All Sciences Proceedings

1st International Conference on Recent Academic Studies

May 2-4, 2023 : Konya, Turkey

ICRAS

All Sciences Proceedings
http://as-proceeding.com/

https://as-proceeding.com/index.php/icras

Comparison of Nonlinearity Value of Substitution Box Generation Approaches

Fırat Artuğer*, Songül Karakuş [2] and Fatih Özkaynak [3]

[1] Department of Computer Engineering / Faculty of Engineering, Munzur University, Turkey
[2] Department of Computer Engineering / Faculty of Engineering and Architecture, Bitlis Eren University, Turkey
[3] Department of Software Engineering / Faculty of Technology, Fırat University, Turkey

*(firatartuger@munzur.edu.tr)

Abstract **–** Substitution box (s-box) is one of the important structures that perform the mixing process for encryption algorithms. Therefore, strong s-box structures are needed to develop effective encryption algorithms. The most important feature of the S-box is that it has a nonlinear structure. In this way, it can effectively scramble the data to be encrypted. More than a hundred new algorithms have been proposed using many approaches to obtain s-box structures with high nonlinearity. In this study, the performances of the s-box generation approaches in recent years were compared according to their non-linearity values. In addition, the advantages and disadvantages of these approaches have been discussed and suggestions have been made especially for researchers who will just start in this field.

Keywords – S-Box, Nonlinearity, Chaos, Optimization, Mathematical Transformation

I. INTRODUCTION

With the rapid development of science, the amount of data is increasing day by day. Ensuring security in both the storage and communication of this data is of vital importance [1]. In particular, sensitive data needs to be effectively protected. At this point, we come across the science of cryptology. Cryptology is the science of encryption and consists of two parts. The first of these is cryptography. Cryptography is the process of developing protocols or algorithms for encrypting data. Another part is the science of password cracking called cryptanalysis. Cryptoanalysis is needed. Because the only way to know that an encryption algorithm is secure is to try to crack it. Many cryptoanalysis methods are available to crack encryption algorithms. If the developed algorithm cannot be broken despite the cryptanalysis, then it is safe. The data encryption standard used today is the AES algorithm [2]. AES is a block cipher algorithm. It first divides the data into blocks of equal length, then encrypts each block within itself and combines the encrypted blocks to obtain the encrypted data. Considering the operation of this algorithm, one of the most important structures that meet the mixing requirement is the s-box. In AES, the s-box is used both in the process of encrypting data and in the generation of subkeys. Therefore, strong s-box structures are always needed to develop strong encryption algorithms.

S-box represents a transformation. It increases the complexity of the algorithm by replacing the raw value with another value. AES uses an 8-bit s-box containing 256 values. When we look at the literature, it is seen that such s-box structures are generally tried to be developed. More than 100 s-box generation algorithms have been proposed using many approaches from the past to the present. Among these approaches, the most; mathematical transformations [3-8], chaotic systems [9-14] and optimization techniques [15-22] are used. In addition, hybrid approaches have been developed [23-25] by combining DNA coding, cellular automata, and the benefits of existing approaches.

In this study, first of all, the s-box structure was explained, and then a performance comparison was made according to the nonlinearity values of the s-box structures obtained as a result of the studies carried out in recent years. The reason for using the nonlinearity value here is that it is the most important criterion desired in an s-box. Since the S-box replaces one value with another value, it should not have a linear structure. The more non-linear the more effective it will be. When we look at the literature, it is seen that most studies try to improve the nonlinearity value.

II. S-BOX STRUCTURES

S-box is a process in which one value is replaced by another value in data divided into blocks. In the AES algorithm, there is an s-box structure with the size of 16 * 16 and it is given in figure 1. Hundreds of studies in the literature have developed new methods to produce such an s-box structure. This topic is still a hot topic. Because optimum solutions have not been reached yet. Different metrics are available to evaluate an s-box structure. This study will focus on nonlinearity. Similar results were observed for most of the other criteria. For example, the SAC criterion should be close to an average value of 0.5 [26]. This value is obtained in most studies. However, nonlinearity values may remain low in most studies. The AES s-box structure has a nonlinearity value of 112.

.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig. 1 AES s-box structure

If we give a simple example to better understand the S-box structure; Passing the value 13 through the s-box means replacing the value in the 1st row, 3rd column. In other words, 7D value will be written instead of 13 value. In this way, this process is completed after the whole block has been passed through the s-box. Moreover, the state of a 4*4 block after it has been passed through the s-box structure in figure 1 is given in figure 2.

