Malaysian Journal of Mathematical Sciences 16(4): 697–715 (2022)
https://doi.org/10.47836/mjms.16.4.04

Malaysian Journal of Mathematical Sciences

Journal homepage: https://mjms.upm.edu.my

A New Design of Substitution Box with Ideal Strict Avalanche Criterion

Mohd Esa, N. F., Abdul-Latip, S. F.*, and Abu, N. A.

Information Security Forensics and Computer Networking (INSFORNET), Centre for Advanced Computing Technology, Universiti Teknikal Malaysia Melaka, Malaysia

E-mail:shekhfaisal@utem.edu.my
**Corresponding author*

Received: 23 March 2022
Accepted: 4 September 2022

Abstract

The use of S-boxes (substitution boxes) to provide nonlinear properties is known to be a common way to design a block cipher. These nonlinear properties are necessary to ensure the security of a block cipher. This manuscript proposes a design construction of a new S-box using affine transformation via cellular automata as a permutation matrix. We incorporate this cellular-automaton permutation matrix into the AES Sbox structure and test various irreducible polynomials. Nonlinearity, bijection, bit independence criterion, strict avalanche effect, linear approximation probability, and differential uniformity are the standard performance requirements used to evaluate the S-boxes that arise. Using this method, we are able to determine an irreducible polynomial that enables the construction of a new S-box design that can achieve an ideal strict avalanche criterion (SAC), which will subsequently provide efficiency in the design of block ciphers.

Keywords: substitution-box; irreducible polynomial; cellular automata; strict avalanche criterion.

1 Introduction

The use of secure block ciphers is critical in many applications such as in medical systems, online banking, and e-commerce, which need data protection in terms of its confidentiality. Currently, most of these applications are protected by the current block cipher standard, namely, the Advanced Encryption Standard (AES)[14]. After the selection of AES in the year 2000, Canright [10] stated that it was expected by the cryptography community that the life of AES will last about 20 years after its announcement. Recent attacks on full-round AES which can be found in [9, 8] seem to confirm this expectation. With more serious attacks to appear, this requires a new effort to identify a new block cipher standard to supersede the AES. Furthermore, AES is designed in many versions to enhance the performance, efficiency and the security margins [23].

Having a secure block cipher requires a good design strategy, particularly on the construction of nonlinear components such as substitution boxes (also known as S-boxes). The main objective of S-box construction is to hide the connection between the plaintext and ciphertext. This component implies that the S-boxes are the fundamental part that gives a block cipher security. This nonlinear property within the S-boxes requires it to produce mathematically random-looking outputs. The effect of not having a "random" output can be seen as in the DES algorithm [12], where it is susceptible to statistical analyses such as differential cryptanalysis [7] and linear cryptanalysis [19], and their variants such as works in [28].

One of the properties contributing to the randomness of the S-boxes is known as Strict Avalanche Criterion (SAC). To the best of our knowledge, an S-box to achieve an ideal SAC of 0.5 is not trivial. As a result, we can only find a very limited number of S-boxes to have this property to avoid a biased output.

An $n \times n$ S-box can be represented as a nonlinear function $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$, where $\mathbb{F}_2^n$ represents the vector space of n-tuple elements in $\mathbb{GF}(2)$. This function forms the basis of the confusion property for block ciphers. Having a large size of an S-box may slow down the encryption process, particularly in a scenario where large data processing is needed. Typically, for a general-purpose block cipher, the size of the S-box normally should not exceed 16×16 to give good performance. In addition, the size of S-boxes may give certain advantages and disadvantages as there will be a trade-off involved between performance, security, and space required for the implementation.

According to the seminal paper by Shannon [25], confusion property is a complex relationship that involves as many plaintexts, secret keys, and ciphertexts bits as possible to provide the security strength for a block cipher. As a result, many S-boxes have been designed using a variety of techniques and assessed based on standard evaluation criteria, such as bijective, strict avalanche criterion (SAC), nonlinearity, bit independence criterion (BIC), linear and differential probabilities, etc. The searching for a cryptographically secure S-box is the most challenging stage to ensure the robustness of a cryptographic algorithm against cryptanalysis.

The basis of an S-box is the construction of its Boolean function. The following characteristics are frequently considered for a cryptographic Boolean function: strong nonlinearity, adequate robustness, and strict avalanche criterion (SAC). The trade-off between these characteristics is a challenging problem that has gotten much attention in the cryptography field [36]. The SAC is also determined based on the completeness property, which defines each output bit depending on all the input bits [30]. The value of avalanche, which deviates from 0.5, results in bias outputs and may cause the block cipher to be susceptible to certain cryptanalytic attacks. Mar and Latt [18] proposed a simple and compact method to measure the value of SAC. This method can also be used to determine the given S-box's completeness further. The value of SAC also affects the efficiency of confusion property. When the SAC achieves the ideal value of 0.5, it shows better confusion properties of the S-box. An encryption technique that does not satisfy this criterion may result in bias output. More precisely, if changing a single bit of the input causes only a single bit of output to change, then cracking the encrypted text becomes easier by using, for example, a divide-and-conquer attack.

Therefore, S-boxes have been previously constructed using various approaches in the literature, such as algebraic techniques, power mapping technologies, heuristic methods, cellular automata, and analytical approaches. To the best of our knowledge, improving the security for an S-box has become a challenge to achieve a better score in SAC for good S-Box property. Particularly, a new S-box structure that can provide an ideal SAC is required to secure the S-box against statistical attacks, such as differential and cryptanalysis.

In this paper, an efficient technique for constructing an S-box is proposed. Our work improves previous work by [1] in two folds; first, we apply affine transformation using cellular automata matrix to construct a robust S-box. Using this technique, we are able to find a new algebraic structure that can avoid fixed points while maintaining a high algebraic degree of the S-box.

Secondly, using the pre-determined algebraic structure, we apply all 30 irreducible polynomials one-by-one to find the most optimal irreducible polynomial over $\mathbb{GF}(2^8)$. This way, we are able to find an ideal SAC of 0.5 which can help design a more robust S-box.

