

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/338444793>

Design a Compact Non-linear S-Box with Multiple-Affine Transformations

Chapter · January 2020

DOI: 10.1007/978-3-030-38752-5_34

CITATIONS

0

READS

38

4 authors, including:



Omar A. Dawood
University of Anbar

22 PUBLICATIONS 55 CITATIONS

[SEE PROFILE](#)



Mohammed Khalaf
Al-Maarif University College

23 PUBLICATIONS 26 CITATIONS

[SEE PROFILE](#)



Hussein Almula
University of South Carolina

3 PUBLICATIONS 5 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:







Design a New Standard Model of Block Cipher (Symmetric Algorithm) Based on NIST Criteria [View project](#)



Developing A New Cryptosystem Model Based on Magic Cube Notations [View project](#)



Design a Compact Non-linear S-Box with Multiple-Affine Transformations

Omar A. Dawood¹ , Mohammed Khalaf² ,
Falath M. Mohammed³ , and Hussein K. Almulla¹ 

¹ College of Computer Science & IT, University of Anbar, Ramadi 31001, Iraq

Omar-Abdulrahman@uoanbar.edu.iq,
the_lionofclub@yahoo.com,
hu_albasri@yahoo.co.uk

² Department of Computer Science, Al-Maarif University College,
Ramadi, Anbar 31001, Iraq

M. I. Khalaf@acritt.org.uk

³ College of Education for Humanities Sciences, University of Anbar,

Ramadi, Anbar 31001, Iraq
falathm@yahoo.com

Abstract. The present paper introduces a new method of S-Box construction which work as a byte-oriented substitution scheme. The S-Box design considers the core part for the building most block cipher algorithms and play a major role in generating confusion property. Modern ciphers build with different types of S-Box of half-byte (nibble of 4-bit) or full-byte 8-bit as lookup tables with distinct mathematical Boolean functions (BFs). The proposed method generates the S-box based on multiplications of multiple different affine transforms with multiple distinct overlapped vectors of 8-bit to achieve high nonlinearity. The construction of S-box focused on use an irreducible polynomial of order eight over Galois Field GF(2⁸). The proposed S-box quit similar to the S-box of Advance Encryption Standard (AES) but with more algebraic complexity and high non-linearity factor.

Keywords: S-box · Strict Avalanche Criterion (SAC) · Affine transform · Confusion property · Galois fields GF(2⁸) · Nonlinearity

1 Introduction

Numerous symmetric block ciphers are concentrated on the Shannon definition for the confusion and diffusion properties. Where the confusion is generated by the substitution process through complicating the correlation between the ciphering key and the ciphertext as complex as possible. Whilst the diffusion property distributes the statistical of plaintext along the resultant ciphertext [1]. The confusion and diffusion properties together increase the cipher complexity over the round transformation via recursive series of substitutions and permutations processes. The substitution means the alteration part of bits or word with other different part. Permutation process refers to the dissipate the sequence of bit regarding to specific arrangement [2].

To make the plaintext are more sophisticate on the one hand non-consistency it is need to spread the plaintext along the statistics of structure. The construction of a new S-box is a necessary issue in designing any secure and robust cryptosystem. Since the design process may be different form cipher to cipher according to the design process. Some S-boxes are built randomly and other mathematically as a fixed lookup table or as a dynamic generation of on-fly method [3]. The designer must realize that the most important part in the algorithm design is the S-box that provide non-linearity. Also, the designer must aware that the S-box construction is not only random values or chaotic numbers. Thus, the design S-boxes can be considered as a mathematical built according to certain context likewise Boolean functions, affine functions, and non-linear equations. The block cipher algorithms based on the non-linearity notation to secure the round transformation [4]. This paper introduces a compact S-box that focused on algebraic design and shows how it achieves the resistance against the most well-known attacks. The present design based on several previous published algorithms that have had a significant impact in terms of internal mathematical design and construction steps which can be viewed in [5–7] respectively.

The proposed S-box contains three levels of affine layering and encapsulated Boolean polynomial with different non-linear equations XORed with multiple of distinct vectors that are responsible for confusion generation. The imposed vectors represent an effective impact on the implementation as well as the protection aspects.