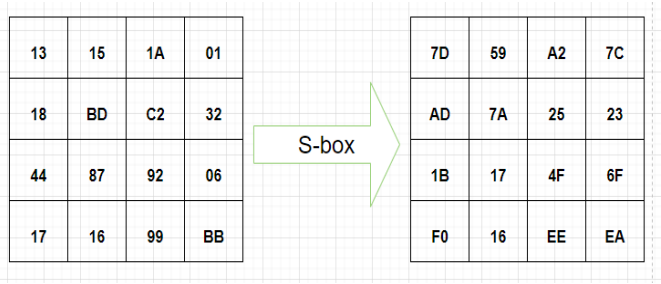

Fig. 2 Passing a sample block through the s-box

III. PERFORMANCE COMPARISON

BIC, SAC, I/O XOR distributions, bijectivity, and nonlinearity metrics are generally used in the literature to evaluate the performance of an s-box structure. When we look at the literature, algorithms are compared by looking at the nonlinearity values. Therefore, only nonlinearity values were considered in this study. An s-box with high nonlinearity makes the algorithm resistant to linear cryptanalysis. The b(k) nonlinearity value of an n-bit long function can be calculated as given in equation 1.

$$\text{NL(b)}=\frac{1}{2}\left[2^n-\left(\max_{h\in\{0,1\}^n}|WS_b(h)|\right)\right] \quad (1)$$

The Walsh spectrum of the function $WS_b(h)$ given in Equation 1 can be calculated as given in Equation 2.

$$WS_b(h)=\sum_{k\in\{0,1\}^n}(-1)^{b(k)\oplus k.h} \quad (2)$$

Where $h\in\{0,1\}^n$ and k.h represents the inner product of k and h values and are calculated as given in equation 3.

$$k.h=(k_1\oplus h_1)+\cdots+(k_n\oplus h_n) \quad (3)$$

The nonlinearity values of s-box structures obtained with different approaches in recent years are given in Table 1.

When the comparison results given in Table 1 are examined, it is seen that the best values are obtained with mathematical transformations. In addition, nonlinearity values, which can be considered high, are often reached in optimization and hybrid methods. However, the nonlinearity value is usually low in s-boxes obtained using only chaos.

Table 1. Performance comparison

Reference	Approach	Average Nonlinearity
[3]	Mathematical Transformation	112
[4]	Mathematical Transformation	112
[5]	Mathematical Transformation	110.5
[6]	Mathematical Transformation	108
[7]	Mathematical Transformation	112
[8]	Mathematical Transformation	107.25
[9]	Chaos	104.7
[10]	Chaos	106.2
[11]	Chaos	106
[12]	Chaos	110
[13]	Chaos	107
[14]	Chaos	106.2
[15]	Optimization	109.5
[16]	Optimization	111
[17]	Optimization	110.5
[18]	Optimization	111.25
[19]	Optimization	109.25
[20]	Optimization	108
[21]	Optimization	109.5
[22]	Optimization	111.75
[23]	Hybrid	110.75
[24]	Hybrid	112
[25]	Hybrid	109

IV. CONCLUSION

In this study, the nonlinearity values of the s-box generation algorithms made in recent years were compared. Chaos, mathematical transformations, and optimization techniques, which are the most popular approaches in this regard, have been used many times. Since each approach has advantages and disadvantages, optimum solutions have not been reached yet. That's why the work continues. Obtaining an s-box with chaos-based methods is quite easy and requires less processing. However, nonlinearity values are mostly low. Nonlinearity values are generally high in mathematical transformation-based methods. However, it can show weaknesses against differential cryptanalysis in various situations. In optimization methods, s-box structures with high nonlinearity values are often obtained. However, there is also the problem of high processing load and complexity of algorithms. In some studies, hybrid methods have been developed by combining these advantages. It is thought that more effective results can be obtained in future studies, especially by using new metaheuristic optimization techniques.

REFERENCES

[1] Artuğer, F., & Özkaynak, F. (2020). A novel method for performance improvement of chaos-based substitution boxes. Symmetry, 12(4), 571.

[2] J. Daemen and V. Rijmen, (1998) ‘‘AES proposal: Rijndael,’’ in Proc. 1st Adv. Encryption Conf., CA, USA, pp. 1–45.

[3] Siddiqui, N., Yousaf, F., Murtaza, F., Ehatisham-ul-Haq, M., Ashraf, M. U., Alghamdi, A. M., & Alfakeeh, A. S. (2020). A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field. Plos one, 15(11), e0241890.

[4] Malik, M. S. M., Ali, M. A., Khan, M. A., Ehatisham-Ul-Haq, M., Shah, S. N. M., Rehman, M., & Ahmad, W. (2020). Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. IEEE Access, 8, 35682-35695.

