Substitution Box Design Based from Symmetric Group Composition

Substitution Box Design Based from Symmetric Group Composition

Muhammad Fahim Bin Roslan[1], Kamaruzzaman Seman[1], Azni Haslizan Ab Halim[2], and M Nor Azizi Syam Mohd Sayuti[1]

[1]Fakulti Kejuruteraan dan Alam Bina, Universiti Sains Islam Malaysia, Nilai, 71800 Negeri Sembilan, Malaysia
[2]Fakulti Sains dan Teknologi, Universiti Sains Islam Malaysia, Nilai, 71800 Negeri Sembilan, Malaysia

fahimroslan17@gmail.com

Abstract. This work shows a new design of substitution box (S-Box) construction for the implementation in the block cipher. The S-Box is the only component in block cipher such as advanced encryption standard (AES) that possess the nonlinearity characteristics. Hence, it is crucial to properly design so that it able resist the cipher against known attack such as linear and differential attacks. Thee construction is based on composition of permutation within the symmetric group. This paper focus on the AES S-Box class which received 8-bit input and produced 8-bit output. This bijective S-Box consist of 256 elements which later involve in the process of composition. Initially, a set of 30 S-Box with high nonlinearity is generated using 30 irreducible polynomials under the finite field $GF(2^8)$. These S-Box is then undergoing two rounds of composition which finally yield about 1.62 million S-Box. More than half of the generated S-Box achieve the nonlinearity of at least 100 with the maximum recorded nonlinearity of 110. This method also guarantee that the generated S-Box is bijective. To show the security level of our construction method, a comparison to other constriction methods is conducted. The methods introduced in this paper have slightly higher nonlinearity compared to several construction with the value of differential uniformity not on the par as AES however comparable to other similar heuristic construction.

Keywords: Block Cipher, Substitution Box, Irreducible Polynomial, Composition

1. Introduction

In today's digital age, security assurance of confidential data is the most important aspect that needs to be emphasized. One of the most popular security measures is by implementing the cryptography schemes where every confidential data needs to be encrypted first before it is sent through the insecure channel. Currently, the most widely used cryptography scheme is advanced encryption standard (AES) which was developed in 2001 [1]. AES is a type of block cipher which adapting the substitution-permutation network (SP-network) and used the same key to encrypt and decrypt the message. The most vital component in block cipher including AES is the implementation of substitution box (S-Box). This is because this component is the only one that provides the nonlinearity effect. Besides that, according to the seminal work of Shannon [2], the S-Box also in line with the effect of confusion which obscures the statistical relationship between the plain text and the secret key. As the most

essential elements in a block cipher, the construction of S-Box needs to obey several good cryptographic properties so that the cipher will have the resistance against a known attack such as linear and differential attack. In most literature that is related to S-Box construction, the essential properties that need to be quantify are the balancedness, nonlinearity, differential uniformity and algebraic degree. All these properties will be discussed in detail in the following section.

Basically, an S-Box is a nonlinear mapping of a Boolean function of n-variables to m-variables that can be defined as $S: \{0,1\}^n \rightarrow \{0,1\}^m$ where $\{0,1\}^n$ is a vector space over $GF(2^n)$ or simply notated as (n, m)-mapping. For the case of AES class S-Box, it would be (n, n)- bijective mapping where $n = 8$. This mapping then forms an S-Box with 256 elements which also form a field under $GF(2^8)$. As the mapping is bijective, the S-Box also represent the permutation of all 256 elements and can be reform by permuting its elements. Under several mathematical method, the permutation of all elements can possibly fulfil the cryptographic properties as stated before. This setting has been adapted in the original AES S-Box construction that has been proposed by its founders Vincent Rijmen and Joan Daemon. The original construction composed of two algebraic approach which are finite field inversion with respect to primitive polynomial $p(x)$ over $GF(2^8)$ and the affine transformation. This approach has yielded the best S-Box configuration as it achieves the highest value of nonlinearity and algebraic degree and lowest in differential uniformity. The algebraic approach may produce the best S-Box though it is very hard to find the alternative method under this approach.

As the S-Box is just the permutation of finite elements, (in the case of AES is 256 elements), its construction is open to any methods that can permute the elements while maintaining the objectives of the search which is to find the best S-Box that fulfilled the cryptographic properties. In most related literature, these methods are characterized as a heuristic or evolutionary approach. This approach consists of various direct searching methods which also lead to the large search area. Finding one good S-Box using this approach still an open problem as until date there is no construction method that can compete with the algebraic approach proposed in the original AES S-Box construction.