This paper has discussed the general background of the substitution layer and the rest of paper is organized into following sections. Section 2 states the related works to the proposed S-box by other researchers. Section 3 introduces the mathematical preliminaries for S-box design and the basic adopted criteria for design strategy. Section 4 includes most popular approaches of S-box construction and the design methodologies. Section 5 applies the proposed S-box design and the main principles for algebraic construction. The security analysis and the investigated results can be shown in Sect. 6. Section 7 Includes the conclusions of this research.

2 Related Works

In this part some related works have been searched and reported by several researchers with modern methods that are so far related to the proposed method, which will be discussed in the section.

In 2016, Rodinko et al. [8], they have introduced a new method for generating S-box with high non-linearity based on appropriate selected criteria. The enhanced generation method reduces the consuming energy for the generated S-box through the generating process and gives a reasonable implementation. The improved method involves minimizing the time checking for the S-box selected criteria through design process.

In 2017, Alamsyah et al. [9], they have proposed a new cryptographic approach based on usage a different mathematical irreducible polynomial of $m(x) = x^8 + x^6 + x^5 + x + 1$ and a distinct constant vector of 8-bit with binary notation (00000001). The enhanced S-box has been evaluated by numerous effective tests via different security criteria likewise SAC, BIC nonlinearity and other criteria. The developed

S-box provides a good security level compared to other popular S-boxes according to the author's claim. The resultant tests stated that the developed S-box is bijective and balance Boolean function.

In 2017, Gomes and Moreno [10], They presented a compact S-box implementation for Twofish cipher by adopted Altera Quartus Cyclone board. The introduced labor characterized by less amount of logical circuit design compared with original design. The main objective behind the design notation is to extend the implementation to a large scope of applications with Field Programmable Gate Array (FPGA) technique. The author plans to adopt this work as a part of big project for customizing the utilization as alternation for the AES cipher.

In 2019, Zahid et al. [11], have been developed a new technique for construction a modern Substitutes-boxes based on Cubic Fractional Transformation (CFT). The strength of the intended S-box was evaluated and assessed by several significant criteria. The authors claimed that the present S-box achieves good results and can be used as a strong S-box for the most modern block cipher algorithms.

3 Mathematical Preliminaries

The present section explains the main notations and comprehensions for the cryptographic mathematical functions. The mathematical guide for the S-box design includes knowledge some Boolean functions with non-linear equations. The S-box is a critical part for the SPN structure since it is the only non-linear part in the algorithm's stages. A large number of S-Box design methods are available with different mathematical notations. Some of the popular methods depend on preprocessing approach for the construction the nonlinear layer. Other methods depend basically on affine transformations with multiplicative inverse. The S-box of AES cipher is considered as a benchmark S-box which inspired by several posterior algorithms. The AES cipher was adopted a new mathematical idea that focuses on wide trail strategy where each part has its own function independently [12]. Thus, the S-box construction comprises 8-bit multiplicative inverse under irreducible polynomial of order eight followed by 8*8 binary affine transform. The calculation of multiplicative inverse on $GF(2^8)$ which requires to be addressed in composite field. An isomorphic mapping function $f(x) = x*y$ with two sides-inverses that is bijective under the set of elements is required to represent the polynomial. The incoming entry polynomial is multiplied and computed under the multiplicative inverse, thereafter, the affine transform is computed and the resultant XORed with constant vector [13].

Let $S = ()$ a non-linear sub-byte transformation with $x \times y$ and the $f(i)$ is a Boolean function from x variables x_1, x_2, \dots, x_n . The affine with multiple equations acts as $S(x) = A(P(x))$ that mapping over the $GF(2^8)$ as an $x * y$ S-box of a non-linear mapping $GF(2)^n \rightarrow GF(2)^n$. Let $w \in \{0, 1\}^n \setminus \{0\}$, $z \in \{0, 1\}^m$. The XORed table entry of an S-box S corresponding to $(w * z)$ is $XOR(w, z) = \#\{x \in \{0, 1\}^n : S(x) \oplus S(x \oplus v1) \oplus S(x \oplus v2) \oplus S(x \oplus v3) = z\}$ where $\#$ is the cardinality in algebraic set with multiple affine. The input polynomial for the internal function is mixed with ciphering key to generate the sub-keys dependent S-boxes. Where each S-box involves p of 8-bit fixed permutation powered with multiple affine which ultimately

