A New Improved AES S-box With Enhanced Properties

Abderrahmane Nitaj[1], Willy Susilo[2], and Joseph Tonien[2]

[1] LMNO, University of Caen Normandie, France
abderrahmane.nitaj@unicaen.fr
[2] Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Australia
{willy.susilo,joseph.tonien}@uow.edu.au

Abstract. The Advanced Encryption Standard (AES) is the most widely used symmetric encryption algorithm. Its security is mainly based on the structure of the S-box. In this paper, we present a new way to create S-boxes for AES and exhibit an S-box with improved cryptographic properties such as Bit Independence Criterion (BIC), periodicity, algebraic complexity, Strict Avalanche Criterion (SAC) and Distance to SAC.

1 Introduction

The Advanced Encryption Standard (AES) [13] is the main and widely used symmetric cryptosystem. It was standardized by NIST in 2000 in replacement of DES [7]. AES is a Substitution Permutation Network (SPN) which is based on a non-linear substitution layer and a linear diffusion layer. The non-linear layer is represented by a 16×16 S-box which is a permutation of the Galois finite field $\mathbb{F}_{2^8}$. The design of the S-box is a challenging task since the security of AES is mainly based on its structure. A strong S-box should satisfy several cryptographic criteria to resist the known cryptanalytic attacks, such as linear cryptanalysis [12] and differential cryptanalysis [1]. Although AES is resistant to linear and differential attacks, it presents some weaknesses in regards with a variety of cryptanalytic criteria. A typical example is that an S-box should have high algebraic degree when expressed as a polynomial. The AES S-box has algebraic degree 254 with only 9 monomials which is very simple [11]. Another weak criterion for the AES S-box is that some elements of $\mathbb{F}_{2^8}$ have short iterative periods as it is the case with $S^2(0x73) = 0x73$, $S^{27}(0xfa) = 0xfa$, $S^{59}(0x00) = 0x00$, $S^{81}(0x01) = 0x01$, and $S^{87}(0x04) = 0x04$ (see [5]). One more weak criterion for the AES S-box is the distance to SAC (Strict Avalanche Criterion) which is evaluated to 432 [5] while it should be as small as possible. Yet another example of the weakness of the AES S-box is its affine transformation period [16,5]. It is equal to 4 which is very low in comparison with the optimal value 16.

In the literature, various techniques and tools have been proposed to create strong S-boxes for AES (see [20,21,9,10,15,17,5] for various constructions of S-boxes). In most cases, the proposed S-box is based on a bijective function on

$\mathbb{F}_{2^8}$ with an explicit formulae. In AES [13], the S-box is a 16×16 table of bytes obtained by a function of the form $f(x) = Ax^{-1} + b$ where, for $x \neq 0$, x^{-1} is the inverse of x in $\mathbb{F}_{2^8}$, and $0^{-1} = 0$, and where A is a 8×8 a circular matrix of bits and $b = 0x63$. In [5], the proposed S-box is obtained by a function of the form $f(x) = A'(A'x + b')^{-1} + b'$ where A' is a 8×8 circular matrix of bits obtained by $0x5b$ and $b' = 0x5d$. The proposed S-box in [5] has better values for some cryptographic criteria. Typically, the distance to SAC is reduced to 372, the iterative period is increased to 256, the affine transformation period is increased to 16, and the the number of terms in the algebraic expression is increased to 255.

In this paper, we propose a new function over $\mathbb{F}_{2^8}$ to construct 16×16 S-boxes of bytes with good cryptographic properties. The function is defined for a byte x by

$$S(x) = \begin{cases} \frac{Ax+\alpha}{Ax+\beta}, & \text{if } x \neq A^{-1}\beta \\ 0x01 & \text{if } x = A^{-1}\beta, \end{cases}$$

where A is an 8×8 invertible matrix of bits and α and β are two fixed different bytes. The cryptographic properties of the new S-boxes depend on the choice of A, α and β and there are approximately 5.3×10^{18} of possible values. In this paper, we consider the parameters

$$A = \begin{pmatrix} 1\,0\,0\,0\,1\,1\,0\,1 \\ 1\,1\,0\,0\,1\,0\,0\,1 \\ 0\,1\,1\,1\,0\,0\,0\,1 \\ 0\,0\,0\,0\,1\,1\,0\,1 \\ 0\,0\,1\,0\,0\,0\,1\,0 \\ 1\,0\,0\,0\,1\,0\,1\,1 \\ 0\,1\,1\,1\,0\,0\,0\,0 \\ 1\,1\,0\,1\,0\,1\,1\,0 \end{pmatrix}, \quad \alpha = 0xfe, \quad \beta = 0x3f.$$

With the former values, some of the cryptographic criteria are improved. The distance to SAC is reduced to 328, the iterative period is increased to 256, and the number of terms in the algebraic expression is increased to 255. We notice that our construction ovoids any affine structure while in AES and in [5], there are induced affine transformations of the form $f(x) = A'x + b$ where the 8×8 bit-matrix A' and the byte b are constant.

The rest of the paper is organized as follows. In Section 2, we present some known facts related to AES, in Section 3, we present the new S-box and, in Section 4, we study the cryptographic criteria of the proposed S-box. In Section 5, we give a comparison of the new S-box with the AES S-box and other existing S-boxes. We conclude the paper in Section 6.

2 Preliminaries

In this section, we present the main mathematical properties that will be used in this paper.