In Section 2, we review some previous related works. Section 3 describes the design construction of our proposed S-box. Section 4 describes the application of the design construction for the new S-box. Section 5 presents the result of property analysis for the proposed S-box design. In Section 6, we present the result of NIST statistical randomness test of the proposed S-box. In Section 7, we present the result and discussion on our new S-box. Finally, we conclude the paper and provide the future direction of our work in Section 8.

2 Related Works

In this section, we review recent related works in the construction of S-box design. Khan and Azam [16] developed an S-box using an approach similar to AES, which is based on affine mapping and the orbit of the power function. Consequently, the author has been able to produce 256 alternative S-boxes, which passes all the cryptographic tests such as SAC, nonlinearity, etc. The result on the SAC of this method is 0.503, which deviates slightly from an ideal value of 0.5. Next, Alamsyah *et al.* [5] presented the construction of the S-box by modifying the chosen irreducible polynomial and affine mapping. To generate multiplicative inverse of the input, [5] selected three irreducible polynomials from a list of 30 irreducible polynomials with a maximum degree of 8 and the highest nonlinearity value. Then, Alamsyah *et al.* [5] created 9 AES-like S-boxes using three affine matrices obtained from [29] and [26]. Alamsyah *et al.* [5] claimed that the proposed S-box could provide a higher security level than the other S-boxes. This work has slightly improved the result on SAC even it also deviates from the ideal value of 0.5.

Then, [17] developed a hybrid strategy based on chaotic maps and algebraic transformations for the S-boxes generation. Malik *et al.* [17] began by producing a key-based set of chaotic logistic maps and used the maps to build an 8×8 rotating matrix. Next the rotational matrix performs an affine transformation on the input components to generate the S-box. They demonstrated that the suggested technique could create 128 different rotational matrices, which can then be utilized to generate 128 distinct S-boxes while maintaining the affine transformation. However, the work of these S-boxes did not attain the ideal SAC value of 0.5.

In other work, [1] developed a robust S-box by combining a cellular automaton rule-based matrix technique with an algebraic structure of fractional linear transformation over $\mathbb{GF}(2^8)$. The results reveal that this work outperforms prior related works. Even though the design of the S-box fulfills the criteria of S-box properties, there is one fixed point that has been found in the S-box in addition to not being able to achieve an ideal value of SAC.

Farwa *et al.* [15] developed the S-box construction method based on linear fractional transformation. A straightforward technique with a single-step function was used to structure the suggested S-box. The strength analysis has revealed that the S-box meets the strong cryptographic requirements and has a resistance against differential and linear cryptanalysis. Then, [6] improved the work [15] by incorporating some permutations into the algebraic structure of the symmetric group on the 8-bit input and then performing a bitwise XOR operation to construct a variation of S-boxes. This work has yielded a good result in all cryptographic tests, including the SAC value of 0.4999, close to the ideal value.

Finally, Zahid and Arshad [33] has proposed a novel cubic polynomial transformation-based (CPT) approach for a new design S-box construction. The use of a cubic polynomial has been able to simplify the design construction of the S-box. Several important criteria were used to analyze and appraise the desired strength of the S-box. Then, in the same year, [34] improved the nonlinearity of the S-box by modifying the algebraic structure to apply cubic fractional transformation (CFT). According to [35], they enhanced nonlinearity from 106.8 to 107 and the SAC value from 0.507 to 0.497. Despite the improvement in the nonlinearity, they are not able to achieve an ideal value of SAC to make the S-box stronger.

Most recent studies have improved on various cryptographic features of the S-box, including the SAC, but none of these efforts has obtained an ideal value of SAC of 0.5, to our knowledge. Therefore, in this manuscript, we would like to take this opportunity to fill this gap by proposing a new S-box design with an ideal SAC value of 0.5 and retaining all other good cryptographic properties.

3 Design Construction of Proposed S-Box

In this section, we discuss the method of S-box construction based on the combination of three elements, namely, cellular automata, irreducible polynomials, and affine transformations. Our proposed S-box structure is based on affine transformation, which has the same structure as AES [14] but uses irreducible polynomial valued 283 (in decimal) as the multiplicative inverse in finite fields. Instead, we use the cellular automata-based rule of 90 that we inspire from the work [1], to modify the permutation affine matrix. Then, we select the most suitable irreducible polynomial, giving an ideal SAC value to the S-box.

3.1 Cellular automata

A cellular automaton (CA) is a parallel computation model studied in automata theory.

Definition 3.1. Let $f : \mathbb{F}_2^d \to \mathbb{F}_2$ and $n \geq d$. We define periodic boundary cellular automata with n

input cells and local rule f, for all $x \in \mathbb{F}_2^n$ as: $F(x_1, x_2, \cdots, x_n) = f(x_1, x_2, \cdots, x_d), \cdots, f(x_{n-(d-2)}, \cdots, x_1), \cdots, f(x_n, \cdots, x_{d-1})$.

CA is a discrete dynamical system that evolves and uses a local rule to form its state transition table. A lattice or cell chain of size M characterises the CA, with a location indicating each cell indexed s and a variable r_s that can only accept i discrete values. As a result, these automata have 2^M distinct states. Most of previous works chose the discrete value i to begin with $i = 2$, while the value of r_s was chosen to begin with $r_s = 0$ or 1. r_s^t represents the CA state at time $t \geq 0$ and position indexed s. As can be seen, all times, spaces, and states of the system have discrete values. The CA evolves according to the local rule of 90 which is defined in equation (1) and also illustrated as in Figure 1 [1, 27],

$$r_s^{t+1} = (r_{s-1}^t + r_{s+1}^t) \; mod \; 2. \tag{1}$$

The cell position indexed s at discrete time $t+1$ is dependent on the adjacent cells both on the left and right at time t (cf. Equation (1) and Figure 1). CA is considered uniform when the same rule is used to update the cells; otherwise, it is termed non-uniform or hybrid. It is crucial to note that two main variables affect the development rules of CA, such as the rules and the initial conditions. For instance, Table 1 shows a partial time-space pattern generated by the evolution rule using Equation (1).