XORed with specific ciphering key. If the ciphering key with length of 128-bit the key dependent S-box will be as follows

$$\begin{aligned}y_0 &= s_0(A_0) = p_1 [p_2 [p_3 [A] \text{ XOR } s_0, 0] \text{ XOR } s_1, v_0] \\y_1 &= s_1(A_1) = p_1 [p_2 [p_3 [A] \text{ XOR } s_0, 1] \text{ XOR } s_1, v_1] \\y_2 &= s_2(A_2) = p_1 [p_2 [p_3 [A] \text{ XOR } s_0, 2] \text{ XOR } s_1, v_2] \\y_3 &= s_3(A_3) = p_1 [p_2 [p_3 [A] \text{ XOR } s_0, 3] \text{ XOR } s_1, v_3]\end{aligned}$$

The S-box construction is built according to different Boolean functions as a bent function that gives a high nonlinearity for the S-box. Suppose the bent function termed as $S : \{0, 1\}^n \rightarrow \{0, 1\}^m$ where m for even number can be considered equal to one. From another perspective, it is simple to produce two functions $g(x)$ and $f(x)$ and proof these two functions are belong to the same class if $g(\vec{x}) = (f(Ax + b))$. In case with two S-boxes the Boolean function will be depicted as $S_2(x) = B(S_1(A(x) + a)) + b$. The opposite implementation for the multiple affine transform can be summarized by the following mathematical formula:

$$\begin{aligned}{}^{-1}y_0 &= s_0(A_0) = p_1^{-1} [p_2^{-1} [p_3^{-1} [A] \text{ XOR } s_0,0] \text{ XOR } s_1,0] \\{}^{-1}y_1 &= s_1(A_1) = p_1^{-1} [p_2^{-1} [p_3^{-1} [A] \text{ XOR } s_0,1] \text{ XOR } s_1,1] \\{}^{-1}y_2 &= s_2(A_2) = p_1^{-1} [p_2^{-1} [p_3^{-1} [A] \text{ XOR } s_0,2] \text{ XOR } s_1,2] \\{}^{-1}y_3 &= s_3(A_3) = p_1^{-1} [p_2^{-1} [p_3^{-1} [A] \text{ XOR } s_0,3] \text{ XOR } s_1,3]\end{aligned}$$

The cryptographic power of any S-box is critically assessment unless it was satisfying the important metrics of S-box design. The most important criteria for the design black box include the mathematical functions for the S-box built. Thus, good S-box must be met the essential metrics for the Boolean functions represented by: bijection, nonlinearity, bit independence criterion, strict avalanche effect, and linear and differential approximation probabilities [14].

1. **Bijection Criteria:** is a class of mathematical function that represents two sets where the element in one set is correspondence to the other element in other set as one-to-one relation. If the S-box $n*n$ then the relation will be pair of related vectors one for input vector of n -bit into m -bit of the mirror in out vector.
2. **Strict-Avalanche Criterion:** is a desirable metric for the measuring the strength of S-box where small change in input vector propagate with a high change in output vector reach to half probability change. The design step will need function dependency on input vector with 50% to have a significant avalanche effect on output vector.
3. **Bit-Independence Criterion:** The Bit-independence concept depicts the immunity of coefficients correlation between the input and output streaming bits. It declares the extent to which outputs i th and j th string bits are affected and changed independently when any change in k th of input bits.
4. **Nonlinearity Criterion:** The non-linearity property states the strength of the mathematical function in S-box design against the differential cryptanalysis. It

prevents the S-box to be mapped linearly from input vector to the output vector. If the S-box is built with high nonlinearity it will ensure high resistance in a linear approximation for the bent function and the affine parameters. The nonlinearity is bounded as an immune procedure against linear cryptanalysis and enhanced the security margin for the cipher.

5. **Balance Criterion:** the balance metric is responsible for balance in Boolean vector where the Boolean function has an equal number of zeros and ones. The importance of balance criterion is to make the cipher hard in terms of attacks. The balance property is highly desired metric for the strong S-box, since it ensures that the bent function cannot be approximated by fixed operations [15, 16].

4 The S-Box Design Methodologies

The power of the cipher design influences by the measure of confusion that generated in the ciphertext. Thus, the strength of the cryptographic block cipher depends heavily on the nature of S-Box design and the type of generation approaches.