2.1 Description of an S-box

An S-box of a block cipher is a $n \times n$ matrix defined by a multivariate Boolean function $S : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that for $x \in \mathbb{F}_{2^n}$,

$$S(x) = (S_{n-1}(x), \ldots, S_0(x)),$$

where S_i, $0 \leq i \leq n-1$ is a component Boolean function. An S-box should be bijective with no fixed point and should guarantee nonlinearity to the cryptosystem and strengthen its cryptographic security. Moreover, it should satisfy several criteria such as balancedness [14], strict avalanche criterion (SAC) [18], distance to SAC [18], bit independence criterion (BIC) [8], algebraic complexity and algebraic degree [2].

2.2 Description of AES

AES is a block cipher with 128- bits blocks. It operates on blocks, called states which are 4×4 arrays of bytes. Each state is indexed $0, \ldots, 15$. The rows are in the form $(i, i+4, i+8, i+12)$ while the columns are in the form $(4i, 4i+1, 4i+2, 4i+3)$ for $0 \leq i \leq 3$. AES has $N_r \in \{10, 12, 14\}$ rounds, formed by the transformations AddRoundKey, SubBytes, ShiftRows, and MixColumns as follows.

1. The first round is preceded by a transformation denoted AddRoundKey.
2. The first $N_r - 1$ rounds are composed by 4 transformations:
   (a) SubBytes Transformation: it is a non linear transformation of the state and is represented by the S-box;
   (b) ShiftRows Transformation: it is a circular shift on the rows of the state;
   (c) MixColumns Transformation: it is a linear transformation of the state;
   (d) AddRoundKey Transformation: it is a transformation of the state by xoring a 128 bit key.
3. The final round is composed by the three transformations:
   (a) SubBytes Transformation;
   (b) ShiftRows Transformation;
   (c) AddRoundKey Transformation.

SubBytes is the transformation that is based on on the S-box. The security of AES depends mainly on the structure of the S-box.

2.3 Structure of the AES S-box

AES uses the Galois field $\mathbb{F}_{2^8}$, defined by

$$\mathbb{F}_{2^8} = \mathbb{F}_2[t]/(t^8 + t^4 + t^3 + t + 1),$$

where each byte $b = (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0) \in \mathbb{F}_2^8$ is mapped to the element

$$b_7t^7 + b_6t^6 + b_5t^5 + b_4t^4 + b_3t^3 + b_2t^2 + b_1t + b_0$$

of the Galois field $\mathbb{F}_{2^8}$. For example, the byte $0x53 = (0, 1, 0, 1, 0, 0, 1, 1)$ is identified with the field element $t^6 + t^4 + t + 1$.

The AES S-box S is constructed by combining two transformations f and g for $x \in \mathbb{F}_{2^8}$ by $S(x) = g \circ f(x)$ where

1. The first transformation is the nonlinear function f defined by

$$f(x) = \begin{cases} 0 & \text{if } x = 0, \\ x^{-1} & \text{if } x \neq 0. \end{cases}$$

   Hence, the function f maps zero to zero, and for a non-zero field element x, it maps the element to its multiplicative inverse x^{-1} in $\mathbb{F}_{2^8}$.
2. The second transformation g is the affine function defined by $g(x) = Ax + b$ where A is 8×8 bit-matrix and b is a constant. Namely, for a field element $x = (x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0)$, $y = Ax + b$ with

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Here is an example showing $S(0x53) = 0xed$:

- $0x53 = (0, 1, 0, 1, 0, 0, 1, 1)$ is mapped to $t^6 + t^4 + t + 1$;
- the inverse of $t^6 + t^4 + t + 1$ modulo $t^8 + t^4 + t^3 + t + 1$ is $t^7 + t^6 + t^3 + t$ so

$$f(t^6 + t^4 + t + 1) = t^7 + t^6 + t^3 + t,$$

  which is $(1, 1, 0, 0, 1, 0, 1, 0)$ in binary form;
- apply the affine transformation g

$$\begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix};$$

- the S-box output is then $(1, 1, 1, 0, 1, 1, 0, 1)$, that is $0xed$.

2.4 Algebraic complexity of AES S-box

The algebraic complexity of an S-box S is measured by the number of non trivial monomials in the representation of S by a polynomial such that

$$S(x) = a_{255}x^{255} + a_{254}x^{254} + \cdots + a_1 x + a_0.$$

The AES S-box is constructed using the function $S(x) = g \circ f(x)$ where $f(x) = x^{-1} = x^{254}$ and $g(x) = Ax + B$. Hence f is a power function and g is an affine function. For a combination of such kind of functions, the following result fixes the algebraic complexity (see [4]).

Theorem 1. *Let $S = g \circ f$ be the function of an S-box on $\mathbb{F}_2^n$ with a power function f and an affine function g. Then the algebraic complexity of S is at most $n + 1$.*

The former result partially explains why the algebraic complexity of AES is 9 [4].

3 The Proposed S-box

In this section, we present the new S-box. We first define a 8×8 invertible matrix A with components in $\mathbb{F}_2$ and two constants $\alpha, \beta \in \mathbb{F}_{2^8}$. The following result gives the number of invertible matrices with entries in $\mathbb{F}_2$ (see [19], Section 3.3).

