Analysis of a New Improved AES S-Box Structure

Rong Cheng(✉), Yu Zhou, Xudong Miao, and Jianyong Hu

Science and Technology on Communication Security Laboratory, Chengdu 610041, China
xidian_chengrong@163.com

Abstract. S-boxes are very important nonlinear components in symmetric ciphers and have a great role in the security of cryptographic algorithms. In algorithm design, 4-bit and 8-bit S-boxes are most commonly used. The S-box of the AES is the best 8-bit S-box in terms of nonlinearity and differential uniformity at present. However, other properties are not the best.

In this paper, we improve and propose a new algebraic structure that can be used to generate S-boxes with excellent performance. The main enhanced properties of the new S-boxes are: strict avalanche criterion (SAC), distance to SAC, the bit independence criterion (BIC), algebraic complexity, inverse algebraic complexity, and periodicity. After comparing with existing S-boxes, the properties of S-boxes proposed in this paper are the best.

Keywords: S-box · AES · Affine transformation · Strict avalanche criterion · Periodicity · Algebraic complexity

1 Introduction

The S-box is a nonlinear function that is widely used in symmetric ciphers. In block ciphers with substitution-permutation network (SPN) structure, S-boxes can provide nonlinearity to the encryption algorithm and greatly improve the difficulty of cryptanalysis. For different cryptanalysis methods, S-boxes have many performance indicators, such as nonlinearity for resistance to linear analysis, difference uniformity for resistance to differential analysis, algebraic degree for resistance to algebraic attacks, and so on. A strong S-box should have good properties.

In addition to the three properties nonlinearity, difference uniformity and algebraic degree, the main properties that is needed to be considered in the design of S-boxes are strict avalanche criterion (SAC), distance to SAC [25], the bit independence criterion [9], and algebraic complexity, as well as the algebraic complexity of inverse S-boxes [5], etc. The AES algorithm [8] is the most widely used cryptographic algorithm with SPN structure, and its S-box reaches the

Q. Jiang et al. (Eds.): SPNCE 2022, LNICST 496, pp. 109–125, 2023.
https://doi.org/10.1007/978-3-031-30623-5_8

current optimum in terms of resistance to differential and linear attacks, but there are still many properties being not good, such as algebraic complexity is only 9 and possible periods are 2, 27, 59, 81 and 87.

In order to improve the AES S-box, many people have made attempts. Liu et al. enhanced the algebraic complexity of AES S-box to 255 [13]. However, the algebraic complexity of the inverse of improved S-box is 9, and other properties such as distance to SAC and periodicity are still very poor. Cui et al. made improvements to the affine transform of the S-box of AES [7] and proved that the upper bound on the algebraic complexity of the S-box of the AES-like structure is 9, which is much smaller than the 255 optimum. Cui et al. further improved [6] on [7] by considering more properties to obtain a better 8-bit S-box. Nitaj et al. proposed a new structure [17] and searched for a better S-box and analyzed it. However, Nitaj et al. did not perform a deeper analysis of the structure, and this novel structure has greater potential for discovery. Based on the [17], Said Eddahmani et al. improved the distance to SAC of the S-box [10]. However, the mean of SAC and the maximal BIC of S-box became worse.

In this paper, we propose a new S-box structure and analyze its properties. Further, we show that they are all affine equivalent to AES S-box. For the most commonly used 4-bit and 8-bit S-boxes in cryptographic algorithms, we find many S-boxes with better properties than other existing S-boxes in our new structure, then compare it with S-boxes in [7] and [17], finally we think it has the best comprehensive performance. It can be used as a better S-box in encryption algorithms.

This paper is organized as follows: In Sect. 2, we introduce several types of S-box generation structures and propose an improved structure in this paper. In Sect. 3, we analyze affine equivalence of S-boxes. In Sect. 4, we propose a 4-bit S-box and an 8-bit S-box. Then we analyze their properties and compare them with existing S-boxes. In Sect. 5, we summary the data in the Table 16 and Table 17, and then conclude in Sect. 6.

2 Preliminaries

Let $\boldsymbol{A} \in \mathbb{F}_2^{n\times n}$ be a matrix and $\boldsymbol{a} \in \mathbb{F}_2^n$ be a vector. Let $\boldsymbol{a} = (t_{n-1}, t_{n-2}, \cdots, t_0)$, then $\boldsymbol{a}$ can be uniquely represented as a number $a \in \mathbb{F}_{2^n}$,

$$a = 2^{n-1}t_{n-1} + 2^{n-2}t_{n-2} + \cdots + t_0.$$

For the convenience of understanding, this paper uses $\boldsymbol{a}$ and a directly without describing their transformation process. In addition, we use a^{-1} and $\boldsymbol{a}^{-1}$ to denote both the inverse of $a \in \mathbb{F}_{2^n}$ and omit the transformation process. In this paper, all 8-bit S-boxes use the finite field $\mathbb{F}_{2^8} = \mathbb{F}_2[t]/(t^8 + t^4 + t^3 + t + 1)$.