1. **Random S-box:** several researchers and designers investigated and searched for long times to design numerous methods for designing various S-boxes. A large number of these methods were random S-boxes generation. The random S-box produces an acceptable security level because it uses a diverse S-boxes per each key. Random S-box is a method that uses different techniques in generation process that withstanding against major of cryptanalysis attacks. Randomness principle give a high computational complexity and has no fixed points of reverse reconstruction steps. Thus, the random s-box is difficult to exploit from the internal structure since it depends on various S-boxes of derived-key for each round [17].
2. **Random with Testing S-box:** Random S-box exhibits a good alternative for the S-box generation process since it has no subject to the underlying pattern that can be exploited in cryptanalysis. The random with testing method depends on pre-selection of the entry input values which have been tested according to different criteria. The resultant of tested output data selects the data those with good features and discard those fail to pass the threshold of testing. Random with Testing S-box is very similar to the random S-box except it contains some pre-computational operations [18].
3. **Human-Base S-box:** S-box is generated by a manual method accompanied with simple mathematical operations this type of design is suitable only for small S-box. In case of large S-box this method would be lossless and uncompact [19].
4. **Mathematical-Base:** S-box is generated according to the mathematical base and algebraic structure. Many researchers have designed and discovered methods for building new benchmarks of strong S-Boxes and investigate their strength against some cryptanalysis attacks. such Strict Avalanche Criterion (SAC), Linear Probability (LP), as Non-linearity (NL), Differential Probability (DP), Bijection and bit Independence Criterion (BIC), and etc. [20].

5 The Proposed S-Box Design

The proposed S-box has been designed with multiple mathematical affine equations. It has put some additional conditions on the non-linear layer of a sub-byte stage that will enhance the avalanche and completeness comprehensions for the intended S-box. In addition, the imposed S-box is developed to fulfill the critical criteria of the best strong ciphers' structures.

5.1 Non-linear Substitution Transformation

The sub-byte layer will be the most discriminating part of the design strategy, as a result, its size and construction process significantly influence the whole algorithm. The S-Box construction contains three affine equations with their convenient vectors. The construction of the forward S-Box basically depends on the following steps, the first step by taking the multiplicative inverse of all tables' of 256 values according to the new irreducible polynomial. $m(x) = x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$. The second step applying the first affine (F1) transform and the outcome XORed with the first constant vector (V1) represented by the value (87) in hex notation as shown in Eq. (1). After that repeated the process with second affine (F2) transform and the result XORed with the second constant vector (V2) that is represented by the value (2B) as stated in Eq. (2). Eventually, repeated the process with third affine (F3) transform and the outcome makes a bit-wise exclusive-OR with the third constant vector (V3) that represented by the value (3D) as stated in Eq. (3). as it explained in Table 2.

$$P \rightarrow M\text{-inverse}(P) \text{ mod } m(x) \text{ where } m(x) \text{ is an irreducible polynomial.}$$

- The first affine equation (F1)
- The first Inv-affine equation (F1')
- The first vector (V1)
- The first Inv-vector (V1')
- The second affine equation (F2)
- The second Inv-affine equation (F2')
- The second vector (V2)
- The second Inv-vector (V2')
- The third affine equation (F3)
- The third Inv-affine equation (F3')
- The third vector (V3)
- The third Inv-vector (V3')

Suppose (A), (X) and (M) are 1st, 2nd and 3rd forward Affine matrices respectively with (8*8) dimension and in another side (B), (Y) and (N) the inverse (Backward) affine matrices respectively. Let (C), (Z) and (S) forward XORed vectors and (CC), (ZZ), and (SS) can be considered as the corresponding backward vectors respectively to make the forward and backward compatible and the whole operations are reversible as stated in Table 1. All these interrelated matrices and the vectors values have been computed mathematically and inaccurately.

Table 1. Non-linear affine of transform matrices with their vectors

Polynomial arrays	Forward matrix	Backward matrix	XORed forward vector	XORed inverse of backward vector
Affine Matrix1	A	B	C	CC
Affine Matrix2	X	Y	Z	ZZ
Affine Matrix3	M	N	S	SS

$$\text{Ciphertext (C)} = (\text{F3}(\text{F2}(\text{F1}(\text{P}) \oplus \text{V1}) \oplus \text{V2}) \oplus \text{V3})$$

Let (V) the entry vector which we want to encrypt it.