2. Related Work

Basically, to construct an S-Box, three approaches available which are the algebraic methods, random search and heuristic methods. The algebraic methods as implemented in the original construction of AES S-Box is the best construction so far though it is very difficult to find an alternative that can give similar strength. However, some literature still discussing simple modification of current algebraic methods as has been done in [3] where the authors change the order of operation between finite field inversion and the affine transformation. The modification aims to improve the algebraic complexity by increasing the total number of terms in the algebraic expression of the S-Box. However, this modification may bring some downside as it downgrades the security of the decryption process. This problem has been solved by applying two affine transform (in [4], [5], [6], and [7]) which maintains the number of terms in the algebraic expression for both encryption and decryption side. The second approach is the least preferred one due to large search space which leads to infeasibility of searching good S-Box in a practical time frame. Besides, using this approach also lead to lower probability of finding one suitable candidate. This has been shown in [8] where the author tried to generate an S-Box using random binary sequence which yielded the set of S-Box with weak cryptography properties.

The well-discussed approach, the heuristic approach is the process of finding good cryptographic properties S-Box that is based on some mathematical method and iteration. There are diverse types of method that have been discussed. Most of the methods can be categorized into several main streams such as chaotic map approach, evolutionary algorithm approach, natural induced approach and several other random methods. Chaotic maps approach is one of the highlighted methods as it involves the iteration of a sequence that is based on chaotic behaviour which is useful in generating an S-Box with various strength. Usually, the resulted S-Box is not as optimal as algebraic approach but still, have the resistance against linear and differential attack. Some example of this implementation can be found in [9], [10], [11], [12], [13], [14], [15] and [16]. Another approach that is also well developed is the

evolutionary algorithms, the algorithms that optimize the search of good S-Box inspired by several natural phenomena. A genetic algorithm that is adapted in [17] and [18] are mimicking the natural selection in which it will select the best S-Box from initial population. The resulted S-Box can be categorized as sub-optimal. Besides fulfilling the cryptography properties, some work showed the genetic algorithm able to generate an S-Box with resilient to side channel attack such as in [19]. Other interesting work can be found in [20] where the construction of S-Box is inspired by the movement of bee waggle dance. The resulted S-Box is sub-optimal.

2.1. Our Contribution

In this paper, a new method of searching S-Box is introduced which is in the category of the heuristic method. The aim is to find the set of S-Box which has higher nonlinearity and algebraic degree and lower in differential uniformity. Besides that, the constructed S-Box using the proposed method is guaranteed to be balanced. As mentioned before, the AES S-Box is just a permutation of 256 elements which can be reformed by permuting its element. These set of permutation can be regarded as a symmetric group element which have composition of permutation as the binary operation. Hence, this paper proposes the construction of S-Box from the composition of permutation of highly nonlinear S-Box constructed by the algebraic approach.

The remaining of this paper is organized as follows. Section 2 is discussing about cryptographic properties of Boolean function which are nonlinearity, differential uniformity and algebraic degree. The fundamental aspects of Boolean function also are presented. In section 3, the background and the structure of propose S-Box construction is presented. The results are presented in section 4. Some comparative study with recent research is carried out within this section. Finally, section 5 concludes the paper.

3. Preliminaries

In this section, some fundamental aspects of Boolean function in the sense of cryptography are presented. For a comprehensive look, the reader may refer to [21].

Let $\mathbb{F}_2^n$ be a vector space of n-variables with the cardinality of 2^n. An S-Box is a type of n, m-function S that has n-binary input and m-binary output which can be defined as the mapping of $S: \mathbb{F}_2^n \to \mathbb{F}_2^m$ where each $\bar{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$ and each $\bar{y} = (y_1, y_2, \dots, y_n) \in \mathbb{F}_2^m$ can be assigned as $S(\bar{x}) = \bar{y}$. This function S can also be called as vectorial Boolean function, comprising of m single Boolean functions called as coordinate function which is defined as $f_i: \mathbb{F}_2^n \to \mathbb{F}_2$ where $i = 1,2, \dots, m$. Most of the cryptography properties that is discuss in this paper are evaluated based on the linear combination of these single Boolean function. In evaluating Boolean function, several types of representation are used such as the truth table, the polarity truth table and the algebraic normal form. The truth table (TT) is simply the collection of all output of Boolean function f with the input vector $\bar{x} \in \mathbb{F}_2^n$ arranged in lexicographical order and has the dimension of 2^n. The polarity truth table on the other hand, is made up of the sign function expressed as $\hat{f} = (-1)^f$ which yield the output of -1 and 1 for the input of 0 and 1 respectively. The algebraic normal form (ANF) represent the Boolean function f in term of polynomial. Generally, the ANF of any variable can be denoted as follows,

$$f(x) = c_0 \bigoplus_{1 \le i \le n} c_i x_i \bigoplus_{1 \le i \le j \le n} c_{ij} x_i x_j \bigoplus \cdots \bigoplus c_{1\dots n} x_1 x_2 \dots x_n \tag{1}$$

where the coefficient $c_0, c_i, c_{ij}, c_{i,\dots,n}$ having the value of either 0 or 1. It has been proven the ANF is unique to each function f in the respective n variables Boolean function. While the longest term in the ANF will determine the algebraic degree of the Boolean function f. If the algebraic degree of given function equal to 1, then that function is called as an affine function, and with the absence of constant term c_0, the function is categorized as linear Boolean function.