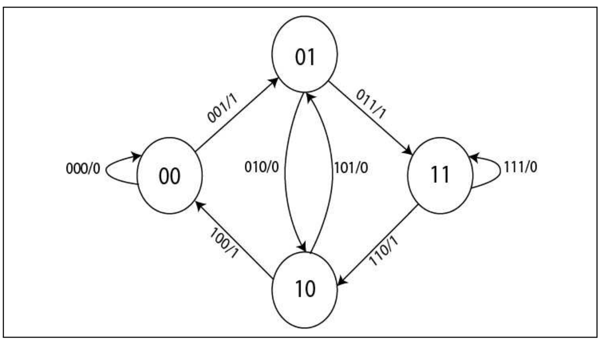

Figure 1: State Diagram of Cellular Automata Rule 90.

To compute the matrix W_L, we set an initial condition vector $v = [0,0,0,1,0,0,0,0]^T$ generating from Table 1 to form the 1^{st} row of matrix A. We ignore the first column from the left of Table 1 as we need to consider the adjacent cells both on the left and right. We repeat this process considering the next row of Table 1 until the last row.

Table 1: A rule 90 arrangement with a single centre value of 1.

space time					$s-1$	s	$s+1$					
t	$\cdots$	0	0	0	0	1	0	0	0	0	0	$\cdots$
$t+1$	$\cdots$	0	0	0	1	0	1	0	0	0	0	$\cdots$
$t+2$	$\cdots$	0	0	1	0	0	0	1	0	0	0	$\cdots$
$t+3$	$\cdots$	0	1	0	1	0	1	0	1	0	0	$\cdots$

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}. \tag{2}$$

The resulting matrix A is then used to construct matrix W_L by applying matrix transposition as shown in Equation (3) below:

$$W_L = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{3}$$

To generate W_R, we use W_L as a multiplier matrix, such that, $W_R = P \times W_L$, where P is a fixed permutation matrix. This matrix can be shown as in Equation (4) below,

$$W_R = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}. \tag{4}$$

Subsequently, using the same method by [1], we construct a square generating matrix W based on the CA rule of 90, allowing us to develop our proposed strong S-box. This matrix has a dimension of 8×8 and is formed by combining both matrices, W_L and W_R. K_R becomes the left and the right parts of W as shown in Equation (5). Then, we apply matrix W into an algebraic structure of an affine transformation as the permutation matrix as described in Section 3.3.

$$W = (W_L | W_R) = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right]. \tag{5}$$

3.2 Irreducible Polynomial

Definition 3.2. A polynomial f over field $\mathbb{F}$ is called irreducible iff f cannot be factorized into two polynomials over $\mathbb{F}$ and both of degree lower than f.

Since the dimension of our proposed S-box is 8×8, thus, we choose an irreducible polynomial of degree 8 to generate its multiplicative inverse. The candidates of irreducible polynomials of degree 8 are listed in Table 2. We investigate each of these polynomials to find the one that can provide optimum performance for our S-box.

Table 2: List of 30 irreducible polynomials in $\mathbb{GF}(2^8)$.

No	Irreducible Polynomial	Binary	Dec
1	$t^8+t^4+t^3+t+1$	100011011	283
2	$t^8+t^4+t^3+t^2+1$	100011101	285
3	$t^8+t^5+t^3+t+1$	100101011	299
4	$t^8+t^5+t^3+t^2+1$	100101101	301
5	$t^8+t^5+t^4+t^3+1$	100111001	313
6	$t^8+t^5+t^4+t^3+t^2+t+1$	100111111	319
7	$t^8+t^6+t^3+t^2+1$	101001101	333
8	$t^8+t^6+t^4+t^3+t^2+t+1$	101011111	351
9	$t^8+t^6+t^5+t+1$	101100011	355
10	$t^8+t^6+t^5+t^2+1$	101100101	357
11	$t^8+t^6+t^5+t^3+1$	101101001	361
12	$t^8+t^6+t^5+t^4+1$	101110001	369
13	$t^8+t^6+t^5+t^4+t^2+t+1$	101110111	375
14	$t^8+t^6+t^5+t^4+t^3+t+1$	101111011	379
15	$t^8+t^7+t^2+t+1$	110000111	391
16	$t^8+t^7+t^3+t+1$	110001011	395
17	$t^8+t^7+t^3+t^2+1$	110001101	397
18	$t^8+t^7+t^4+t^3+t^2+t+1$	110011111	415
19	$t^8+t^7+t^5+t+1$	110100011	419
20	$t^8+t^7+t^5+t^3+1$	110101001	425
21	$t^8+t^7+t^5+t^4+1$	110110001	433
22	$t^8+t^7+t^5+t^4+t^3+t^2+1$	110111101	445
23	$t^8+t^7+t^6+t+1$	111000011	451
24	$t^8+t^7+t^6+t^3+t^2+t+1$	111001111	463
25	$t^8+t^7+t^6+t^4+t^2+t+1$	111010111	471
26	$t^8+t^7+t^6+t^4+t^3+t^2+1$	111011101	477
27	$t^8+t^7+t^6+t^5+t^2+t+1$	111100111	487
28	$t^8+t^7+t^6+t^5+t^4+t+1$	111110011	499
29	$t^8+t^7+t^6+t^5+t^4+t^2+1$	111110101	501
30	$t^8+t^7+t^6+t^5+t^4+t^3+1$	111111001	505

3.3 Affine Transformation

Definition 3.3. An affine function is defined in Boolean function over $\mathbb{GF}(2)$ as $f(x) = u \cdot x \oplus c = u_1x_1 \oplus u_2x_2 \oplus \cdots u_nx_n \oplus c$ where $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$; $u = (u_1, u_2, \cdots, u_n) \in \mathbb{F}_2^n$; and $c \in \mathbb{F}_2^n$.