$$\mathbf{A} * \mathbf{B} = \mathbf{I}$$

$$\mathbf{X} * \mathbf{Y} = \mathbf{I}$$

$$\mathbf{M} * \mathbf{N} = \mathbf{I}$$

Where (I) is an Identity matrix

Forward Operations: Where F1, F2, and F3 represent the three functions or levels of affine transform and P1, P2 and P3 refer to the initial entry for the plaintext in each layer of affine mapping equations respectively.

$$\mathbf{F1} = \mathbf{A} * [\mathbf{V}] \oplus \mathbf{C}$$

$$= \mathbf{AV} \oplus \mathbf{C}$$

$$\mathbf{F2} = \mathbf{X} * [\mathbf{P1}] \oplus \mathbf{Z}$$

$$= \mathbf{X} * [\mathbf{AV} \oplus \mathbf{C}] \oplus \mathbf{Z}$$

$$= \mathbf{XAV} \oplus \mathbf{XC} \oplus \mathbf{Z}$$

$$\mathbf{F3} = \mathbf{M} * \mathbf{P2} \oplus \mathbf{S}$$

$$\mathbf{F3} = \mathbf{M} * [\mathbf{XAV} \oplus \mathbf{XC} \oplus \mathbf{Z}] \oplus \mathbf{S}$$

$$= \mathbf{MXAV} \oplus \mathbf{MXC} \oplus \mathbf{MZ} \oplus \mathbf{S}$$

Ex. Let the Input vector $b = 13$

$$\mathbf{A} * 13 \oplus \mathbf{C} = \mathbf{B0}$$

$$= \mathbf{B0} * \mathbf{X} = \mathbf{EA} \oplus \mathbf{Z} = \mathbf{C1}$$

$$= \mathbf{C1} * \mathbf{M} = \mathbf{D5} \oplus \mathbf{S} = \mathbf{E8}$$

$$b' \begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = A \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} * b \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \oplus C \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \tag{1}$$

$$b'' \begin{bmatrix} b''_0 \\ b''_1 \\ b''_2 \\ b''_3 \\ b''_4 \\ b''_5 \\ b''_6 \\ b''_7 \end{bmatrix} = X \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} * b' \begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} \oplus Z \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \tag{2}$$

$$b''' \begin{bmatrix} b'''_0 \\ b'''_1 \\ b'''_2 \\ b'''_3 \\ b'''_4 \\ b'''_5 \\ b'''_6 \\ b'''_7 \end{bmatrix} = M \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} * b'' \begin{bmatrix} b''_0 \\ b''_1 \\ b''_2 \\ b''_3 \\ b''_4 \\ b''_5 \\ b''_6 \\ b''_7 \end{bmatrix} \oplus S \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \tag{3}$$

Table 2. Forward proposed S-box

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

5.2 Non-linear Substitution Transformation

The inverse of the proposed S-box is constructed by applying the reverse steps of the forward procedure. Firstly, mapping the inverse of the third affine transform XORed with the corresponding Inv-vector that is represented by (73) in hex representation as it is shown in Eq. (4). Secondly mapping the inverse of the second affine transform XORed with the corresponding Inv-vector that represented by (F6) as shown in Eq. (5). Finally, mapped the first affine transform XORed with the corresponding Inv-vector that represented by (3C) as it is clarified in Eq. (6) and the outcome has taken by the multiplicative inverse according to the irreducible polynomial and consequently the backward or InvS-Box as shown in Table 3. The rational clue for the user more constant vectors is to increase the complexity of the S-box and make it difficult computationally, in addition, to eliminating any fixed point of tractable computation respectively. The following are the mathematical proof that represents the backward operations details and the underlined terms indicate either to a null operation or identity operation.

Backward Operation: where the (F1', F2' and F3') are the three inverse process or Functions

$$\text{Plaintext (P)} = (\mathbf{F1}'(\mathbf{F2}'(\mathbf{F3}'(\mathbf{P}) \oplus \mathbf{V3}) \oplus \mathbf{V2}) \oplus \mathbf{V1})$$

$$\mathbf{F3}' = \mathbf{N} * [\mathbf{MXAV} \oplus \mathbf{MXC} \oplus \mathbf{MZ} \oplus \mathbf{S}] \oplus \mathbf{SS}$$

$$= \underline{\mathbf{NMXAV}} \oplus \underline{\mathbf{NMXC}} \oplus \underline{\mathbf{NMZ}} \oplus \underline{\mathbf{NS}} \oplus \underline{\mathbf{SS}}$$

