Al-Kitab Journal for Pure Sciences (2023); 7(1):48-56.

https://doi.org/10.32441/kjps.07.01.p5

Al-Kitab Journal for Pure Sciences
ISSN: 2617-1260 (print), 2617-8141(online)
www.kjps.isnra.org

Generation S-box and P-layer For PRESENT Algorithm Based On 6D Hyper Chaotic System

Mohammed D. Taha *, **Khalid A. Hussein**
Computer Sciences Dept. College of Education, Mustansiriyah University, Baghdad, Iraq

*Corresponding Author: muhammed84@uomustansiriyah.edu.iq

Citation: Taha MD, Hussein KA. Generation S-box and P-layer For PRESENT Algorithm Based On 6D Hyper Chaotic System. Al-Kitab J. Pure Sci. [Internet]. 2023 Jul. 30 [cited 2023 Jul. 30];7(1):48-56. Available from: https://isnra.net/index.php/kjps/article/view/925 https://doi.org/10.32441/kjps.07.01.p5.

Keywords: S-Box, P-Layer, random generation,6D 6D Chaotic System, PRESE Block cipher.

Article History

Received	29 Apr. 2023
Accepted	23 July. 2023
Available online	30 July. 2023

Abstract:

In the era of data-driven applications and resource-constrained devices, the need for lightweight algorithms has become increasingly important. Lightweight algorithms refer to computational techniques that strike a balance between efficiency and resource utilization, making them well-suited for low-power devices, embedded systems, and scenarios with limited computational capabilities. For the new encryption method PRESENT, which was put forth in 2007, S-box directly affects the algorithm's security, whereas the p-layer mostly functions as a confusing factor during the encryption process. This paper provides a brief explanation of the PRESENT algorithm's operation and suggests an enhanced S-box and p-layer to address the issue that the main PRESENT S-box and P-layer have an anti-fixed point. The random generate of S-boxes and P-layers for PRESENT algorithms using 6D chaotic systems to generate 10 new S-boxes and 10 new P-layers. Finally, the security analysis has been completed, and the results indicate that the chaos S-box and P-layer are better able to with stand differential attacks and linear assaults and are suitable for protecting sensitive data.

Keywords: S-Box, P-Layer, random generation, 6D Chaotic System, PRESENT, Block cipher.

التوليد العشوائي S-BOX و P-LAYER لخوارزميات PRESENT باستخدام أنظمة فوضوية D6 لتوليد عشرة S-BOX جديدة و عشرة P-LAYERS جديدة

محمد ضياء الدين طه* & خالد علي حسين

قسم علوم الحاسبات. كلية التربية ، الجامعة المستنصرية ، بغداد ، العراق

muhammed84@uomustansiriyah.edu.iq

في عصر التطبيقات القائمة على البيانات والأجهزة ذات الموارد المحدودة، أصبحت الحاجة إلى خوارزميات خفيفة الوزن ذات أهمية متزايدة. تشير الخوارزميات خفيفة الوزن إلى التقنيات الحسابية التي تحقق التوازن بين الكفاءة واستخدام الموارد، مما يجعلها مناسبة تمامًا للأجهزة منخفضة الطاقة والأنظمة المضمنة والسيناريوهات ذات القدرات الحسابية المحدودة. بالنسبة لطريقة التشفير الجديدة PRESENT، والتي تم طرحها في عام ٢٠٠٧، يؤثر S-BOX بشكل مباشر على أمان الخوارزمية، بينما تعمل P-LAYER في الغالب كعامل مربك أثناء عملية التشفيرK تقدم هذه الورقة شرحًا موجزًا لعملية خوارزمية PRESENT وتقترح وجود S-BOX وP-LAYER محسّنًا لمعالجة المشكلة المتمثلة في أن PRESENT S-BOX يحتوي على نقطة مقاومة ثابتة. التوليد العشوائي S-BOX وP-LAYER لخوارزميات PRESENT باستخدام أنظمة فوضوية D٦ لتوليد عشرة S-BOX جديدة وعشرة P-LAYERS جديدة. أخيرًا تم الانتهاء من تحليل الأمان، وتشير النتائج إلى أن الفوضى S-BOX وP-LAYER أكثر قدرة على تحمل الهجوم التفاضلي والاعتداء الخطي ومناسبان لحماية البيانات الحساسة.