[5] Ahmad, M., & Al-Solami, E. (2020). Improved 2D Discrete Hyperchaos Mapping with Complex Behaviour and Algebraic Structure for Strong S-Boxes Generation. Complexity, 2020.

[6] Isa, H., Syed Junid, S. A. A., Z’aba, M. R., Endut, R., Ammar, S. M., & Ali, N. (2023). Enhancement of Non-Permutation Binomial Power Functions to Construct Cryptographically Strong S-Boxes. Mathematics, 11(2), 446.

[7] Razaq, A., Ahmad, M., Yousaf, A., Alawida, M., Ullah, A., & Shuaib, U. (2022). A group theoretic construction of large number of AES-like substitution-boxes. Wireless Personal Communications, 122(3), 2057-2080.

[8] Arshad, B., Siddiqui, N., Hussain, Z., & Ehatisham-ul-Haq, M. (2022). A Novel Scheme for Designing Secure Substitution Boxes (S-Boxes) Based on Mobius Group and Finite Field. Wireless Personal Communications, 1-22.

[9] Özkaynak, F. (2020). An analysis and generation toolbox for chaotic substitution boxes: A case study based on chaotic labyrinth rene thomas system. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 44(1), 89-98.

[10] Lambić, D. (2020). A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. Nonlinear Dynamics, 100(1), 699-711.

[11] Artuğer, F., & Özkaynak, F. (2022). A method for generation of substitution box based on random selection. Egyptian Informatics Journal, 23(1), 127-135.
[12] Artuğer, F., & Özkaynak, F. (2021). An effective method to improve nonlinearity value of substitution boxes based on random selection. Information Sciences, 576, 577-588.
[13] Yang, S., Tong, X., Wang, Z., & Zhang, M. (2023). S-box generation algorithm based on hyperchaotic system and its application in image encryption. Multimedia Tools and Applications, 1-25.
[14] Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., & Kaçar, S. (2017). A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. Nonlinear dynamics, 87(2), 1081-1094.
[15] Zamli, K. Z., Din, F., Alhadawi, H. S., Khalid, S., Alsolai, H., Nour, M. K., ... & Assam, M. (2022). Exploiting an Elitist Barnacles Mating Optimizer implementation for substitution box optimization. ICT Express.
[16] Khan, H., Hazzazi, M. M., Jamal, S. S., Hussain, I., & Khan, M. (2023). New color image encryption technique based on three-dimensional logistic map and Grey wolf optimization based generated substitution boxes. Multimedia Tools and Applications, 82(5), 6943-6964.
[17] Artuğer, F. (2023). A New S-box Generator Algorithm Based on 3D Chaotic Maps and Whale Optimization Algorithm. Wireless Personal Communications, 1-19.
[18] Ahmad, M., & Al-Solami, E. (2020). Evolving dynamic S-boxes using fractional-order hopfield neural network based scheme. Entropy, 22(7), 717.
[19] Zamli, K. Z., Kader, A., Din, F., & Alhadawi, H. S. (2021). Selective chaotic maps Tiki-Taka algorithm for the S-box generation and optimization. Neural Computing and Applications, 1-18.
[20] Kang, M., & Wang, M. (2022). New genetic operators for developing S-boxes with low boomerang uniformity. IEEE Access, 10, 10898–10906.
[21] Zamli, K. Z., Din, F., Alhadawi, H. S., Khalid, S., Alsolai, H., Nour, M. K., ... & Assam, M. (2022). Exploiting an Elitist Barnacles Mating Optimizer implementation for substitution box optimization. ICT Express.
[22] Artuğer, F., & Özkaynak, F. (2022). SBOX-CGA: substitution box generator based on chaos and genetic algorithm. Neural Computing and Applications, 34(22), 20203-20211.
[23] Haque, A., Abdulhussein, T. A., Ahmad, M., Falah, M. W., & Abd El-Latif, A. A. (2022). A Strong Hybrid S-Box Scheme Based on Chaos, 2D Cellular Automata and Algebraic Structure. IEEE Access, 10, 116167-116181.
[24] Basha, H. A. M. A., Mohra, A. S. S., Diab, T. O. M., & El Sobky, W. I. (2022). Efficient image encryption based on new substitution box using DNA coding and bent function. IEEE Access, 10, 66409-66429.
[25] Gangadari, B. R., & Ahamed, S. R. (2018). Programmable cellular automata-based low-power architecture to S-box: An application to WBAN. Circuits, Systems, and Signal Processing, 37(3), 1116-1133.
[26] Webster, A. F., & Tavares, S. E. (1985). On the design of S-boxes. In Conference on the theory and application of cryptographic techniques (pp. 523-534). Springer, Berlin, Heidelberg.