$$= \mathbf{XAV} \oplus \mathbf{XC} \oplus \mathbf{Z} \oplus \text{Null}$$

$$\mathbf{F2}' = \mathbf{Y} * [\mathbf{XAV} \oplus \mathbf{XC} \oplus \mathbf{Z}] \oplus \mathbf{ZZ}$$

$$= \underline{\mathbf{YXAV}} \oplus \underline{\mathbf{YXC}} \oplus \underline{\mathbf{YZ}} \oplus \underline{\mathbf{ZZ}}$$

$$\mathbf{AV} \oplus \mathbf{C} \oplus = \text{Null}$$

$$\mathbf{F1}' = \mathbf{B} * [\mathbf{AV} \oplus \mathbf{C}] \oplus \mathbf{CC}$$

$$\underline{\mathbf{BAV}} \oplus \underline{\mathbf{BC}} \oplus \underline{\mathbf{CC}}$$

$$= \mathbf{V} \oplus \text{Null}$$

$$= \mathbf{V} \rightarrow (\text{The Original Vector})$$

$$\text{Let the Input Vector} = \mathbf{E8}$$

$$\mathbf{N} * \mathbf{E8} = \mathbf{B2} \oplus \mathbf{SS} = \mathbf{C1}$$

$$= \mathbf{C1} * \mathbf{Y} = \mathbf{46} \oplus \mathbf{ZZ} = \mathbf{B0}$$

$$= \mathbf{B0} * \mathbf{B} = \mathbf{2F} \oplus \mathbf{CC} = \mathbf{13}$$

$$b'' \begin{bmatrix} b''_0 \\ b''_1 \\ b''_2 \\ b''_3 \\ b''_4 \\ b''_5 \\ b''_6 \\ b''_7 \end{bmatrix} = \mathbf{N} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} * b''' \begin{bmatrix} b'''_0 \\ b'''_1 \\ b'''_2 \\ b'''_3 \\ b'''_4 \\ b'''_5 \\ b'''_6 \\ b'''_7 \end{bmatrix} \oplus \mathbf{SS} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad (4)$$

$$b' \begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = Y \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} * b'' \begin{bmatrix} b''_0 \\ b''_1 \\ b''_2 \\ b''_3 \\ b''_4 \\ b''_5 \\ b''_6 \\ b''_7 \end{bmatrix} \oplus ZZ \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \tag{5}$$

$$b \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = B \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} * b' \begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} \oplus CC \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \tag{6}$$

Table 3. Backward proposed S-box

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

6 Security Analysis and Experimental Results

In this section, the main themes will be discussed and the pros and cons of the proposed S-box will be diagnosed from the point of view of cryptography aspects. The proposed S-box characterized with an organized internal structure that tends to be balanced and non-sacrifice. The “balanced term means that the algorithm has an elegant step with the same execution time in encryption & decryption processes in opposite to the AES cipher that suffers from some delay in decryption with embedded devices. The modern design for the non-linear stage or S-box built does not need to construct with three tables in

forward and the same in backward or to enlarge it with a big size on the account of memory and the hardware requirements. So the S-Box has been reduced to work only with one table in encryption and its inverse for decryption and supported by three correlated affine transforms to defeat the algebraic, interpolation and large range attacks.

We have experimented the construction of S-Box with all equations of the irreducible polynomial (30 equations of degree 8) see ref [21] and there have gotten thirty different of new S-box tables with their inverses. The designers aware to the idea that the design process with three affine is equal to that one affine in term of S-box design but in fact, the design of S-box with three affine gives a completely different of hex-values distribution map compared with single affine overall 30 irreducible equations. The enhanced S-box is designed to face and overcomes the linear and differential attacks as well as to consume the same execution time for encryption and decryption in order to eliminate the timing attacks and to combat the power analysis attack. The last part in the round transformation that plays an important role in security strength is the key-dependent S-box algorithm that is responsible for the sub-keys scheduling, which acts the nerve of the proposed model and should be kept secret. The Related-key attacks almost not effective (even if the $2^{99.5}$ chosen plaintext/cipher text value all the consideration about it still theoretical entirely and was not from evaluation criteria during the AES selection. The complexity of the brute force attack is appraised by 2^{k-1} encryptions. The attacker is unable to estimate or reconstruct the algebraic equations from the deduced information hence, each stage built separately and the algebraic attack becomes very hard.