الكلمات المفتاحية: S-BOX، P-LAYER، التوليد العشوائي ، نظام الفوضى D6، خوارزميات التشفير PRESENT.

1. INTRODUCTION:

The Internet of Things (IoT) is a transformative force that connects interconnected physical objects, enabling seamless communication and data exchange [1]. Encryption is crucial for data security and privacy in IoT ecosystems [2], [3]. Lightweight block ciphers are popular for securing IoT devices and communications, as they are computationally efficient and require minimal hardware and memory resources [4], [5]. These ciphers strike a balance between security and efficiency, using techniques like substitution-permutation networks, bitwise operations, and compact key schedules [4], [6]. Cryptography and secure communication techniques ensure the confidentiality and integrity of sensitive information [7], [8]. One such technique is substitution-permutation (SP) networks, which consist of two components: S-boxes and P-layers[7]. S-boxes introduce nonlinearity into the encryption process, making it more resistant to cryptanalysis techniques [9], [10]. P-layers, also known as permutation layers, enhance the diffusion of information throughout the encryption process, achieving higher security and resistance against attacks [11], [12]. The

hybridization of lightweight systems and chaotic dynamics aims to leverage the strengths of both approaches [13], [14]. By combining lightweight algorithms with chaotic behavior, it becomes possible to achieve enhanced security, robustness, and efficiency in resource-constrained environments [13], [15]. This integration allows for the development of novel encryption schemes, data-hiding techniques, and optimization algorithms that can withstand cryptographic attacks, adapt to changing environments, and operate effectively with limited resources [13], [15].

The 6D-chotic system [16].Combines chaos theory with substitution and permutation principles, employing S-boxes and P-layers in a unique way [17], [18]. This approach offers advantages in security, efficiency, and resistance to attacks, enhancing the robustness and effectiveness of encryption techniques and protecting sensitive data in various applications [13].

2. Research Methods:

A. Chaotic System

Chaos, is sometimes known as the "butterfly effect [16].Is a phenomenon that results from the complex, aperiodic behavior of deterministic systems that exhibits remarkable sensitivity to minute changes in initial conditions [15].In the framework of Shannon's confusion and diffusion principles, this characteristic of chaos has been used in cryptography [13]. Chaotic events have demonstrated potential as a source of pseudo randomness in information security by utilizing their mixing property and great sensitivity to tiny fluctuations [2], [13], [17]. Due to their deterministic character, chaotic maps—nonlinear dynamical systems that display chaotic behavior—have proven to be especially helpful in the field of cryptography. Numerous cryptographic applications, such as picture encryption methods, and block and stream ciphers, have been made more secure by researchers using these chaotic system properties [2], [4]. Hyper chaotic behavior can be seen in the six-dimensional hyper chaotic system. It can be formulated mathematically as Eq. (1) [16].

$$\begin{aligned} \dot{x} &= -ax + by + cw - dv \\ \dot{y} &= ex - fxz - ge^{v} \\ \dot{z} &= -hz + xy + iv \\ \dot{w} &= -w - yz - gv \\ \dot{v} &= x + jy - iz \end{aligned} \qquad (1)$$

$$\dot{u} = kx - Lu - jzw$$

The system outlined in Eq. (1) has seven states, including x, y, z, w, v, u, and t R, and exhibits hyper chaotic behavior. The constants for the following parameters are all positive: a, b, c, d, e, f, g, h, i, j, k, and l **[16].**

B. PRESENT Algorithm:

Is a simple block cipher developed for restricted settings, such sensor networks and RFID tags. It supports key sizes of 80 or 128 bits and works with 64-bit blocks of data. In order to achieve non-linearity, PRESENT employs an S-box and a substitution-permutation network (SPN) topology **[4]**.