Lemma 1. *Let $\mathbb{F}_q$ be a finite field with q elements. For $n \geq 2$, let $GL(n, \mathbb{F}_q)$ be the group of invertible $n \times n$ matrices with entries in $\mathbb{F}_q$. The order of $GL(n, \mathbb{F}_q)$ is*

$$|GL(n, \mathbb{F}_q)| = \prod_{k=0}^{n-1} \left(q^n - q^k\right).$$

For $n = 8$ and $q = 2$, the group $GL(8, \mathbb{F}_2)$ of invertible 8×8 matrices A with entries in $\mathbb{F}_2$, the order is

$$|GL(8, \mathbb{F}_2)| = 5\ 348\ 063\ 769\ 211\ 699\ 200 \approx 5.3 \times 10^{18}.$$

Let

$$A = \begin{pmatrix} 1\,0\,0\,0\,1\,1\,0\,1 \\ 1\,1\,0\,0\,1\,0\,0\,1 \\ 0\,1\,1\,1\,0\,0\,0\,1 \\ 0\,0\,0\,0\,1\,1\,0\,1 \\ 0\,0\,1\,0\,0\,0\,1\,0 \\ 1\,0\,0\,0\,1\,0\,1\,1 \\ 0\,1\,1\,1\,0\,0\,0\,0 \\ 1\,1\,0\,1\,0\,1\,1\,0 \end{pmatrix}$$

and

$$\alpha = 0xfe = (1,1,1,1,1,1,1,0), \quad \beta = 0x3f = (0,0,1,1,1,1,1,1).$$

The new S-box is generated by the multivariate Boolean function S_N defined for $x \in \mathbb{F}_{2^8}$ by

$$S_N(x) = \begin{cases} \frac{Ax+\alpha}{Ax+\beta}, & \text{if } Ax + \beta \neq 0 \\ 0x01 & \text{if } Ax + \beta = 0, \end{cases} \tag{1}$$

Here are two examples showing $S_N(0xdd) = 0xed$ and $S_N(0xfa) = 0x01$.

Example 1: $S_N(0xdd) = 0xed$

- $0xdd = (1,1,0,1,1,1,0,1) = (x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0)$
- apply the affine transformation $Ax + \beta$

$$\begin{pmatrix} 1\,0\,0\,0\,1\,1\,0\,1 \\ 1\,1\,0\,0\,1\,0\,0\,1 \\ 0\,1\,1\,1\,0\,0\,0\,1 \\ 0\,0\,0\,0\,1\,1\,0\,1 \\ 0\,0\,1\,0\,0\,0\,1\,0 \\ 1\,0\,0\,0\,1\,0\,1\,1 \\ 0\,1\,1\,1\,0\,0\,0\,0 \\ 1\,1\,0\,1\,0\,1\,1\,0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

so $Ax + \beta = (1,0,1,1,1,0,0,0) = 0xb8$
- apply the affine transformation $Ax + \alpha$

$$\begin{pmatrix} 1\,0\,0\,0\,1\,1\,0\,1 \\ 1\,1\,0\,0\,1\,0\,0\,1 \\ 0\,1\,1\,1\,0\,0\,0\,1 \\ 0\,0\,0\,0\,1\,1\,0\,1 \\ 0\,0\,1\,0\,0\,0\,1\,0 \\ 1\,0\,0\,0\,1\,0\,1\,1 \\ 0\,1\,1\,1\,0\,0\,0\,0 \\ 1\,1\,0\,1\,0\,1\,1\,0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

so $Ax + \alpha = (0,1,1,1,1,0,0,1) = 0x79$
- Calculate the S-box value

$$\begin{aligned} S_N(0xdd) &= \frac{Ax+\alpha}{Ax+\beta} \\ &= \frac{0x79}{0xb8} \\ &= \frac{t^6+t^5+t^4+t^3+1}{t^7+t^5+t^4+t^3} \\ &= t^7+t^6+t^5+t^3+t^2+1 \pmod{t^8+t^4+t^3+t+1} \\ &= (1,1,1,0,1,1,0,1) \\ &= 0xed. \end{aligned}$$

Example 2: $S_N(0xfa) = 0x01$

- $0xfa = (1,1,1,1,1,0,1,0) = (x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0)$
- apply the affine transformation $Ax + \beta$

$$\begin{pmatrix} 1\,0\,0\,0\,1\,1\,0\,1 \\ 1\,1\,0\,0\,1\,0\,0\,1 \\ 0\,1\,1\,1\,0\,0\,0\,1 \\ 0\,0\,0\,0\,1\,1\,0\,1 \\ 0\,0\,1\,0\,0\,0\,1\,0 \\ 1\,0\,0\,0\,1\,0\,1\,1 \\ 0\,1\,1\,1\,0\,0\,0\,0 \\ 1\,1\,0\,1\,0\,1\,1\,0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