The basic challenges of building steps for the proposed S-box till now, that it has the same as the AES structure where the encryption and decryption processes do not completely utilize the self-stages since the inverses of S-box and linear mapping have to be executed separately. The proposed S-box has been checked by several statistical analytical tests and exhibited accepted implications. Understanding the strength and weakness of any algorithm gives a good conception of the algorithm but the evaluation and assessment of algorithm construction are not easy. Since it includes the algebraic and statistical analysis and may be the hardware implementation. So many tools have been developed by companies and individual developers and released on the internet to use in measuring and evaluating the algorithms according to several important metrics. But each of these tools gave differentiate results from each other and none of them provides accurate measurements, thus; there are no uniformly standard criteria in evaluation and analysis.

The analysis and the assessment of the proposed S-box also comprise the algebraic characteristics for the internal structure between the suggested S-box and the AES S-box from several factors for each stage in the round transformation as it is shown in Table 4. The intended S-box showed great similarities in characteristics and qualities with S-box of AES cipher but with more complexity and non-linearity criteria.

- **The Algebraic Complexity:** is the study of the minimum number of operations sufficient to perform various computations. It can be seen that there are 9 for S-box and 253 nonzero coefficients involved in algebraic expression for the AES S-box coefficients, but with the triple affine the count of algebraic raise from 9 to 253 and the inverse S-box stays 255, which enhances the capability of the S-box so as to face algebraic attack and interpolation attack.

- **Non-linearity property:** refers to the weight of the lowest weight nonzero Hadamard coefficient that is equal to the nonlinearity. Therefore, the nonlinearity of the proposed S-box with the upper bound is 114. Thus. This factor tends to be solid to defeat the effectively linear cryptanalysis.
- **The Differential Uniformity:** is a mapping of values for every non-zero input difference and any output difference with the number of possible inputs that has a uniform upper bound. Therefore, there are only four values in uniform mapping form. It is clear that the proposed S-box is differential with 4 uniformity, which makes the differential cryptanalysis very hard.

Table 4. Algebraic comparison between the S-box of AES and the proposed S-box

Algebraic properties	Proposed S-box	AES cipher
Correlation immunity property	Zero	Zero
Algebraic degree property	Seven	Seven
Algebraic complexity property	252/255	9/255
Bijection property	Yes	Yes
Strict avalanche criteria (SAC)	1/2	1/2
Non-linearity property	113	112
Differential uniformity property	4	4
Power mapping property	By-Three affine	By-One affine
S-box dependency property	Yes	Yes
Key scheduling property	Yes	Yes

7 Conclusions

A new compact and adaptable S-box that based on a new design strategy with multiple affine transforms has been constructed. The essence of design lies in increasing the confusion of the algorithm and enhancing the key dependent S-box. The suggested S-box characterized by high non-linearity and maximize algebraic complexity to encounter the cryptanalytic attacks. The design scheme is to defeat the linear and differential attacks and to reinforce the security metric. The proposed S-box has been tested by different assessment tests according to various irreducible polynomials and it has been applied an accepted result. Finally, the proposed S-box can be adopted as a compact S-box for the modern block cipher algorithms with multi-security layers.

References

1. Dragomir, I.R., Lazăr, M.: Generating and testing the components of a block cipher. In: Proceedings of the 8th International Conference on Electronics, Computers and Artificial Intelligence, IEEE, ECAI 2016, pp. 1–4 (2017). <https://doi.org/10.1109/ecai.2016.7861190>
2. Lin, Z.: Diffusion and confusion of chaotic iteration based hash functions. In: International Conference on Embedded and Ubiquitous Computing (EUC) and 15th International