In **Table 1**, a lookup table called the PRESENT S-box is displayed. It accepts a 4-bit input and generates a 4-bit output **[19]**.

Table 1: PRESENT algorithm of the S-box table

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

In PRESENT algorithm, the P-layer (Permutation layer) is a diffusion operation that operates on the output of the S-box substitution. It is a simple transposition layer that reorders the bits within a 64-bit block is shown in **Table 2 [4],[19]**.

Table 2: PRESENT algorithm of the Player substitution table

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
p(i)	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
p(i)	4	20	36	52	5	21	37	53	6	22	38	54	11	27	43	59
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
p(i)	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
p(i)	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

3. Proposed Method:

The suggested encryption method uses a hybrid technique to safely encrypt a variety of data types, including photos, text, documents, and videos. The proposed scheme constructs 10 new S-boxes and 10 new P-layers to enhance the security of the encryption process. The input initial state parameters x, y, z, w, v, u, t R, a, b, c, d, e, f, g, h, i, j, k, and l, as given in Eq. (1), are used to produce the S-boxes and P-layer. Calculations and hexadecimal code conversions are performed on the values of xi, yi, zi, wi, vi, and ui. For each number, the first five digits, ranging from 7 to 11, are extracted, and duplicates are checked and eliminated. The resulting cipher text is highly secure and suitable for protecting sensitive data. Show in **Figure 1**.

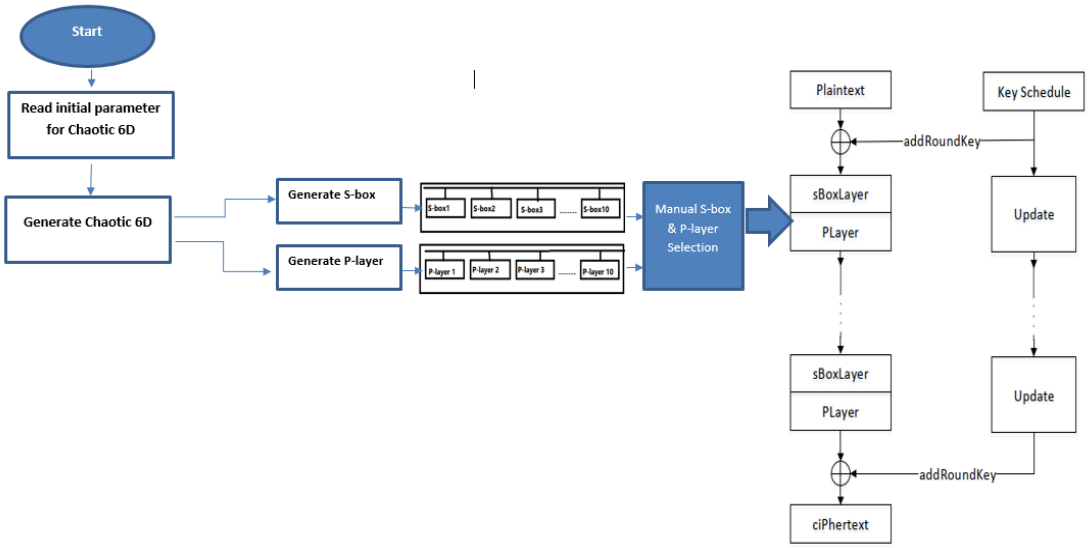

Figure 1: Random Generate S-box and P-layer For PRESENT Algorithm Based on Chaotic 6D

Algorithm 1 :S-Box Generation:

Input: SBox=[0xc,0x5,0x6,0xb,0x9,0x0,0xa,0xd,0x3,0xe,0xf,0x8,0x4,0x7,0x1,0x2],

Initial parameter for Chaotic 6D: a = 18, b = 16, c = 0.5, d = 5.3, e = 32, f = 9, g = 5,

h = 2, i = 4.1, j = 3, k = 12, l = 4

Output: generate Ten S-box

1-Start

2-Read parameters x, y, z, w, v, u, and dt R, as well as Eq. (1)

3-Generate Chaotic 6D

4-index=0,

5- **While(index<10)**

6- i=0 , SBoxv =[]

7- While (i <16)

8- The xi, yi, zi, wi, vi, and ui numbers are computed and translated to hexadecimal form. For each number, the first five digits (7 to 11) are retrieved, and any duplicates are verified for and eliminated.