so $Ax + \beta = (0, 0, 0, 0, 0, 0, 0, 0) = 0x00$

– Therefore, using the definition of S_N in (1), we get

$$S_N(0xfa) = 0x01.$$

Applying the function S_N to $\mathbb{F}_{2^8}$, we get the new S-box presented in Table 1.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	36	94	89	cb	77	96	d2	4b	05	f7	ab	c5	6d	a1	d6	5b
1	61	91	e7	d0	1f	a9	43	1d	9b	be	f4	b8	42	63	87	bb
2	02	58	c3	ac	e4	e5	eb	b3	83	70	64	20	57	08	60	85
3	2f	90	07	ee	23	33	81	12	14	ea	39	21	62	cd	28	2e
4	2c	f6	dd	25	bc	11	a7	e6	fd	53	98	9c	38	1b	5c	54
5	75	95	26	00	09	3b	44	9d	15	5d	1c	9a	5f	c9	a4	78
6	5a	f3	0b	0c	e9	0a	06	3e	71	e1	fa	f5	7f	65	19	df
7	8e	32	fb	74	50	d9	72	24	45	0f	69	76	da	41	b1	db
8	79	80	3a	49	e8	bf	73	16	18	8d	ce	a3	0e	c6	ef	e3
9	d7	99	6e	35	fc	af	a2	c1	de	c2	1e	d1	6c	f1	aa	7e
a	8c	52	d4	4a	7c	93	f0	e2	d8	66	04	9e	84	3c	13	ae
b	86	88	a5	68	d3	37	3d	56	6a	5e	7a	ad	c8	b2	40	67
c	0d	b7	46	7d	a6	82	6b	3f	34	22	b0	c0	29	4e	59	7b
d	c7	31	ba	47	fe	c4	d5	e0	92	b9	10	a0	8b	ed	55	97
e	ca	1a	f9	2a	cc	f2	4c	51	03	30	4d	f8	b4	bd	cf	48
f	ec	2b	9f	ff	27	17	b6	8f	8a	b5	01	a8	6f	4f	dc	2d

Table 1. The new S-box

The inverse function of S_N is S_N^{-1} and is defined for a byte y by

$$S_N^{-1}(y) = \begin{cases} A^{-1}\left(\frac{\beta y + \alpha}{y+1}\right), & \text{if } y \neq 0x01 \\ A^{-1}\beta & \text{if } y = 0x01. \end{cases}$$

The new inverse S-box is presented in Table 2.

4 Cryptographic Criteria of the New S-box

4.1 Linear Cryptanalysis of the New S-box

The resistance against linear cryptanalysis of a block cipher with an S-box function S over $\mathbb{F}_{2^n}$ is measured by the non-linearity parameter $NL(S)$, defined as (see [2], Section 3)

$$NL(S) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^{n*}, b \in \mathbb{F}_2^n} \left| \sum_{x \in \mathbb{F}_{2^n}} (-1)^{a \cdot S(x) \oplus b \cdot x} \right|,$$

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	53	fa	20	e8	aa	08	66	32	2d	54	65	62	63	c0	8c	79
1	da	45	37	ae	38	58	87	f5	88	6e	e1	4d	5a	17	9a	14
2	2b	3b	c9	34	77	43	52	f4	3e	cc	e3	f1	40	ff	3f	30
3	e9	d1	71	35	c8	93	00	b5	4c	3a	82	55	ad	b6	67	c7
4	be	7d	1c	16	56	78	c2	d3	ef	83	a3	07	e6	ea	cd	fd
5	74	e7	a1	49	4f	de	b7	2c	21	ce	60	0f	4e	59	b9	5c
6	2e	10	3c	1d	2a	6d	a9	bf	b3	7a	b8	c6	9c	0c	92	fc
7	29	68	76	86	73	50	7b	04	5f	80	ba	cf	a4	c3	9f	6c
8	81	36	c5	28	ac	2f	b0	1e	b1	02	f8	dc	a0	89	70	f7
9	31	11	d8	a5	01	51	05	df	4a	91	5b	18	4b	57	ab	f2
a	db	0d	96	8b	5e	b2	c4	46	fb	15	9e	0a	23	bb	af	95
b	ca	7e	bd	27	ec	f9	f6	c1	1b	d9	d2	1f	44	ed	19	85
c	cb	97	99	22	d5	0b	8d	d0	bc	5d	e0	03	e4	3d	8a	ee
d	13	9b	06	b4	a2	d6	0e	90	a8	75	7c	7f	fe	42	98	6f
e	d7	69	a7	8f	24	25	47	12	84	64	39	26	f0	dd	33	8e
f	a6	9d	e5	61	1a	6b	41	09	eb	e2	6a	72	94	48	d4	f3

Table 2. The new inverse S-box

where $u \cdot v$ is the dot product of u and v, defined by

$$u \cdot v = (u_{n-1}, \cdots, u_0) \cdot (v_{n-1}, \cdots, v_0) = u_{n-1}v_{n-1} \oplus \cdots \oplus u_0 v_0.$$

The non-linearity parameter $NL(S)$ is upper bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$ (see [6]). For $n = 8$, the upper bound becomes $2^7 - 2^3 = 120$ while the non-linearity value $NL(S)$ is 112 for both AES S-box and the new S-box, which is very close to the maximal value of perfect nonlinear function.

4.2 Differential Cryptanalysis of the New S-box

The resistance against differential cryptanalysis of a block cipher with S-box function S over $\mathbb{F}_{2^n}$ is measured by the the differential uniformity parameter $\delta(S)$, defined as

$$\delta(S) = \max_{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}} D(a, b),$$

where, for $(a, b) \in \mathbb{F}_{2^n}^2$,

$$D(a, b) = \left| \{x \in \mathbb{F}_{2^n} \mid S(x) + S(x + a) = b\} \right|,$$

is the differential distribution of the S-box. For the new S-box, we have the following properties which are similar than the AES S-box:

- $D(0, 0) = 256$.
- For all $a \neq 0$, $D(a, 0) = 0$.
- For all $b \neq 0$, $D(0, b) = 0$.