The multiplicative inverse of the affine transformation for input $x \in \mathbb{GF}(2^8)$ such that $f(x) = (x)^{-1}$ [13] is given by Equation (6):

$$(x)^{-1} = \begin{cases} (x)^{254}, & x \neq 0 \\ 0, & x = 0. \end{cases} \tag{6}$$

We consider the affine transformation as a Boolean function in $\mathbb{GF}(2^n)$ such that $y = \alpha x^{-1} + \beta$, where α is an invertible $n \times n$ matrix; and β is the addition of a constant vector within the same space. The inverse of y in $\mathbb{GF}(2^n)$ is represented as $x = \gamma y^{-1} + \lambda$, where γ is an invertible $n \times n$ inverse matrix; λ is the addition of an 8-bit constant vector; while x^{-1} and y^{-1} are the multiplicative inverse of the input and output bytes of an S-box respectively. Therefore, for our 8×8 S-box, we use affine mapping in $\mathbb{GF}(2^8)$ as shown in Equation (7) below. To compute the affine transformation for our S-box, we represent the invertible permutation matrix α as the matrix K as described in Section 3.1; vector x is chosen such that $x \in \{0,1\}^8$; while the translation vector β is given a decimal value 71. It is important to note that β and λ play a crucial role as translation vectors (cf. Equation (7) and (8)) since they can help to avoid fixed points, $S(x) = x$.

$$y = \alpha x^{-1} + \beta = \begin{bmatrix} 1&0&0&0&0&1&0&0 \\ 0&1&0&0&1&0&1&0 \\ 1&0&1&0&0&0&0&1 \\ 0&0&0&1&1&0&1&0 \\ 1&0&1&0&0&1&0&0 \\ 0&1&0&0&1&0&0&0 \\ 1&0&0&0&0&0&0&1 \\ 0&0&0&0&1&0&0&0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}^{-1} \oplus \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix}. \tag{7}$$

$$x = \gamma y^{-1} + \lambda = \begin{bmatrix} 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0&1 \\ 1&0&0&0&1&0&1&0 \\ 0&1&0&1&0&1&0&1 \\ 1&0&1&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&1&0&0&0&1&0&0 \\ 1&0&1&0&1&0&0&0 \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix}^{-1} \oplus \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} w_0 \\ w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \\ w_7 \end{bmatrix}. \tag{8}$$

4 Application of the Design Construction for a New S-box

In this section, we show the application of the design construction for a new S-box with an ideal SAC. First, we determine the dimension of the S-box that is constructed. We choose to construct an 8×8 S-box as it is suitable for both general purpose and lightweight block ciphers. Next, we identify a suitable algebraic construction, namely, the affine transformation of Boolean function, $y = \alpha x^{-1} + \beta$, where α represents an affine matrix based on cellular automata rule of 90. Based on the identified algebraic construction, we compute affine matrix α using the method introduced by [1]. We initialize the S-box with the byte values in ascending order row by row in the similar fashion as used in the AES S-box by [14] starting with 00 until FF. Then, we identify the 30 candidates of an irreducible polynomial over $\mathbb{GF}(2^8)$ to determine the multiplicative inverse, x^{-1}, of the input. To do this, we construct 30 different candidates of S-boxes, each based on different irreducible polynomials as listed in Table 2. Through an experiment, we evaluate each of the S-boxes with standard evaluation criteria, namely, nonlinearity, strict avalanche criterion (SAC), bit independence criterion (BIC), linear approximation probability, and differential probability. From the experiment, we are able to find an irreducible polynomial that can generate an S-box with ideal SAC (i.e. 0.5), as shown in Equation (9) below:

$$m(t) = t^8 + t^7 + t^4 + t^3 + t^2 + t + 1. \tag{9}$$

Table 3 summarizes the application of affine transformation on each byte of the S-bot using Equation (9) as the irreducible polynomial. As a result, we are able to obtain the S-box and its inverse as shown in Table 4 and Table 5 respectively.

Table 3: Application of affine transformation on each byte of the S-box using $t^8 + t^7 + t^4 + t^3 + t^2 + t + 1$ as the irreducible polynomial.

x	x^{-1}	$y = \alpha x^{-1} + \beta$	*Decimal*	*Binary*	*Hex*
0	0	$\alpha(0) \oplus 71$	71	01000111	47
1	1	$\alpha(1) \oplus 71$	18	00101000	12
2	207	$\alpha(207) \oplus 71$	34	00000100	22
3	138	$\alpha(138) \oplus 71$	105	01111001	69
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
253	79	$\alpha(79) \oplus 71$	38	00100110	26
254	108	$\alpha(108) \oplus 71$	64	01000000	40
255	76	$\alpha(76) \oplus 71$	81	01010001	51

Table 4: Proposed S-box.

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

5 Property Analysis of the New S-Box

This section presents the results of cryptographic properties for our newly designed S-box. We apply the following important tests that are widely used as shown in [2, 3, 20], namely, the strict avalanche criterion (SAC), bit independence criterion (BIC), nonlinearity (NL), linear approximation probability (LP), and differential approximation probability (DP). The numerical results for the properties for our S-box is comparable to the AES S-box and some other existing S-boxes but with a significant improvement in the value of SAC. The results of the comparative performance between our S-box and other recently published S-boxes are presented in Section 7.

Table 5: Inverse Proposed S-box.

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

5.1 Balanced Boolean Function

Definition 5.1. A Boolean function is called as a balanced function when the value of its output either 0 or 1 occurs equally likely for any possible inputs.

More precisely, the Boolean function $f(x)$ is balanced *iff* it meets the following Equation, (10)

$$H_w\left(f\left(x\right)\right) = \sum_{x=0}^{2^n-1} f\left(x\right) = 2^{n-1}, \tag{10}$$

where H_w is the Hamming weight of the truth table; and n is the number of Boolean variables representing the number of bits in the truth table of $f\left(x\right)$. For instance, if $n = 8$, then the Hamming weight for the balanced Boolean function is $H_w\left(f\left(x\right)\right) = 128$. Thus, to avoid biased output, our S-box adopt the property of a balanced Boolean function.