3.1. Nonlinearity

Nonlinearity N_f is a measure of Hamming distance between the Boolean function f and the set of all affine function, $l_{a,b}$ which can be shown as

$$N_f = \min_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2} \text{dist}(f, \ell_{a,b}) \tag{2}$$

The higher value of N_f as in Eq.(2) shows the better nonlinearity of such function f which also indicates that function f have greater Hamming distance to the set of affine function $\ell_{a,b}$. Frequently, the quantity of N_f is evaluated using the Walsh-Hadamard Transform (WHT) that utilize the sign function $\hat{f}$. The WHT is denoted as $W_f(\omega)$ as follows,

$$W_f(\omega) = \sum_{x\in\mathbb{F}_2^n} (-1)^{\langle x,\omega\rangle \oplus f(x)} \tag{3}$$

with $\forall\omega \in \mathbb{F}_2^n$. The output of Eq.(3) is known as the Walsh spectrum which has the range value of $W_f(\omega) \in [-2^n, 2^n]$. Using the Walsh spectrum, the nonlinearity of function f can be defined as,

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\omega\in\mathbb{F}_2^n} \left|W_f(\omega)\right| \tag{4}$$

In the S-Box S which comprise of several single Boolean functions, the value of nonlinearity is given by any coordinate function $f_i, i = 1,2,\dots,m$ that achieve the minimum value of N_f based on Eq.(4). As for AES class S-Box ($m = n = 8$), the maximum achievable value of N_f is 112.

3.2. Differential Uniformity

This property is highly related to differential attack proposed by [22] where they study the relationship between the difference in plaintext and the corresponding difference in ciphertext. To avoid differential attack, the S-Box S should have smaller value in difference distribution table in which the smallest value is denoted as δ that is given by the following equation,

$$\delta = \max_{a,b\in\mathbb{F}_2^n, a\neq 0} \left|x \in \mathbb{F}_2^n : S(x+a) + S(x) = b\right| \tag{5}$$

This δ parameter only take even values. Thus, the smallest value would be 2, and such S-Box can be called as almost perfect nonlinear. The best value achievable by the AES class S-Box is 4. Such S-Box would be called as 4-uniform S-Box.

3.3. Algebraic Degree

Algebraic degree is determined by the longest term in ANF as shown in Eq. (1). Higher algebraic degree is more favourable as it gives strength to S-Box to thwart higher order differential attack [23]. For an S-Box S, the algebraic degree is evaluated based on coordinate function f_i. The expression to evaluate algebraic degree of an S-Box is shown as [24]

$$AD(S) = \max\{\deg(f_i) \mid i = 1,2,\dots,m\} \tag{6}$$

For AES class S-Box, the optimum algebraic degree to resist algebraic attack is 7.

4. The Proposed S-Box

4.1. AES S-Box Construction

AES substitution box (S-Box) is composed of two components which are finite field inversion and the affine transformation. In the first component, the finite field inversion maps each element in $GF(2^8)$ to its own multiplicative inverse by using the irreducible polynomial $p(x)$. However, the element zero is mapped to itself. Hence, for each element $\alpha \in GF(2^8)$, its multiplicative inverse $\gamma \in GF(2^8)$ is determined by

$$\alpha\gamma \equiv 1 \bmod p(x) \tag{7}$$

The polynomial $p(x)$ can be selected from 30 different irreducible polynomials with maximum degree of 8. In original AES S-Box, the irreducible polynomial is set as $p(x) = x^8 + x^4 + x^3 + x + 1$ which in the first list of possible irreducible polynomial as presented in Table 1.

Table 1. List of Irreducible Polynomial $p(x)$

Irreducible Polynomial of Degree 8	
11B	169
1B1	13F
18B	1DD
11D	171
1BD	14D
18D	1E7
12B	177
1C3	15F
19F	1F3
12D	17B
1CF	163
1A3	1F5
139	187
1D7	165
1A9	1F9

Table 1 present all possible polynomial in hexadecimal form. The first one in the list for example is presented as $11B_{hex}$ which can be converted to binary as 100011011_{bin}. Each binary bit represents the coefficient of the polynomial with the position of the bit determined the exponent. Hence the left-most of the binary bit represent x^8 while the right most of the bit represent $x^0 = 1$.