- For all $a \neq 0$, $|\{b \in \mathbb{F}_{2^n} | D(a,b) = 0\}| = 129$.
- For all $b \neq 0$, $|\{a \in \mathbb{F}_{2^n} | D(a,b) = 0\}| = 129$.
- For all $a \neq 0$, $|\{b \in \mathbb{F}_{2^n} | D(a,b) = 2\}| = 126$.
- For all $b \neq 0$, $|\{a \in \mathbb{F}_{2^n} | D(a,b) = 2\}| = 126$.
- For all $a \neq 0$, $|\{b \in \mathbb{F}_{2^n} | D(a,b) = 4\}| = 1$.
- For all $b \neq 0$, $|\{a \in \mathbb{F}_{2^n} | D(a,b) = 4\}| = 1$.
- For all $\delta \notin \{0,2,4\}$, $\left|\{(a,b) \in \mathbb{F}_{2^n}^2 | D(a,b) = \delta\}\right| = 0$.

The lower bound of the differential uniformity for an S-box defined over $\mathbb{F}_{2^n}$ is 2 [3]. The maximal differential uniformity for the new S-box is 4, which is similar than the AES S-box (see [3,4]).

4.3 Bit Independence Criterion (BIC) of the New S-box

The bit independence criterion (BIC) was introduced by Webster and Tavares in [18]. It states that, if any input bit i is inverted in x, this changes any output bits j and k without any dependence on each other. This is useful to avoid any statistical pattern or statistical dependencies between output bits of the output vectors. Hence, for a strong S-box, the dependence between output bits should be as small as possible.

Definition 1. *Let $S : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a multivariate Boolean function defining an S-box. Let $\alpha_i = (\delta_{i,n-1}, \ldots, \delta_{i,0})$ where $\delta_{i,i} = 1$ and $\delta_{i,j} = 0$ if $i \neq j$. For all $x \in \mathbb{F}_{2^n}$, the corresponding vector to $S(x) \oplus S(x \oplus \alpha_i)$ is*

$$v(i,x) = (a_{i,n-1}(x), \ldots, a_{i,0}(x)).$$

The list $(a_{i,j}(x))$ of all $x \in \mathbb{F}_{2^n}$ is denoted $a_{i,j}$.

The correlation coefficient of $(a_{i,j}, a_{i,k})$ is defined as

$$\mathrm{corr}(a_{i,j}, a_{i,k}) = \frac{\frac{1}{2^n}\left(\sum_{x \in \mathbb{F}_{2^n}} a_{i,j}(x) a_{i,k}(x)\right) - E(a_{i,j})E(a_{i,k})}{\sqrt{E\left(a_{i,j}^2\right) - (E(a_{i,j}))^2} \cdot \sqrt{E\left(a_{i,k}^2\right) - (E(a_{i,k}))^2}},$$

where $E(t)$ is the expected value of the list t.
A bit independence parameter corresponding to the independence of the output bits j and k under the effect of the change of the input bit i is defined as

$$BIC(j,k) = \max_{0 \leq i \leq n-1} \mathrm{corr}(a_{i,j}, a_{i,k}).$$

The table of $BIC(i,j)$, $0 \leq i,j \leq 7$, for the new S-box is listed in Table 3. For comparison, the table of $BIC(i,j)$, $0 \leq i,j \leq 7$, for the AES S-box is listed in Table 4.

For the whole S-box, defined by the function S, the bit independence criterion parameter is defined as

$$BIC(S) = \max_{0 \leq j < k \leq n-1} BIC(j,k).$$

For the new S-box, the BIC value is 0.12. This is better than the BIC of the AES S-box which is 0.13.

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$
$j=0$	1.	0.090	0.097	0.12	0.097	0.067	0.12	0.090
$j=1$	0.090	1.	0.12	0.093	0.098	0.094	0.12	0.097
$j=2$	0.097	0.12	1.	0.095	0.12	0.095	0.10	0.12
$j=3$	0.12	0.093	0.095	1.	0.064	0.12	0.12	0.12
$j=4$	0.097	0.098	0.12	0.064	1.	0.12	0.064	0.072
$j=5$	0.067	0.094	0.095	0.12	0.12	1.	0.093	0.093
$j=6$	0.12	0.12	0.10	0.12	0.064	0.093	1.	0.059
$j=7$	0.090	0.097	0.12	0.12	0.072	0.093	0.059	1.

Table 3. Table of $BIC(a_j, a_k)$ for the New S-box

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$
$j=0$	1	0.098	0.12	0.12	0.12	0.13	0.066	0.095
$j=1$	0.098	1	0.098	0.13	0.067	0.12	0.098	0.12
$j=2$	0.12	0.098	1	0.12	0.097	0.067	0.098	0.12
$j=3$	0.12	0.13	0.12	1	0.12	0.13	0.066	0.096
$j=4$	0.12	0.067	0.097	0.12	1	0.097	0.12	0.066
$j=5$	0.13	0.12	0.067	0.13	0.097	1	0.10	0.071
$j=6$	0.066	0.098	0.098	0.066	0.12	0.10	1	0.098
$j=7$	0.095	0.12	0.12	0.096	0.066	0.071	0.098	1

Table 4. Table of $BIC(a_j, a_k)$ for the AES S-box

4.4 Periodicity of the New S-box

The periodicity of an S-box is related to the number of minimum compositions to get the identity function (see [5,16]).