The affine transformation $f(x) = \alpha x^{-1} + \beta$ over $\mathbb{GF}(2^n)$ is a balanced Boolean function. Suppose $X = \{x_0, \cdots, x_{2^n-1}\}$ and $y = \{f(x_0), \cdots, f(x_{2^n-1})\}$ is the input and output of the truth table respectively; and $i \in \{0, \cdots, \log_2 2^{n-1}\}$ is the bit index. Then, y satisfies balanced Boolean function since $(\sum_{x\in X} \lfloor \frac{y}{2^i} \rfloor)\ mod\ 2 = 2^{n-1}$.

5.2 Bijective

Definition 5.2. The S-box is said to be bijective iff every output of a Boolean has a unique value within the range of $[0,\ 2^n\ -\ 1]$.

This property is required for every S-box to be invertible. Thus, for this reason, our S-box is designed to meet the bijective property within the interval of $[0\ ,\ 255]$.

An affine Boolean function is bijective if the affine matrix $(\alpha_{ij}) \in \mathbb{R}^{m\times n}$ is invertible. Therefore, a matrix α is invertible *iff* $\alpha \times \alpha^{-1} = I_n$, where $I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$ and *det* $\alpha, |\alpha| = 0$. Thus, by showing $\alpha \times \alpha^{-1} = I_n$ and $|\alpha| = 0$, enables us to confirm our proposed construction is bijective.

5.3 Strict Avalanche Criterion (SAC)

Definition 5.3. An n-bit Boolean function $y = f(x)$, with $n \geq 3$ is said to satisfy the strict avalanche criterion if flipping a single bit input results in exactly 50% of the output bits will be changed as formalized in Equation 11.

$$f(x \oplus e) \oplus f(x) \triangleq \sum_{k=0}^{2^n-1} [f(x_k \oplus e) \oplus f(x_k)] = 2^{n-1}, \tag{11}$$

where $e \in \mathbb{F}_2^n$ *with* $H_w(e) = 1$.

The SAC requires that if a single bit at position i in the input value is changed, the probability of causing the change at j-th bit in the output value should be approximately 0.5, for $i, j \in \{1, 2, 3, \dots, 8\}$. The dependency matrix in Table 6 shows the SAC values of the proposed S-box. Note that, the average value of SAC from Table 6 for the S-box is equal to 0.5000. This SAC value confirms the proposed S-box satisfies an ideal SAC property which gives the best result compared to the other 29 S-boxes.

Table 6: Dependency matrix for strict avalanche criterion (SAC) values.

0.53125	0.45313	0.53125	0.54688	0.46875	0.48438	0.56250	0.45313
0.45313	0.54688	0.51563	0.53125	0.51563	0.46875	0.51563	0.53125
0.51563	0.45313	0.46875	0.51563	0.51563	0.51563	0.50000	0.51563
0.48438	0.48438	0.48438	0.45313	0.51563	0.51563	0.45313	0.56250
0.51563	0.53125	0.46875	0.53125	0.50000	0.51563	0.45313	0.53125
0.46875	0.45313	0.50000	0.51563	0.43750	0.50000	0.53125	0.51563
0.53125	0.51563	0.53125	0.46875	0.45313	0.43750	0.51563	0.50000
0.51563	0.48438	0.53125	0.48438	0.53125	0.45313	0.51563	0.50000

5.4 Bit Independence Criterion (BIC)

Definition 5.4. A Boolean function satisfies the bit-independence criterion (BIC) for input i and output j, iff when the input bit i is inverted then the output bits j and $j + k$ should change independently, for $k > 0$ and $j + k \leq 8$.

The S-box that generates the output bits independently from each other will have stronger security. If an S-box fulfills the BIC property, all the constituent Boolean functions of the S-box provide high nonlinearity and meet the SAC property very well. Table 7 illustrates the nonlinearity for BIC values for constituent Boolean functions of the proposed S-box. Table 7 shows that the average nonlinearity value for BIC is 112. According to [4], if an S-box exhibits nonlinearity and SAC, it fulfills BIC. The resulting nonlinearity scores of 112 for the proposed S-box demonstrate a weak linear relationship among the output bits, thoroughly validating the BIC property of our S-box.

Table 7: Bit independence criterion (BIC) results for nonlinearity.

-	112	112	112	112	112	112	112
112	-	112	112	112	112	112	112
112	112	-	112	112	112	112	112
112	112	112	-	112	112	112	112
112	112	112	112	-	112	112	112
112	112	112	112	112	-	112	112
112	112	112	112	112	112	-	112
112	112	112	112	112	112	112	-

5.5 Nonlinearity (NL)

Definition 5.5. The nonlinearity of a Boolean function is the Hamming distance between the set of all affine mappings and the Boolean function and is formalized as in Equation (12)

$$N_f = 2^{n-1}(1 - 2^{-n} \max |W_f(z)|), \tag{12}$$

where $W_f(z)$ denote the Walsh spectrum as shown in Equation (13); and $x, z \in \mathbb{GF}(2^n)$.

$$W_f(z) = \sum (-1)^{f(x) \oplus x \cdot z}. \tag{13}$$

Note that, the theoretical maximum value of nonlinearity of a Boolean function in $\mathbb{GF}(2^8)$ is 120 as described in [11]. However, the average nonlinearity value for our S-box is 112 which is comparable to the AES S-box. Table 8 shows our S-box's nonlinearity of all eight constituent Boolean functions. The proposed S-box can reduce linearity and avoid linear cryptanalysis to be applied successfully.

Table 8: Nonlinearities of constituent Boolean functions of proposed S-box.

Boolean function	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
Nonlinearity	112	112	112	112	112	112	112	112

5.6 Linear Approximation Probability (LP)

Definition 5.6. *Linear approximation probability is a measure to determine the maximum value of imbalances or bias between input and output bits for an event as formulated in Equation (14).*

$$LP = \min_{(M_x, M_y \neq 0)} \left| \left(\frac{\#\{x \mid x \cdot M_x = S(x) \cdot M_y\}}{2^n} - \frac{1}{2} \right) \right|, \tag{14}$$

where M_x and M_y represent the input and output masks respectively; x denotes the set of all possible inputs; and n is the length of input (or output) for the S-box.

The result of this analysis is shown in Table 11. Since the result of our S-box outperforms other existing S-boxes, this implies it is more secure to linear cryptanalysis as a result of having a low value of linear approximation probability.