The second component transform the finite field inversion output γ by using the affine transform which can be presented as

$$\beta = A\gamma + c \tag{8}$$

where β is the output of the transformation, A is the constant affine matrix and c is the additive constant. The constant affine matrix is 8×8 invertible matrix while c is the 8-bit constant vector. Eq. 8 can be presented as follows,

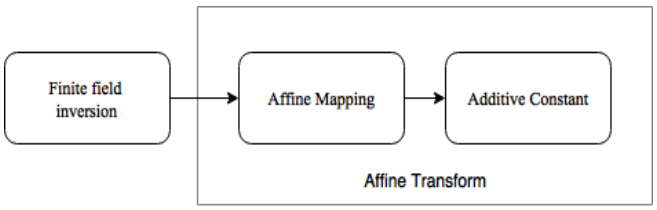

Figure 1. Phase of S-Box Construction

$$\begin{bmatrix}\beta_0\\ \beta_1\\ \beta_2\\ \beta_3\\ \beta_4\\ \beta_5\\ \beta_6\\ \beta_7\end{bmatrix} = \begin{bmatrix}1&1&0&0&0&0&0&1\\ 1&1&1&0&0&0&0&0\\ 0&1&1&1&0&0&0&0\\ 0&0&1&1&1&0&0&0\\ 0&0&0&1&1&1&0&0\\ 0&0&0&0&1&1&1&0\\ 0&0&0&0&0&1&1&1\\ 1&0&0&0&0&0&1&1\end{bmatrix}\begin{bmatrix}\gamma_0\\ \gamma_1\\ \gamma_2\\ \gamma_3\\ \gamma_4\\ \gamma_5\\ \gamma_6\\ \gamma_7\end{bmatrix} + \begin{bmatrix}c_0\\ c_1\\ c_2\\ c_3\\ c_4\\ c_5\\ c_6\\ c_7\end{bmatrix} \tag{9}$$

To summarize, the S-Box act as the mapping from input element $\boldsymbol{\alpha} \in \boldsymbol{GF}(\mathbf{2^8})$ to the output $\boldsymbol{\beta} \in \boldsymbol{GF}(\mathbf{2^8})$ by using two main component which are finite field inversion and the affine mapping as shown in figure 1. Alternatively, the S-Box can be presented as a function $\boldsymbol{S}(\boldsymbol{\alpha}) = \boldsymbol{\beta}$.

4.2. New Method to Construct AES Class S-Box

This section introduces our proposed technique to construct the AES class S-Box. The irreducible polynomial $p(x)$ in the original AES S-Box can be replaced by other 29 available irreducible polynomials as presented in table 1. Hence, at least 30 different AES class S-Box can be generated from the list itself. Besides, based on [21] and [22], it is also possible to replace the affine matrix and the additive constant in order to generate new permutation while maintaining the algebraic structure of multiplicative inverse. This paper idea is to compose these S-Box by using the method of composition of permutation. The method is possible as every generated S-Box is a permutation of elements of finite field $GF(2^8)$. The idea of composition of permutation can be illustrated as follows.

Consider a bijective mapping $\sigma: X_n \to X_n$ with the set $X_n = \{1,2,\dots,n\}$. The notation of bijective mapping or permutation σ can be represented as Cauchy's two-line representation as follows,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \tag{10}$$

where the first row is the element of X_n and the second row is its permutation under bijective mapping σ. Different bijective mapping will result in different permutation. For any set M with n elements, there are exactly $n!$ different possible permutations that can be generated. Each of this permutation is an element in a group called symmetric group denoted as $Sym(S)$. As a group, the operation associated with the group element is called as composition denoted as $\circ$ while the identity is the mapping i denoted as $i: i(k) = k$ for all $k \in X_n$. Composition process map any element of X_n from permutation σ and π to $\pi(\sigma(k))$. As the $Sym(X)$ is not Abelian, two permutation would produce two different composition in which it can be represented as $\sigma \circ \pi \neq \pi \circ \sigma$.

4.3. The Construction of S-Box

Based on previous section 4.1, our idea is to compose S-Box generated from different irreducible polynomials $p(x)$. We present two approach of construction which are named as Setting 1 and Setting 2. In Both approaches, the initial set of S-Box were constructed using 30 different irreducible polynomials $p(x)$ in which each $p(x)$ produced one S-Box. Then, two round of composition process were done in which first round produced 900 different S-Box for each approach and the second round produced another 810,000 S-Box. In total, there were exactly 1,621,800 different S-Box from both approaches. In general, there are two main steps in our construction which are generating initial S-Box and proceeded by composing process. The flowchart of the construction is illustrated in figure 2.