Definition 2. *Let $S : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the function defining an S-box. For $x \in \mathbb{F}_{2^n}$, the period of x under S is the smallest positive integer r such that $S^r(x) = x$.*

It is shown in Table 5 that in AES, there are 5 possible periods, namely 2, 27, 59, 81 and 87 containing respectively 2, 27, 59, 81 and 87 different elements of $\mathbb{F}_{2^8}$.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	59	81	59	59	87	59	59	59	87	81	87	27	81	81	81	59
1	81	81	81	81	27	87	81	81	87	59	81	87	87	87	81	87
2	59	59	87	27	59	59	27	81	87	59	87	27	87	27	59	87
3	87	59	27	59	87	87	59	87	59	81	81	87	81	81	87	59
4	81	81	87	81	87	27	87	81	59	87	87	81	59	81	87	81
5	87	87	59	87	59	87	27	81	59	87	87	81	87	59	59	81
6	87	27	81	59	81	81	59	87	27	87	59	59	87	81	27	59
7	87	87	81	2	81	59	59	59	81	87	81	59	81	81	81	59
8	81	81	81	81	81	87	87	81	87	87	81	81	81	59	59	2
9	87	81	81	87	87	87	87	87	87	87	87	27	87	59	27	27
a	81	27	81	87	87	59	59	87	59	59	81	81	81	87	87	87
b	87	27	87	81	59	59	87	59	87	27	87	81	81	81	87	87
c	87	81	59	59	87	59	59	59	27	81	81	87	81	81	81	81
d	87	87	59	59	59	59	87	81	27	87	81	27	87	81	87	27
e	81	81	87	81	87	87	59	87	27	81	81	81	81	87	87	27
f	81	27	87	81	87	59	87	27	81	87	27	59	87	59	81	81

Table 5. Periodicity of the AES S-box

For the new S-box, as shown in Table 6, 256 is the unique period so that the distribution of elements of $\mathbb{F}_{2^8}$ is more balanced for the periodicity criterion.

4.5 Fixed and opposite points

Definition 3. *The opposite of $x \in \mathbb{F}_{2^8}$ is the field element $\bar{x} \in \mathbb{F}_{2^8}$ such that $x + \bar{x} = 0xff$.*

The AES S-box has no fixed point, that is $S(x) \neq x$ and no opposite fixed points, that is $S(x) \neq \bar{x}$) for all $x \in \mathbb{F}_{2^8}$ (see [6]). Similarly, the new S-box has no fixed points and no opposite fixed points.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
1	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
2	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
3	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
4	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
5	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
6	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
7	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
8	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
9	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
a	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
b	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
c	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
d	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
e	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256
f	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256	256

Table 6. Periodicity of the new S-box

4.6 Algebraic Complexity of the New S-box

Let S be an S-box over $\mathbb{F}_{2^n}$. Then S is completely defined by the set $\{(x_i, y_i) \mid x_i \in \mathbb{F}_{2^n},\ y_i = S(x_i)\}$. A polynomial expression for S is determined by Lagrange's interpolation polynomial

$$P(x) = \sum_{i=0}^{2^n-1} y_i L_i(x), \quad L_i(x) = \frac{\prod_{j\neq i}(x - x_j)}{\prod_{j\neq i}(x_i - x_j)}.$$

The polynomial $P(x)$ is of degree of at most $2^n - 1$ and the number of its non-zero monomials is called the *algebraic complexity*. For AES, the polynomilal is [4]

$$\begin{aligned} P(x) =& 05x^{254} + 09x^{253} + f9x^{251} + 25x^{247} + f4x^{239} + 01x^{223} + b5x^{191} \\ &+ 8fx^{127} + 63, \end{aligned}$$

which shows that the algebraic complexity for AES is 9. For the new S-box, the polynomial is of the form

$$P(x) = \sum_{i=0}^{255} a_i x^i,$$

where the list of the coefficients a_i is listed in Table 7. From this table, we see that the algebraic complexity of the new S-box is 255, which is optimal and makes it more resistant to possible algebraic attacks than the AES S-box.

	f	e	d	c	b	a	9	8	7	6	5	4	3	2	1	0
f	00	b6	6c	30	3e	32	e5	06	68	b2	9c	8e	54	b9	0d	c8
e	01	c0	6d	aa	3a	0c	1a	7e	eb	52	48	4e	b5	cf	8a	5c
d	56	5b	1d	0b	42	43	4d	06	5c	15	37	49	02	ea	e9	d6
c	c4	35	b7	f2	ca	d0	0c	9a	28	ba	1c	8a	d7	ef	31	be
b	2e	ac	b5	6e	b1	6c	18	61	a3	06	8f	c4	10	0e	3b	c1
a	ff	55	f8	60	99	0c	b8	3a	88	90	ad	c6	61	83	a7	16
9	a4	48	5a	1b	a4	1f	b8	c4	3c	af	d5	33	4d	90	7d	60
8	cf	65	7e	5d	bb	43	b4	41	95	6c	0c	86	e0	02	b2	93
7	a2	6f	c6	e1	1d	71	6a	93	9d	12	c6	9f	d4	5e	c7	84
6	c3	84	1f	38	6e	a9	52	ea	98	97	ec	1f	bd	12	c4	32
5	49	ae	1a	63	b4	fe	7b	b4	e7	f4	04	2b	f8	e4	f2	47
4	fa	e3	04	c6	72	f8	fb	2c	bf	c8	e6	e1	0c	2a	2d	4a
3	e5	c3	73	0c	99	8a	8d	a9	25	39	16	c1	1b	3f	c0	19
2	5d	fd	9b	5d	fb	1d	f9	c7	a8	c4	03	48	63	63	15	83
1	f6	50	18	50	3c	57	96	0b	dc	dd	41	a0	fd	05	e7	50
0	13	66	d8	f8	fa	ea	93	72	a7	1d	5b	5e	0b	75	45	36