5.7 Differential Approximation Probability (DAP)

Definition 5.7. The differential approximation probability (DP) is a measure to determine the propagation of differential characteristics resulting from two different inputs with a specific differential value. The input differential Δx must uniquely maps to an output differential Δy to ensure the S-box shows a differential uniformity. It can be formalized as in Equation (15).

$$DP(\Delta x \to \Delta y) = \left[\frac{\#\{x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^n} \right], \tag{15}$$

where X denotes the set of all possible input values; and n represents the length of the input (or output) of the S-box.

To provide resistance against differential cryptanalysis requires low differential uniformity. The numerical results of our S-box with regards to differential uniformity are highlighted (i.e. S-box 18) in Table 11.

6 The result of NIST statistical randomness test

In this section, we provide the result of statistical randomness test using the tool provided by the NIST [24] on our newly proposed S-box. These tests aim at identifying any non-randomness that may present within [0,255] range of output sequence. In the statistical tests specified by NIST-800-22, the findings were assessed using the predetermined p-value. If the specified p-value is 0.001, then the resulting p-values must be more than or equal to 0.001 in order to pass the test. The files being tested should include sequences of zeroes and ones recorded in bytes. All entries within the proposed S-box are converted into binary sequences to result in 2048-bit stream.

Table 9: NIST statistical tests and their results for the proposed S-box.

No	NIST test name	p-value	Status
1	Frequency	1.00000	Passed
2	Block Frequency	0.82091	Passed
3	Cumulative Sums (Forward)	0.98416	Passed
	Cumulative Sums (Backward)	0.98416	Passed
4	Runs	0.85968	Passed
5	Longest Run of Ones	1.00000	Passed
6	Binary Matrix Rank	0.48125	Passed
7	FFT	0.71511	Passed
8	Non-Overlapping	0.44529	Passed
9	Overlapping Template	0.10761	Passed
10	Universal	Not applicable	
11	Serial p-value 1	0.86986	Passed
	Serial p-value 2	0.89241	Passed
12	Linear Complexity	0.05169	Passed
13	Approximate Entropy	0.00116	Passed
14	Random Excursions	Not applicable	
15	Random Excursions Variant	Not applicable	

The result of the statistical randomness test on the proposed S-box using the tools from NIST-800-22 are shown in Table 9. Out of 15 tests, only 12 can be applied successfully. However the remaining 3 tests namely the universal statistical test, the random excursions test and the random excursions variant test cannot be applied to the proposed S-box, since the length of the output sequence of the S-box is only 2048 bits which is shorter than the minimum length required by those tests.

7 Result and Discussion

There are four key findings of our work. First, we are able to find that the S-box, which employs $t^8+t^7+t^4+t^3+t^2+t+1$ as the irreducible polynomial, can provide an ideal value of SAC (which is 0.5) in our experiment. As a result, we have constructed the best S-box based on the SAC. In addition, our S-box has a high value of nonlinearity similar to the AES S-box as shown in Table 10. Having this high nonlinearity will result in resistance to linear cryptanalysis. Table 11 highlighted the proposed S-box's differential approximation probability and linear approximation probability values, 0.0015625 and 0.0625, respectively. These small values of DP and LP give our S-box its cryptographic strength as they offer a huge potential to resist against differential and linear cryptanalysis, respectively. Our proposed S-box also fulfills the randomness properties when using the tests provided by the NIST in [24].

Table 10: Numerical result comparison of the strict avalanche criterion (SAC), bit independence criterion (BIC), nonlinearity (NL) for our propose S-boxes with previous work of S-boxes design.

S-box Method	Nonlinearity Min	Nonlinearity Max	Nonlinearity Average	SAC	Offset SAC	BIC-NL
AES [14]	112	112	112	0.4999	0.0001	112
Khan and Azam [16]	112	112	112	0.503	0.003	112
Farwa et al. [15]	112	112	112	0.5016	0.0016	112
Alamsyah et al. [5]	112	112	112	0.501	0.001	112
Aboytes-Gonzalez et al. [1]	112	112	112	0.4998	0.0002	112
Zahid and Arshad [33]	104	108	106.8	0.507	0.007	103.9
Zahid et al. [34]	106	108	107	0.497	0.003	103.5
Malik et al. [17]	112	112	112	0.501	0.001	112
Anees and Chen [6]	112	112	112	0.4999	0.0001	112
Nitaj et al. [21]	112	112	112	0.501	0.001	112
Nizam Chew and Ismail [22]	112	112	112	0.4981	0.0019	112
Zahid et al [32]	104	110	107.5	0.4980	0.0020	103.5
Zahid et al [31]	110	112	111.5	0.506	0.006	104.2
Zahid et al [35]	110	112	111.5	0.502	0.002	103.7
S-box 1	112	112	112	0.5076	0.0076	112
S-box 2	112	112	112	0.4985	0.0015	112
S-box 3	112	112	112	0.5046	0.0046	112
S-box 4	112	112	112	0.4993	0.0007	112
S-box 5	112	112	112	0.5081	0.0081	112
S-box 6	112	112	112	0.5073	0.0073	112
S-box 7	112	112	112	0.5081	0.0081	112
S-box 8	112	112	112	0.4941	0.0059	112
S-box 9	112	112	112	0.5044	0.0044	112
S-box 10	112	112	112	0.5051	0.0051	112
S-box 11	112	112	112	0.5017	0.0017	112
S-box 12	112	112	112	0.5024	0.0024	112
S-box 13	112	112	112	0.4963	0.0037	112
S-box 14	112	112	112	0.5039	0.0039	112
S-box 15	112	112	112	0.5027	0.0027	112
S-box 16	112	112	112	0.5049	0.0049	112
S-box 17	112	112	112	0.4995	0.0005	112
S-box 18	112	112	112	**0.5000**	**0**	112
S-box 19	112	112	112	0.5029	0.0029	112
S-box 20	112	112	112	0.5061	0.0061	112
S-box 21	112	112	112	0.4988	0.0012	112
S-box 22	112	112	112	0.5032	0.0032	112
S-box 23	112	112	112	0.4468	0.0532	112
S-box 24	112	112	112	0.5078	0.0078	112
S-box 25	112	112	112	0.4983	0.0017	112
S-box 26	112	112	112	0.5007	0.0007	112
S-box 27	112	112	112	0.5061	0.0061	112
S-box 28	112	112	112	0.5005	0.0005	112
S-box 29	112	112	112	0.5024	0.0024	112
S-box 30	112	112	112	0.5002	0.0002	112

Table 11: Numerical result comparison of linear approximation probability (LP), and differential approximation probability (DP) of proposed S-boxes with previous work of S-boxes design.