The difference between Setting 1 and Setting 2 lies in the first step in which the initial set of S-Box was set different. In Setting 1, the initial set was generated by employing all 30 irreducible polynomials using the method introduced in section 4.1. The affine matrix and the additive constant were set the same as in the original AES S-Box. Hence from this process, there would be exactly 30 different generated S-Box. While in Setting 2, some modification was done by selecting a proper additive constant for each irreducible polynomial to remove the fixed point (FP) and the opposite fixed point (OFP). FP is defined as the mapping to itself; $S(\alpha) = \alpha$ while OFP is defines as $S(\alpha) = \bar{\alpha}$ in which $\alpha \oplus \bar{\alpha} = \mathbf{0}$. Each irreducible polynomial (IP) with its respective additive constant (AC) is shown in table 2. While figure 3 and figure 4 show the configuration of the initial set for setting 1 and setting 2 respectively. All generated initial S-Box were then stored for further use in second step.

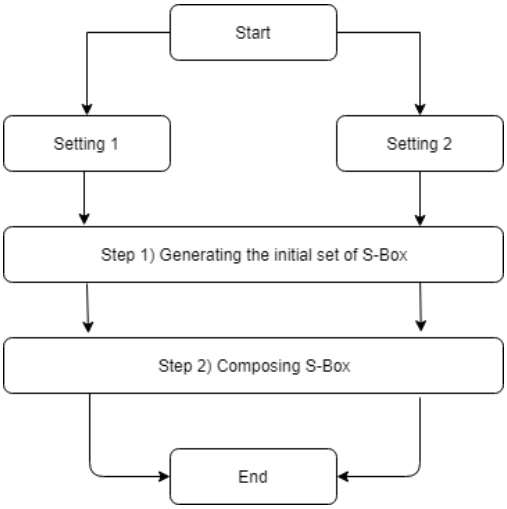

Figure 2. Flowchart of Setting 1 and Setting 2

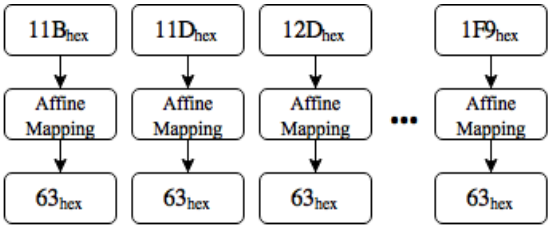

Figure 3. Setting 1 initial S-Box

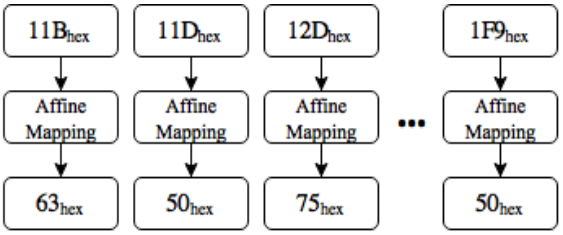

Figure 4. Setting 2 initial S-Box

The second step which is the composing process was done in a similar way for both approaches. From the first step, each setting now has 30 S-Box that acts as the initial set. The initial set was then applied two rounds of composition process. As stated before, the non-Abelian properties of symmetric

group yield two different result for different order of operation ($S_i \circ S_j \neq S_j \circ S_i$). Each S-Box from second round composition was then tested using cryptography properties mentioned in section 2. The following Algorithm 1 and Algorithm 2 show the details about the composition process for Setting 1 and Setting 2. Several variables are introduced such as $InitS, R_1S, R_2S$ which store the list of S-Box.

Table 2. List of Irreducible Polynomial with its Respective Additive Constant.

IP	AC	IP	AC	IP	AC
11B	63	169	7E	1B1	6B
11D	50	171	5A	1BD	54
12B	75	177	70	1C3	63
12D	75	17B	66	1CF	6B
139	62	187	66	1D7	C4
13F	50	18B	93	1DD	49
14D	65	18D	5F	1E7	55
15F	56	19F	7A	1F3	6E
163	3C	1A3	6D	1F5	69
165	85	1A9	80	1F9	50

Algorithm 1: 1st Round Composition

INPUT Initial Set of S-Box, $InitS$
OUTPUT Round 1 composition S-Box, R_1S

```
Call for the InitS
Set tot = 1
for i = 1 to 30
    Set a = InitS(i)
    for j = 1 to 30
        Set b = InitS(j)
        Do a composition process c = a ∘ b
        Set R1S(tot) = c
        Set tot = tot + 1
    end
end
```

Algorithm 2: Second Round Composition

INPUT 1st Round Composition R_1S
OUTPUT Round 2 composition S-Box with its cryptography properties, R_2S, N_f, δ, AD

```
Call for the R1S
Set tot = 1
for i = 1 to 30
    Set a = R1S(i)
    for j = 1 to 30
        Set b = R1S(j)
        Do a composition process c = a ∘ b
        Set R2S(tot) = c
        Set tot = tot + 1
        Test and store nonlinearity, Nf
```

```
11              Test and store differential uniformity, δ
12              Test and store algebraic degree, AD
13          end
14      end
```

5. Result and Discussion

In this section, the generated S-Box for 2nd round composition mentioned in previous section are tested using the cryptography properties defined in section 2. It follows by a comparative study between related works found in the literature. In summary both setting achieve the maximum nonlinearity $N_f = 110$ for single coordinate function. However, for the entire S-Box, the maximum achievable N_f is 106. The following Table 3 and Table 4 shows the best S-Box for Setting 1 and Setting 2 respectively.