Table 7. Algebraic expression of the new S-box

Similarly, the algebraic expression of the inverse of the new S-box is presented in Table 8 and has 254 monomials which is almost optimal.

	f	e	d	c	b	a	9	8	7	6	5	4	3	2	1	0
f	00	b6	f2	44	37	81	c5	73	49	ff	bb	0d	7e	c8	8c	3a
e	01	b7	f3	45	36	80	c4	72	48	fe	ba	0c	7f	c9	8d	3b
d	d7	61	25	93	e0	56	12	a4	9e	28	6c	da	a9	1f	5b	ed
c	d6	60	24	92	e1	57	13	a5	9f	29	6d	db	a8	1e	5a	ec
b	65	d3	97	21	52	e4	a0	16	2c	9a	de	68	1b	ad	e9	5f
a	64	d2	96	20	53	e5	a1	17	2d	9b	df	69	1a	ac	e8	5e
9	b2	04	40	f6	85	33	77	c1	fb	4d	09	bf	cc	7a	3e	88
8	b3	05	41	f7	84	32	76	c0	fa	4c	08	be	cd	7b	3f	89
7	20	96	d2	64	17	a1	e5	53	69	df	9b	2d	5e	e8	ac	1a
6	21	97	d3	65	16	a0	e4	52	68	de	9a	2c	5f	e9	ad	1b
5	f7	41	05	b3	c0	76	32	84	be	08	4c	fa	89	3f	7b	cd
4	f6	40	04	b2	c1	77	33	85	bf	09	4d	fb	88	3e	7a	cc
3	45	f3	b7	01	72	c4	80	36	0c	ba	fe	48	3b	8d	c9	7f
2	44	f2	b6	00	73	c5	81	37	0d	bb	ff	49	3a	8c	c8	7e
1	92	24	60	d6	a5	13	57	e1	db	6d	29	9f	ec	5a	1e	a8
0	93	25	61	d7	a4	12	56	e0	da	6c	28	9e	ed	5b	1f	53

Table 8. Algebraic expression of the inverse of the new S-box

4.7 Strict Avalanche Criterion (SAC) of the New S-box

In [18], Webster and Tavares introduced an important criterion for strong S-boxes, called strict avalanche criterion (SAC). This criterion states that a single bit change in the input of a strong S-box should change the output bit with probability approaching $\frac{1}{2}$.

Definition 4. *A vectorial Boolean function $S : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ satisfies SAC if and only if for all i, $0 \leq i \leq n-1$,*

$$\sum_{x \in \mathbb{F}_{2^n}} f(x) \oplus S(x \oplus \alpha_i) = \left(2^{n-1}, \ldots, 2^{n-1}\right),$$

where the binary representation of $\alpha_i \in \mathbb{F}_{2^n}$ is a vector of length n with a 1 in the ith position and 0 elsewhere.

Consequently, an S-box having a value of SAC closer to $\left(2^{n-1}, \ldots, 2^{n-1}\right)$ has a good SAC property. Table 9 gives the SAC values of the new S-box and Table 10 gives the Sac values of the AES S-box.

α_i	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 2	Bit 1
00000001	120	120	132	136	132	132	136	120
00000010	136	140	132	128	124	124	132	140
00000100	128	120	136	128	136	132	116	124
00001000	136	128	132	132	132	120	128	120
00010000	128	140	124	124	116	128	128	116
00100000	136	120	128	132	132	132	128	132
01000000	128	128	144	124	128	116	120	120
10000000	124	132	132	124	128	132	124	128

Table 9. SAC of the new S-box

α_i	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 2	Bit 1
00000001	128	116	124	116	144	116	132	132
00000010	136	128	116	124	128	144	124	120
00000100	128	136	128	124	120	128	132	132
00001000	140	128	136	128	116	120	136	136
00010000	136	140	128	128	132	116	128	116
00100000	136	136	140	120	120	132	132	116
01000000	124	136	136	120	132	120	136	136
10000000	132	124	136	124	136	132	144	132

Table 10. SAC of the AES S-box

From Table 9 and Table 10, we see that the mean value for SAC for the new S-box is 128.625 while it is 129.25 for the AES S-box.

4.8 Distance to SAC of the New S-box

In general, the SAC criterion is not absolutely performed by an S-box. A practical way to measure the deviation of the SAC the S-box is to compute the distance to sac.

Definition 5. *Let $S : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the function defining an S-box such that*

$$S(x) = (f_{n-1}(x), \ldots, f_0(x)).$$

The distance to SAC of S is the value

$$DSAC(S) = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} \left| \sum_{x \in \mathbb{F}_{2^n}} f_i(x \oplus \alpha_j) \oplus f_i(x) - 2^{n-1} \right|.$$

where the binary representation of $\alpha_j \in \mathbb{F}_{2^n}$ is a vector of length n with a 1 in the jth position and 0 elsewhere.

A strong S-box should have a small DSAC. From Table 10, we find that DSAC for the AES S-box is 432 (see [5]) while Table 9 shows that DSAC for the new S-box 328.