9- If (S[i] contents in SBox [])

a-Yes, i=i+1 , if(i<6) , yes-move to step 9, no- move to step 3

b. **No**, SBoxv[index]=S[i], index=index +1,

10- End.

Algorithm 2 :P-layer Generation:-

Input: PBox = [0,16,32,48,1,17,33,49,2,18,34,50,3,19,35,51,

4,20,36,52,5,21,37,53,6,22,38,54,7,23,39,55,

8,24,40,56,9,25,41,57,10,26,42,58,11,27,43,59,

12,28,44,60,13,29,45,61,14,30,46,62,15,31,47,63]

Initial parameter for Chaotic 6D: a = 18, b = 16, c = 0.5, d = 5.3, e = 32, f = 9, g = 5

h = 2, i = 4.1, j = 3, k = 12, l = 4

Output: generate Ten P-Layer

1-Start

2-Read parameters x, y, z, w, v, u, and dt R, as well as Eq. (1)

3-Generate Chaotic 6D

4-index=0,

5- **While(index<10)**

6- i=0 , PBoxv =[]

7- While (i <64)

8- The xi, yi, zi, wi, vi, and ui numbers are computed and translated to hexadecimal form. For each number, the first five digits (11 to 15) are retrieved, and any duplicates are verified for and eliminated.

9- If (S[i] contents in PBox [])

a-Yes, i=i+1 , if(i<6) , yes-move to step 9, no- move to step 3

b. **No**, PBoxv [index]=S[i], index=index +1,

10- End.

4. Results and Calculations:

On a machine running 64-bit Windows 10 Home with an Intel Core i5-6300U processor clocked at 2.40 GHz to 2.50 GHz, 8 GB of RAM, and the Python programming language, the proposed solution was experimentally tested. the proposed solution was experimentally tested to generate 10 new S-box and inverse S-box in **Figure 2**,and to generate 10 new P-layer and inverse P-layer respectively as shown in **Figure 3**, **4**, and **Figure 5**.