Table 3. Setting 1 Best S-Box

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

5.1. Nonlinearity of New S-Box

In this paper, we defined the nonlinearity N_f of the S-Box as the minimum nonlinearity value that achieve by its coordinate function f_i. Therefore, the initial S-Box for Setting 1 and Setting 2 should have N_f = 112 as all coordinate function f_i achieve this value. For 2nd round generated S-Box, the value of nonlinearity ranging from 78 to 106. Similar research like in [25] state that an optimum value for strong S-Box should have $N_f \geq 100$. Our generated S-Box for Setting 1 have exactly 460,768 S-Box that have nonlinearity at least 100 while for Setting 2, about 461,050 different S-Box achieve the optimum value. Roughly, for both setting, about 57% constitute of the optimum S-Box out of 810,000 S-Box. The detail of nonlinearity distribution is shown in figure 5 and figure 6. As presented in both figure, most of the generated S-Box achieve the nonlinearity value of 100. Both setting manage to generate the highest N_f = 106 which only constituted less than 1% from total constructed S-Box. In details, there are exactly 106 and 107 S-Box that achieve N_f = 106 for setting 1 and setting 2 respectively. From our construction, we could also trace the single coordinate function that achieve $N_f = 110$. Table 5 shows in detail the nonlinearity of eight coordinate function for the best S-Box for Setting 1 and Setting 2 and the comparison with other methods of S-Box construction.

Table 4. Setting 2 Best S-Box

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

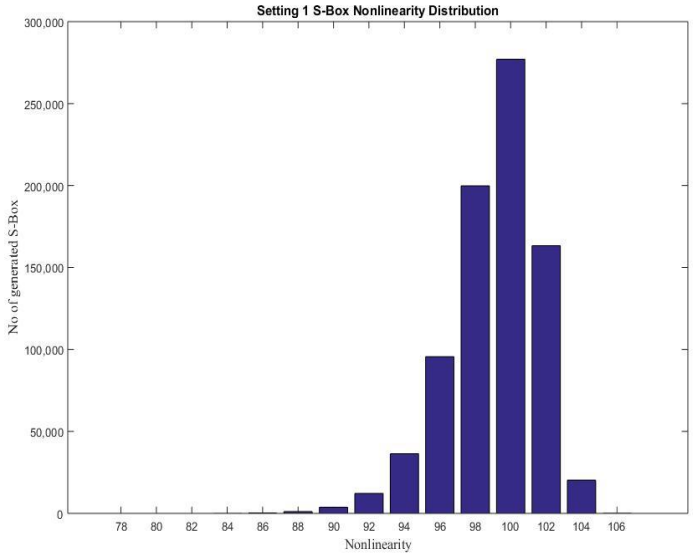

Figure 5. Setting 1 Nonlinearity Distribution

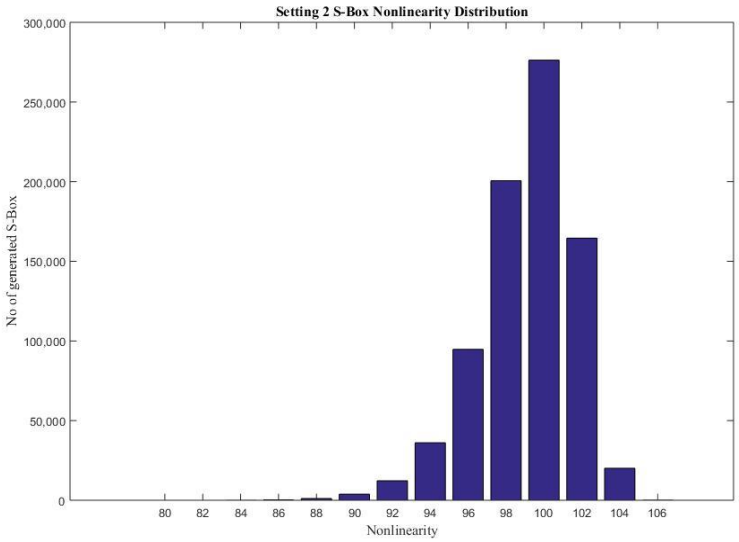

Figure 6. Setting 2 Nonlinearity Distribution

Table 5. List of S-Box Nonlinearity

Method	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	Average
AES	112	112	112	112	112	112	112	112	112
[13]	112	112	112	112	112	112	112	112	112
[23]	110	108	108	110	108	108	110	112	109.25
Setting 2	**110**	**108**	**106**	**106**	**108**	**110**	**108**	**106**	**107.75**
Setting 1	**106**	**106**	**106**	**106**	**110**	**110**	**108**	**106**	**107.25**
[24]	106	108	106	108	106	106	110	108	107.25
[25]	108	106	108	108	108	106	108	106	107.25
[12]	108	106	106	106	106	106	108	108	106.75
[26]	108	106	106	106	106	108	108	106	106.75
[18]	106	108	106	106	106	110	104	106	106.50
[9]	106	108	104	102	106	102	104	106	104.75