S-box Method	LP	DP
AES [14]	0.0625	0.0015625
Khan and Azam [16]	0.0625	0.0015625
Farwa et al. [15]	0.0625	0.0015625
Alamsyah et al. [5]	0.0625	0.0015625
Aboytes-Gonzalez et al. [1]	0.0625	0.0015625
Zahid and Arshad [33]	0.14	0.054
Zahid et al. [34]	0.156	0.039
Malik et al. [17]	0.0625	0.0015625
Anees and Chen [6]	0.0625	0.0015625
Nitaj et al. [21]	0.0625	0.0015625
Nizam Chew and Ismail [22]	0.0625	0.0015625
Zahid et al. [32]	0.14063	0.039063
Zahid et al. [31]	0.125	0.039063
Zahid et al. [35]	0.125	0.039063
S-box 1	0.0625	0.0015625
S-box 2	0.0625	0.0015625
S-box 3	0.0625	0.0015625
S-box 4	0.0625	0.0015625
S-box 5	0.0625	0.0015625
S-box 6	0.0625	0.0015625
S-box 7	0.0625	0.0015625
S-box 8	0.0625	0.0015625
S-box 9	0.0625	0.0015625
S-box 10	0.0625	0.0015625
S-box 11	0.0625	0.0015625
S-box 12	0.0625	0.0015625
S-box 13	0.0625	0.0015625
S-box 14	0.0625	0.0015625
S-box 15	0.0625	0.0015625
S-box 16	0.0625	0.0015625
S-box 17	0.0625	0.0015625
S-box 18	0.0625	0.0015625
S-box 19	0.0625	0.0015625
S-box 20	0.0625	0.0015625
S-box 21	0.0625	0.0015625
S-box 22	0.0625	0.0015625
S-box 23	0.0625	0.0015625
S-box 24	0.0625	0.0015625
S-box 25	0.0625	0.0015625
S-box 26	0.0625	0.0015625
S-box 27	0.0625	0.0015625
S-box 28	0.0625	0.0015625
S-box 29	0.0625	0.0015625
S-box 30	0.0625	0.0015625

Since our work to find the invertible matrices is based on an experiment, one should examine the relationship between the rule of cellular automata and its initial vectors. To be more precise, the new invertible matrices can be constructed mathematically rather than finding the invertible matrices through an experiment. We leave this problem as the scope of future research.

8 Conclusion

An S-box is a popular nonlinear element in symmetric block ciphers. We have proposed a unique method to design an efficient strong S-box by incorporating an affine transformation based on cellular automata matrix under a suitable modulo irreducible polynomial. Our proposed S-box is tested for cryptographic strength using various properties such as strict avalanche criterion (SAC), bit independence criterion (BIC), nonlinearity, linear approximation probability (LP), and differential approximation probability (DP). We have obtained significant results using these tests compared to the other related S-boxes available in the literature. Our method enables us to obtain an ideal SAC value of 0.5 from the proposed S-box. The potential scores of BIC, nonlinearity, SAC, and other criteria of our S-box represent its prospective candidature for future block ciphers.

As for future work, one should try to formulate the relationship between the rule of cellular automata and its initial condition to find the invertible matrix mathematically instead of experimentally. Finally, we also would like to see the result of using our proposed S-box in the AES block cipher or any new block cipher designs, particularly regarding security.

Acknowledgement This research paper is supported by Fundamental Research Grant Scheme (FRGS) numbered FRGS/1/2022/ICT04/UTEM/02/1 funded by Ministry of Higher Education, Malaysia. We thank the reviewers for the constructive comments and editor for the guidance.

Conflicts of Interest The author declares no conflict of interest.

References

[1] J. Aboytes-González, J. Murguía, M. Mejía-Carlos, H. González-Aguilar & M. Ramírez-Torres (2018). Design of a strong S-box based on a matrix approach. *Nonlinear Dynamics*, *94*(3), 2003–2012. https://doi.org/10.1007/s11071-018-4471-z.

[2] C. M. Adams & S. Tavares (1990). The use of bent sequences to achieve higher-order strict avalanche criterion in S-box design. *Technical Report TR 90-013*, pp. 1–18. Queen's University, Kingston, Ontario.

[3] C. M. Adams & S. Tavares (1990). Good S-boxes are easy to find. In *Advances in Cryptology-CRYPTO 89 Proceedings*, volume 435 pp. 612–615. https://doi.org/10.1007/0-387-34805-0_56.

[4] C. Adams & S. Tavares (1990). The structured design of cryptographically good S-boxes. *Journal of Cryptology*, *3*, 27–41. https://doi.org/10.1007/BF00203967.

[5] Alamsyah, A. Bejo & T. B. Adji (2018). The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box. *Nonlinear Dynamics*, *93*(4), 2105–2118. https://doi.org/10.1007/s11071-018-4310-2.

[6] A. Anees & Y.-P. P. Chen (2020). Designing secure substitution boxes based on permutation of symmetric group. *Neural Computing and Applications*, *32*(11), 7045–7056. https://doi.org/10.1007/s00521-019-04207-8.

[7] E. Biham & A. Shamir (1993). Differential cryptanalysis of the full 16-round DES. In *Advances in Cryptology - CRYPTO 92*, volume 740 pp. 487–496. https://doi.org/10.1007/3-540-48071-4_34.

[8] A. Biryukov & D. Khovratovich (2009). Related-key cryptanalysis of the full AES-192 and AES-256. In *Advances in Cryptology-ASIACRYPT 2009*, volume 5912 pp. 1–18. https://doi.org/10.1007/978-3-642-25385-0_19.