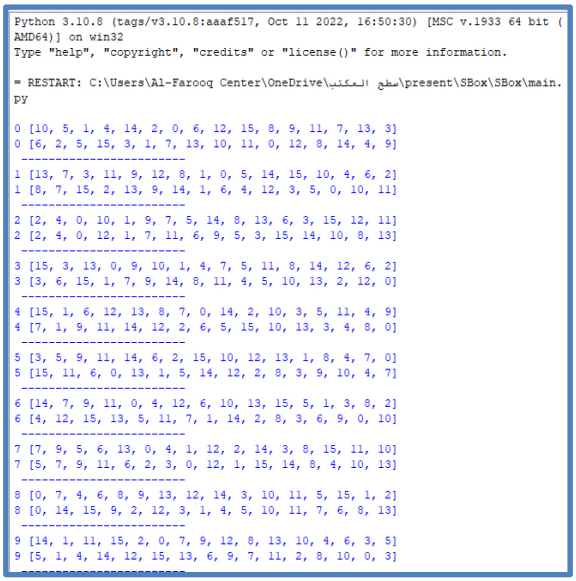

Figure 2: Radom generation S-box and inverse

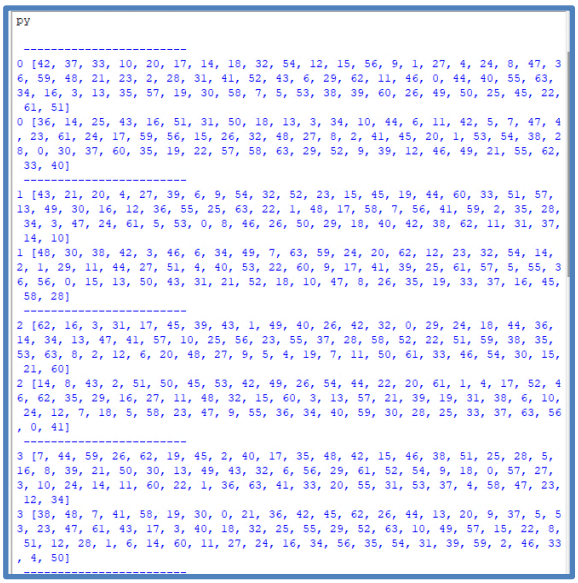

Figure 3: Radom generation P-layer and inverse

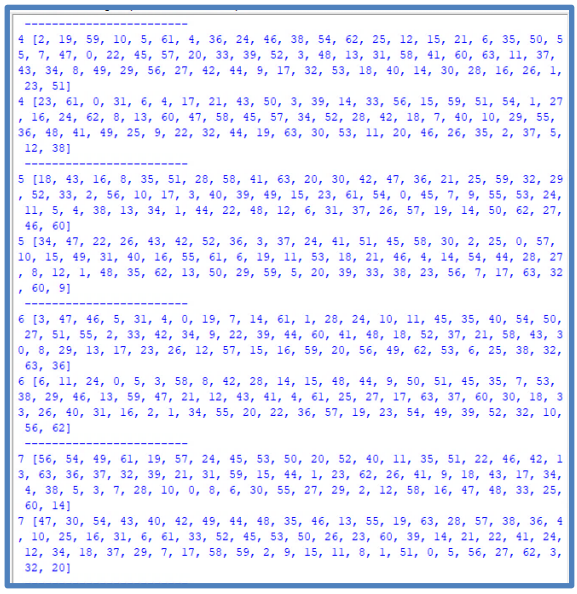

Figure 4: Result 3; Radom generation P-layer and inverse

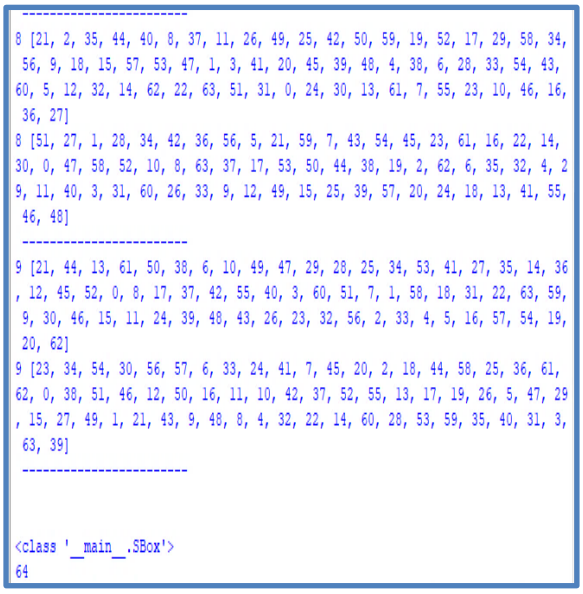

Figure 5: Result 4; Radom generation P-layer and inverse

5. Conclusion

The random generation of an S-box and a P-layer is a common technique used in cryptography to enhance the security of symmetric key algorithms. The main PRESENT S-box and P-layer have an anti-fixed point, which is resolved by the random generation of S-boxes and P-layers for PRESENT algorithms using a 6D chaotic system; the algorithm's resistance to differential and linear assault has been well established. we introduce additional unpredictability and confusion into the encryption process. This randomness makes it more difficult for an attacker to analyze and exploit patterns in the data. It enhances the resistance against various cryptographic attacks, such as differential cryptanalysis and linear cryptanalysis. It increases complexity and makes it more challenging for attackers to decrypt encrypted data.

6. Reference:

[1] Naru ER, Saini H, Sharma M. A recent review on lightweight cryptography in IoT. Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017. 2017. p. 887-90. doi: 10.1109/I-SMAC.2017.8058307.

