESENT: An ultra-lightweight block cipher*. in *International Workshop on Cryptographic Hardware and Embedded Systems*. 2007. Springer.

7. Vallejo, J.C., M.A. Sanjuan, and M.A. Sanjuán, *Predictability of Chaotic Dynamics*. 2017: Springer.

8. Rosenstein, M.T., J.J. Collins, and C.J. De Luca, *A practical method for calculating largest Lyapunov exponents from small data sets*. Physica D: Nonlinear Phenomena, 1993. 65(1-2): p. 117-134.

9. Hao, L. and L. Min, *Statistical tests and chaotic synchronization based pseudorandom number generator for string bit sequences with application to image encryption*. The European Physical Journal Special Topics, 2014. 223(8): p. 1679-1697.