[9] A. Bogdanov, D. Khovratovich & C. Rechberger (2011). Biclique cryptanalysis of the full AES. In *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 pp. 344–371. https://doi.org/10.1007/978-3-642-25385-0_19.

[10] D. Canright (2005). A very compact S-box for AES. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 441–455. https://doi.org/10.1007/11545262_32.

[11] C. Carlet & C. Ding (2007). Nonlinearities of S-boxes. *Finite fields and their applications*, *13*(1), 121–135. https://doi.org/10.1016/j.ffa.2005.07.003.

[12] D. Coppersmith (1994). The data encryption standard (DES) and its strength against attacks. *Tatra Mountains Mathematical Publications*, *38*(3), 243–250. https://doi.org/10.1147/rd.383.0243.

[13] J. Cui, L. Huang, H. Zhong, C. Chang & W. Yang (2011). An improved AES S-box and its performance analysis. *International Journal of Innovative Computing, Information and Control*, *7*(5), 2291–2302.

[14] J. Daemen & V. Rijmen (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Berlin, Heidelberg, Berlin, Germany.

[15] S. Farwa, T. Shah & L. Idrees (2016). A highly nonlinear S-box based on a fractional linear transformation. *SpringerPlus*, *2016*(5), 12 pages. https://doi.org/10.1186/s40064-016-3298-7.

[16] M. Khan & N. A. Azam (2015). S-boxes based on affine mapping and orbit of power function. *3D Research*, *6*, Article ID: 12. https://doi.org/10.1007/s13319-015-0043-x.

[17] M. S. M. Malik, M. A. Ali, M. A. Khan, M. Ehatisham-Ul-Haq, S. N. M. Shah, M. Rehman & W. Ahmad (2020). Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. *IEEE Access*, *8*, 35682–35695. https://doi.org/10.1109/ACCESS.2020.2973679.

[18] P. P. Mar & K. M. Latt (2008). New analysis methods on strict avalanche criterion of S-boxes. *International Journal of Mathematical and Computational Sciences*, *2*(12), 899–903. https://doi.org/10.5281/zenodo.1072660.

[19] M. Matsui (1994). Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT 93*, volume 765 pp. 386–397. https://doi.org/10.1007/3-540-48285-7_33.

[20] W. Millan (1998). How to improve the nonlinearity of bijective S-boxes. In *Information Security and Privacy*, volume 1438 pp. 181–192. https://doi.org/10.1007/BFb0053732.

[21] A. Nitaj, W. Susilo & J. Tonien (2020). A new improved AES S-box with enhanced properties. In *Australasian Conference on Information Security and Privacy*, pp. 125–141. https://doi.org/10.1007/978-3-030-55304-3_7.

[22] L. C. Nizam Chew & E. S. Ismail (2020). S-box construction based on linear fractional transformation and permutation function. *Symmetry*, *12*(5), 826. https://doi.org/10.3390/sym12050826.

[23] A. Nur Azman (2021). An efficient 2048-bit block cipher. *Malaysian Journal of Mathematical Sciences*, *15*(S), 141–167.

[24] A. Rukhin, J. Soto, J. Nechvatal, M. Smid & E. Barker (2001). *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, Gaithersburg, MD. http://purl.access.gpo.gov/GPO/LPS72078.

[25] C. E. Shannon (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, *28*(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.

[26] W. Stallings (2010). *Cryptography and Network Security: Principles and Practice*. Prentice Hall Press, United States.

[27] S. Uguz, E. Acar & S. Redjepov (2018). Three states hybrid cellular automata with periodic boundary condition. *Malaysian Journal of Mathematical Sciences*, *12*(3), 305–321.

[28] S. Vaudenay (1996). An experiment on DES statistical cryptanalysis. In *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, pp. 139–147. https://doi.org/10.1145/238168.238206.

[29] U. Waqas, S. Afzal, M. A. Mir & M. Yousaf (2014). Generation of AES-like S-boxes by replacing affine matrix. In *2014 12th International Conference on Frontiers of Information Technology*, pp. 159–164. https://doi.org/10.1109/FIT.2014.38.

[30] A. Webster & S. E. Tavares (1985). On the design of S-boxes. In *Conference on the theory and application of cryptographic techniques*, pp. 523–534. https://doi.org/10.1007/3-540-39799-X_41.

[31] A. H. Zahid, M. Ahmad, A. Alkhayyat, M. T. Hassan, A. Manzoor, A. K. Farhan et al. (2021). Efficient dynamic S-box generation using linear trigonometric transformation for security applications. *IEEE Access*, *9*, 98460–98475. https://doi.org/10.1109/ACCESS.2021.3095618.

[32] A. H. Zahid, E. Al-Solami & M. Ahmad (2020). A novel modular approach based substitution-box design for image encryption. *IEEE Access*, *8*, 150326–150340. https://doi.org/10.1109/ACCESS.2020.3016401.

[33] A. H. Zahid & M. J. Arshad (2019). An innovative design of substitution-boxes using cubic polynomial mapping. *Symmetry*, *11*(3), 10 pages. https://doi.org/10.3390/sym11030437.

[34] A. H. Zahid, M. J. Arshad & M. Ahmad (2019). A novel construction of efficient substitution-boxes using cubic fractional transformation. *Entropy*, *21*(3), 13 pages. https://doi.org/10.3390/e21030245.

[35] A. H. Zahid, H. Rashid, M. M. U. Shaban, S. Ahmad, E. Ahmed, M. T. Amjad, M. A. T. Baig, M. J. Arshad, M. N. Tariq, M. W. Tariq et al. (2021). Dynamic S-box design using a novel square polynomial transformation and permutation. *IEEE Access*, *9*, 82390–82401. https://doi.org/10.1109/ACCESS.2021.3086717.

[36] Y. Zheng & X.-M. Zhang (2000). On relationships among avalanche, nonlinearity, and correlation immunity. In *Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, pp. 470–482. Springer-Verlag, Berlin, Heidelberg.