[2] Rashid AA, Hussein KA. Image encryption algorithm based on the density and 6D logistic map. Int J Electr Comput Eng. 2023;13(2):1903-13. doi: 10.11591/ijece.v13i2.pp1903-1913.

[3] Jasim OA, Hussein KA. Parallel key generation based on nonlinear feedback shift registers and hyper chaotic system. 2021. p. 1-8.

[4] Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, et al. PRESENT: An ultra-lightweight block cipher. 2007. p. 450-66.

[5] Said G, Shahab M, Ali M, Ahmed A, Aijaz A, Khan M. Lightweight secure aggregated data sharing in IoT-enabled wireless sensor networks. IEEE Access. 2022;10:33571-85. doi: 10.1109/ACCESS.2022.3160231.

[6] Santos JC. Choosing the future of lightweight encryption algorithms. 2018. p. 124.

[7] Wang H, Zheng H, Hu B, Tang H. Improved lightweight encryption algorithm based on optimized S-box. Proceedings - 2013 International Conference on Computational and Information Sciences, ICCIS 2013. 2013. p. 734-7. doi: 10.1109/ICCIS.2013.198.

[8] Rashid AA, Hussein KA. A parallel programming for robust chaotic map generation based on two and dimensional equation system. J Eng Appl Sci. 2019;14(11):3741-5.

[9] Jasim OA, Hussein KA. A hyper-chaotic system and adaptive substitution box (S-Box) for image encryption. 2021 International Conference on Advanced Computer Applications (ACA), Maysan, Iraq, 2021. p. 144-9. doi: 10.1109/ACA52198.2021.9626793.

[10] Taher HM, Abd Al-Rahman SQ, Shawkat SA. Best S-box amongst differently sized S-boxes based on the avalanche effect in the advance encryption standard algorithm. Int J Electr Comput Eng. 2022;12(6):6535-44. doi: 10.11591/ijece.v12i6.pp6535-6544.

[11] Kubba ZM, Hoomod HK. Modified PRESENT encryption algorithm based on new 5D chaotic system. IOP Conf Ser Mater Sci Eng. 2020;928(3). doi: 10.1088/1757-899X/928/3/032023.

[12] Hussein KA, Mahmood SA, Abbass MA. A new permutation-substitution scheme based on Henon chaotic map for image encryption. 2019 2nd Sci Conf Comput Sci. 2019. p. 63-8.

[13] Hoomod HK, Naif JR, Ahmed IS. A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and novel 5D chaotic system. Period Eng Nat Sci. 2020;8(4):2333-45. doi: 10.21533/pen.v8i4.1738.

[14] Mohammed AH, Shibeeb AK, Ahmed MH. Image cryptosystem for IoT devices using 2-D Zaslavsky chaotic map. Int J Intell Eng Syst. 2022;15(2):543-53. doi: 10.22266/ijies2022.0430.48.

[15] Zhou S, Tang Y, Liu Y, Wang X, Zhou X. Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box. Nonlinear Dyn. 2023. doi: 10.1007/s11071-023-08312-1.

[16] Mehdi SA, Ali ZL. A new six-dimensional hyper-chaotic system. 2019 Int Eng Conf. 2021. p. 211-5.

[17] Salman RS, Farhan AK, Shakir A. Creation of S-box based one-dimensional chaotic logistic map: Colour image encryption approach. Int J Intell Eng Syst. 2022;15(5):378-89. doi: 10.22266/ijies2022.1031.33.

[18] Mahmood SA, Hussein KA, Jurn YN, Albahrani EA. Parallelizable cipher of color image based on two-dimensional chaotic system. Indones J Electr Eng Comput Sci. 2019;18(1):101-11. doi: 10.11591/ijeecs.v18.i1.pp101-111.

[19] Tang Z, Liu X, Liu J, Sun X, Xu G. A random PRESENT encryption algorithm based on dynamic S-box. Int J Secur Its Appl. 2016;10(3):383-92. doi: 10.14257/ijsia.2016.10.3.33.