5.2. Differential Uniformity of New Constructed S-Box

The generated S-Box using the proposed method show a decent value of differential uniformity. Majority of the generated S-Box achieve the value 12 while the minimum achievable value is 10. Compared to original AES S-Box, the differential uniformity of our S-Box is weaker against differential cryptanalysis. However, we could show that our generated S-Box are better and comparable to most of the construction under the category of heuristic and random methods. The comparison of differential uniformity value with other constructions is summarized in Table 6.

5.3. Algebraic Degree of New Constructed S-Box

Higher algebraic degree is more favourable as it reflects the complexity of algebraic structure of the S-Box. The maximum value of algebraic degree that can be achieved by AES class S-Box is 7. Our constructed S-Box from setting 1 and setting 2 shows the maximum algebraic degree of 7. The comparison against another S-Box construction is represented in Table 6.

5.4. Fixed Point/Opposite Fixed Point

Our best constructed S-Box for Setting 1 and Setting 2 managed to get rid of the existence of fixed point ($S(\alpha) = \alpha$) and the opposite fixed point ($S(\alpha) = \bar{\alpha}$). This property also listed and summarized in Table 6.

5.5. Comparative Analysis of Different S-Box Construction

After all, we have summarized our result and perform one comparative analysis with other construction of AES class S-Box. Table 6 shows several S-Box constructions from the literature. There are four cryptographic properties that have been considered. The construction listed in the table are arranged in descending order in term of nonlinearity.

Table 6. Comparative Analysis of Different S-Box Construction

Proposed S-Box	N_f	δ	AD	FP/OFP	Technique
AES	112	4	7	0/0	Finite field inversion
[13]	112	4	7	2/2	Chaotic logistic maps in linear fractional transformation
[23]	108	8	7	0/0	Chaotic maps and composition method
Setting 1	106	10	7	0/0	Composition of permutation method
Setting 2	106	10	7	0/0	Composition of permutation method
[24]	106	4	7	2/2	Hybrid heuristic method
[12]	106	10	7	0/0	Chaotic maps and composition method
[26]	106	10	7	0/1	Chaotic system
[25]	106	12	7	1/2	Projective general linear group
[18]	104	6	7	1/1	Modified immune algorithm
[9]	102	10	7	0/0	Discrete chaos maps system
[27]	98	6	7	0/3	Tangent delay for elliptic chaotic sequence

Table 6 shows the comparison of several S-Box constructions which are arranged in descending order in term of N_f. Based on that list, the highest achievable value of nonlinearity using heuristic method is 112 through chaotic maps method. Our proposed S-Box ranked 4th and 5th based on nonlinearity level. However, several constructions with lower nonlinearity may have better δ compared to our construction. Even though the value of δ is lower, it is still comparable to some other construction. Besides that, we manage to produce our S-Box with no fixed point or opposite fixed point without modifying the affine transformation and furthermore the AD for our proposed S-Box achieve the maximum value of 7 for both setting.

6. Conclusion

The new proposed method in this paper manages to generate more than 1.6 million different S-Box with different quality. The best quality S-Box generated using the proposed method has the combination of $N_f = 112$, $\delta = 10$ and $AD = 7$. Compared to similar construction, our construction may have a stand in term of NL, and comparable value in term of DU. This simple composition method presented in this paper can be utilized in several ways which result in various quality of S-Box. Our paper just presented the composition of two different S-Box at a time with highest quality S-Box from finite field inversion acts as an initial set. It is also possible to compose more than three S-Box at a time with different of construction setting.

References

[1] P. NIST FIPS, "197: Announcing the advanced encryption standard (AES)," 2001.
[2] C. E. Shannon, "Communication Theory of Secrecy Systems.pdf," *Differ. Unif. mappings Cryptogr.*, vol. 28, no. 4, pp. 656–715, 1949.
[3] L. Jingmei, W. Baodian, C. Xiangguo, and W. Xinmei, "An AES S-box to increase complexity

and cryptographic analysis," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 1, pp. 724–728, 2005.

[4] O. Karaahmetoğlu, M. T. Sakalli, E. Buluş, and I. Tutănescu, "A new method to determine algebraic expression of power mapping based S-boxes," *Inf. Process. Lett.*, vol. 113, no. 7, pp. 229–235, 2013.