5 Comparison with existing S-boxes

In Table 11, we listed the performance of the AES S-box, the S-box proposed by Cui et al. [5] and the new S-box. The table shows that, for all cryptographic criteria, the performance of the new S-box is equal or better than the former ones and they are closer to the performances of an optimal S-box. This implies that the new S-box has better security than the former ones and is suitable for use in AES.

Criterion	AES S-box	Cui et al. S-box [5]	**New S-box**	Optimal value
Linear Cryptanalysis	112	112	**112**	120
Differential Cryptanalysis	4	4	**4**	4
Periodicity	less than 87	256	**256**	256
Algebraic Complexity	9	255	**255**	255
Inverse Algebraic Complexity	255	253	**254**	255
Mean of SAC	129.25	127.9375	**128.25**	128
Distance to SAC	432	372	**328**	0
Maximal BIC	0.13	0.13	**0.12**	0

Table 11. Comparison of the new S-box with two former S-boxes

6 Conclusion

In this paper, we presented a new S-box for the AES encryption scheme and analyzed its security by studying the main cryptographic criteria. For all the criteria, the performances of the new S-box are at least as good as the performances of the existing S-boxes. More specifically, the new S-box has better distance to SAC, better BIC and better algebraic complexity.

References

1. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, vol.4, no.1, pp. 3–72 (1991)
2. Carlet, C.: Vectorial Boolean Functions for Cryptography. In: Y. Crama & P. Hammer (Eds.), Boolean Models and Methods in Mathematics, Computer Science, and Engineering (Encyclopedia of Mathematics and its Applications, pp. 398–470. Cambridge: Cambridge University Press (2010)
3. Canteaut, A.: Lecture Notes on Cryptographic Boolean Functions, March 10, 2016, `https://www.rocq.inria.fr/secret/Anne.Canteaut/poly.pdf`
4. Cui, L., Cao, Y.: A new S-box structure named affine-power-affine, International Journal of Innovative Computing, Information and Control, Volume 3, Number 3, pp. 751–759 (2007)
5. Cui, J., Huang, L., Zhong, H., Chang, C., Yang, W.: An improved AES S-box and its performance analysis, International Journal of Innovative Computing, Information and Control, Volume 7, Number 5(A), pp. 2291–2302 (2011)
6. Daemen J., Rijmen V.: AES Proposal: Rijndael (1999) `https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf`
7. Data Encryption Standard, National Bureau of Standards, NBS FIPS PUB 46, U.S. Department Of Commerce, (1977)
8. Detombe, J., Tavares, S.: Constructing large cryptographically strong S-boxes. In: Seberry J., Zheng Y. (eds) Advances in Cryptology - AUSCRYPT'92. AUSCRYPT 1992. Lecture Notes in Computer Science, vol 718. Springer, Berlin, Heidelberg pp. 165–181 (1992)
9. Dragomir, I.R., Lazar, M.: Generating and testing the components of a block cipher, 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Ploiesti, 2016, pp. 1-4 (2016)
10. Juremi, J., Mahmod, R., Sulaiman, S.: A Proposal for Improving AES S-box with Rotation and Key-Dependent. In Proceedings of the International Conference on Digital Cyber Security, CyberWarfare and Digital Forensic, Kuala Lumpur, Malaysia, pp. 26–28 (2012)
11. Ma, H., Liu, L.: Algebraic expression for AES S-box and InvS-box, Computer Engineering, vol. 32, no. 18, pp. 149–151 (2006)
12. Matsui, M.: Linear Cryptanalysis method for DES cipher, Advances in Cryptology-EUROCRYPT'93, Springer-Verlag, Berlin, pp. 386–397 (1994)
13. National Institute of Standards and Technology: Federal Information Processing Standards Publication 197: Announcing the Advanced Encryption Standard (AES). `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf` (accessed June, 09, 2019).

14. Prouff, E.: DPA attacks and S-boxes. In: Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers. Volume 3557 of Lecture Notes in Computer Science, Springer pp. 424–441 (2005)
15. Sahoo, O.B., Kole, D.K., Rahaman, H.: An optimized S-box for Advanced Encryption Standard (AES) design. In Proceedings of the International Conference on Advanced Computer Communication, Chennai, India, pp. 3–5 (2012)
16. Wang, Y.B.: Analysis of structure of AES and its S-box, Journal of PLA University: Science and Technology, vol. 3, no. 3, pp. 13–17 (2002)
17. Wang, H., Zheng, H., Hu, B., Tang, H.: Improved lightweight encryption algorithm based on optimized S-box, 2013 International Conference on Computational and Information Sciences, Shiyang, 2013, pp. 734-737 (2013)
18. Webster, A.F, Tavares, S.E.: On the Design of S-Boxes, In: Williams H.C. (eds) Advances in Cryptology - CRYPTO'85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg, pp. 523–534 (1985)
19. Wilson, R.A.: The Finite Simple Groups, Graduate Texts Mathematics 251, Springer-Verlag (2009)
20. Zahid, A.H. , Arshad, M.J.: An innovative design of substitution-boxes using cubic polynomial mapping, Mathematics, Computer Science, Symmetry (2019)
21. Zahid, A.H., Arshad, M.J., Ahmad, M.: A novel construction of efficient substitution-boxes using cubic fractional transformation, Entropy 21 (2019), no. 3, Paper No. 245 (2019)