- Symposium on Distributed Computing and Applications for Business Engineering (DCABES). IEEE, pp. 444–447 (2016)
3. Du, Z.Q., Xu, Q.J., Zhang, J., Li, M.: Design and analysis of dynamic S-box based on Feistel. In: Proceedings of 2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference, IAEAC 2015, pp. 590–594. IEEE (2016). <https://doi.org/10.1109/iaeac.2015.7428622>
 4. Agrawal, D.P., Wang, H., Dey, S., Ghosh, R.: A review of cryptographic properties of 4-bit S-boxes with generation and analysis of crypto secure S-boxes. In: Computer Cyber Security, pp. 527–555 (2019). <https://doi.org/10.1201/9780429424878-20>
 5. Dawood, O.A., Rahma, A.M.S., Abdul Hossen, A.M.J.: The new block cipher design (Tigris Cipher). *Int. J. Comput. Netw. Inf. Secur.* **7**(12), 10–18 (2015)
 6. Dawood, O.A., Rahma, A.M.S., Abdul Hossen, A.M.J.: New symmetric cipher fast algorithm of reversible operations' queen (FAROQ) cipher. *Int. J. Comput. Netw. Inf. Secur.* **9**, 29–36 (2017)
 7. Dawood, O.A., Rahma, A.M.S., Mohssen, A., Hossen, J.A.: The euphrates cipher. *IJCSI Int. J. Comput. Sci.* **12**(2), 154–160 (2015)
 8. Rodinko, M., Oliynykov, R., Gorbenko, Y.: Optimization of the high nonlinear S-boxes generation method. In: Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), vol. 70, pp. 93–105. in Tatra Mountains Mathematical Publications (2017)
 9. Alamsyah Bejo, A., Adji, T.B.: AES S-box construction using different irreducible polynomial and constant 8-bit vector. In: 2017 IEEE Conference on Dependable and Secure Computing, pp. 366–369 (2017). <https://doi.org/10.1109/desec.2017.8073857>
 10. Gomes, O.D.S.M., Moreno, R.L.: A compact S-box module for 128/192/256-bit symmetric cryptography hardware. In: Proceedings - 2016 9th International Conference on Developments in eSystems Engineering, DeSE 2016, pp. 94–97 (2017). <https://doi.org/10.1109/dese.2016.17>
 11. Zahid, A.H., Arshad, M.J., Ahmad, M.: A novel construction of efficient substitution-boxes using cubic fractional transformation. *Entropy* **21**, 245 (2019)
 12. Dawood, O.A., Hammadi, O.I., Asman, T.K.: Developing a new secret symmetric algorithm for securing wireless applications. In: Proceedings - 2018 1st Annual International Conference on Information and Sciences, AiCIS 2018, pp. 152–157 (2019). <https://doi.org/10.1109/aicis.2018.00038>
 13. Shreenivas Pai, N., Raghuram, S., Chennakrishna, M., Karthik, A.S.V.: Logic optimization of AES S-Box. In: International Conference on Automatic Control and Dynamic Optimization Techniques, ICACDOT 2016, pp. 1042–1046 (2017). <https://doi.org/10.1109/icacdot.2016.7877745>
 14. Dawood, O.A., Sagheer, A.M., Al-Rawi, S.S.: Design large symmetric algorithm for securing big data. In: Proceedings - International Conference on Developments in eSystems Engineering, DeSE 2018-September, pp. 123–128 (2019)
 15. Cui, L., Cao, Y.A.: New S-box structure named affine-power-affine. *Int. J. Innov. Comput. Inf. Control* **3**, 751–759 (2007)
 16. Lee, J., et al.: Avalanche and bit independence properties of photon-counting double random phase encoding in gyrator domain. *Curr. Opt. Photon.* **2**(4), 368–377 (2018)
 17. Lambi, D., Živkovi, M.: Comparison of random S-Box generation methods. *Publications DE L'Institute Mathematique Nouvelle série* **93**(107), 109–115 (2013)
 18. Mroczkowski, P.: Generating pseudorandom S-boxes – a method of improving the security of cryptosystems based on block ciphers. *J. Telecommun. Inf. Technol.* **2**, 74–79 (2009)
 19. Ivanov, G., Nikolov, N., Nikova, S.: Cryptographically strong s-boxes generated by modified immune algorithm. In: Pasalic, E., Knudsen, L.R. (eds.) *BalkanCryptSec 2015*.

- LNCS, vol. 9540, pp. 31–42. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-29172-7_3
20. Sagheer, A.M., Al-Rawi, S.S., Dawood, O.A.: Proposing of developed advance encryption standard. In: Proceedings - 4th International Conference on Developments in eSystems Engineering, DeSE 2011, pp. 197–202 (2011). <https://doi.org/10.1109/dese.2011.74>
 21. Baylis, J., Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge (1988). Math. Gaz. 72, 335