[5] M. T. Sakalli, B. Aslan, E. Buluş, A. Ş. Mesut, F. Büyüksaraçoğlu, and O. Karaahmetoğlu, "On the algebraic expression of the AES S-box like S-boxes," *Commun. Comput. Inf. Sci.*, vol. 87 CCIS, no. PART 1, pp. 213–227, 2010.

[6] L. Cui and Y. Cao, "A new S-box structure named affine-power-affine," *Int. J. Innov. Comput. Inf. Control*, vol. 3, no. 3, pp. 751–759, 2007.

[7] M. T. Tran, D. K. Bui, and A. D. Duong, "Gray S-box for Advanced Encryption Standard," *Proc. - 2008 Int. Conf. Comput. Intell. Secur. CIS 2008*, vol. 1, pp. 253–258, 2008.

[8] P. Mroczkowski, "Generating Pseudorandom S-Boxes – a Method of Improving the Security of Cryptosystems Based on Block Ciphers," *J. Telecommun. Inf. Technol.*, vol. nr 2, pp. 74–79, 2009.

[9] G. Xu, G. Zhao, and L. Min, "The design of dynamical S-boxes based on discrete chaos map system," *Proc. - 2009 IEEE Int. Conf. Intell. Comput. Intell. Syst. ICIS 2009*, vol. 2, pp. 473–478, 2009.

[10] G. Chen, "A novel heuristic method for obtaining S-boxes," *Chaos, Solitons and Fractals*, vol. 36, no. 4, pp. 1028–1036, 2008.

[11] D. Lambić, "A new discrete chaotic map based on the composition of permutations," *Chaos, Solitons and Fractals*, vol. 78, pp. 245–248, 2015.

[12] D. Lambić, "A novel method of S-box design based on chaotic map and composition method," *Chaos, Solitons and Fractals*, vol. 58, pp. 16–21, 2016.

[13] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "An efficient approach for the construction of LFT S-boxes using chaotic logistic map," *Nonlinear Dyn.*, vol. 71, no. 1–2, pp. 133–140, 2013.

[14] G. Tang, X. Liao, and Y. Chen, "A Novel Method for Designing S-boxes based on Chaotic Maps," *Chaos, Solitons & Fractals*, vol. 23, no. 2, pp. 413–419, 2005.

[15] G. Liu, W. Yang, W. Liu, and Y. Dai, "Designing S-boxes based on 3-D four-wing autonomous chaotic system," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1867–1877, 2015.

[16] Ü. Çavu and A. Zengin, "A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system," *Nonlinear Dyn.*, vol. 87, no. 2, pp. 1081–1094, 2017.

[17] G. Ivanov, N. Nikolov, and S. Nikova, "Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties," *Cryptogr. Commun.*, vol. 8, no. 2, pp. 247–276, 2016.

[18] G. Ivanov, N. Nikolov, and S. Nikova, "Cryptographically strong S-boxes generated by modified immune algorithm," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9540, pp. 31–42, 2016.

[19] S. Picek, K. Papagiannopoulos, B. Ege, L. Batina, and D. Jakobovic, "Confused by confusion: Systematic evaluation of DPA resistance of various S-boxes," in *Systematic evaluation of DPA resistance of various s-boxes. In International Conference in Cryptology in India*, 2014, pp. 374–390.

[20] H. Isa, N. Jamil, and M. R. Z. Z'aba, "Construction of Cryptographically Strong S-Boxes Inspired by Bee Waggle Dance," *New Gener. Comput.*, vol. 34, pp. 221–238, 2016.

[21] Alamsyah, A. Bejo, and T. B. Adji, "The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box," *Nonlinear Dyn.*, 2018.

[22] Alamsyah, A. Bejo, and T. Bharata Adji, "AES S-Box Construction Using Different Irreducible Polynomial and Constant 8-bit Vector," in *Dependable and Secure Computing, 2017 IEEE Conference on. IEEE, 2017*, 2017, pp. 366–369.

[23] D. Lambić, "A novel method of S-box design based on chaotic map and composition method," *Chaos, Solitons and Fractals*, vol. 58, pp. 16–21, 2014.
[24] H. Isa, N. Jamil, and M. R. Z, "Hybrid Heuristic Methods in Constructing Cryptograpgically Strong S-Boxes," *Int. J. Cryptol. Res.*, vol. 6, no. 1, pp. 1–15, 2016.
[25] Attaullah, S. S. Jamal, and T. Shah, "A Novel Algebraic Technique for the Construction of Strong Substitution Box," *Wirel. Pers. Commun.*, 2017.
[26] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," *Neural Comput. Appl.*, pp. 1–10, 2017.
[27] A. Hussain Alkhaldi, I. Hussain, and M. A. Gondal, "A novel design for the construction of safe S-boxes based on TD ERC sequence," *Alexandria Eng. J.*, vol. 54, no. 1, pp. 65–69, 2015.