2.1 Algebraic Expression of the S-Box

A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a function with n input variables and only one output variable in $\mathbb{F}_2$. Let $\mathcal{B}_n$ be the set of n-variable Boolean functions.

Similar to Boolean functions, the S-box $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is an n-input, m-output function, and which variables can be seen as Boolean functions:

$$F = (f_{m-1}, f_{m-2}, \ldots, f_0),$$

where $f_i \in \mathcal{B}_n$ $(0 \le i \le m-1)$ is the *coordinate function* of F. In this paper, we consider only the case where $n = m$.

Affine equivalent is a really important definition in the study of the properties of S-box. Two S-boxes $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are affine equivalent, if there exists affine invertible matrices $\boldsymbol{B_1} \in \mathbb{F}_2^{n\times n}$ and $\boldsymbol{B_2} \in \mathbb{F}_2^{n\times n}$, s.t.

$$G = \boldsymbol{B_2}(F(\boldsymbol{B_1}x + a)) + b$$

for $x \in \mathbb{F}_2^n$, where $a, b \in \mathbb{F}_2^n$. In the following, we use the symbol $G \sim F$ to indicate that G is affine equivalent to F.

In the following, we give three algebraic structures of S-boxes. The algebraic expression of AES-like S-box consists of two transformations: $f : x \longmapsto x^{-1}$ and $g : x \longmapsto \boldsymbol{A}x + b$, where $\boldsymbol{A}$ is an invertible matrix in $\mathbb{F}_2^{8\times 8}$ and $b \in \mathbb{F}_2^8$. That is $S_{AES}(x) = g \circ f(x)$, then

$$S_{AES}(x) = \boldsymbol{A}x^{-1} + b.$$

The matrix $\boldsymbol{A}$ in the AES algorithm is a cyclic matrix and $b = 0x63$ ($0x$ means it is a hexadecimal number, and similarly, $(01100011)_2$ means a binary number).

$$S_{AES}(x) = \boldsymbol{A}x^{-1} + b = \begin{bmatrix} 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \\ 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}.$$

To overcome the shortcomings of AES S-box, [6] and [7] proposed improved structure for AES S-box. It consists of three transformations, that is $S_{APA}(x) = g \circ f \circ g(x)$. Then

$$S_{APA}(x) = \boldsymbol{A}(\boldsymbol{A}x + b)^{-1} + b,$$

where $\boldsymbol{A}$ is an invertible matrix in $\mathbb{F}_2^{8\times 8}$ and $b \in \mathbb{F}_2^8$. The structure named *Affine-Power-Affine* S-box in [7]. The properties of S-box in [7] can be found in Table 17.

Although $S_{APA}(x)$ is greatly improved compared to AES S-box, many of its properties are not optimal. [17] presented the structure of a new improved AES S-box $S_{new20}(x)$. That is

$$S_{new20}(x) = \begin{cases} \dfrac{\boldsymbol{A}x + \alpha}{\boldsymbol{A}x + \beta} & \text{if } \boldsymbol{x} \neq \boldsymbol{A}^{-1}\beta \\ 0x01 & \text{if } \boldsymbol{x} = \boldsymbol{A}^{-1}\beta \end{cases},$$

where $\boldsymbol{A}$ is an invertible matrix in $\mathbb{F}_2^{8\times 8}$ and $\alpha, \beta \in \mathbb{F}_2^8$. The properties of S-box in [17] can be found in Table 17.

Based on the [17], Said Eddahmani et al. improved the distance to SAC of the S-box [10]. The structure is

$$S_{new21}(x) = \begin{cases} \dfrac{a\boldsymbol{A}\cdot x + b}{c\boldsymbol{A}\cdot x + d} & \text{if } \boldsymbol{x} \neq \boldsymbol{A}^{-1}\dfrac{d}{c} \\ \dfrac{a}{c} & \text{if } \boldsymbol{x} = \boldsymbol{A}^{-1}\dfrac{d}{c} \end{cases},$$

where $\boldsymbol{A}$ is an invertible matrix in $\mathbb{F}_2^{8\times 8}$ and $a, c \in \mathbb{F}_2^8/\{0\}$, $b, d \in \mathbb{F}_2^8$. $S_{new21}(x)$ is a permutation in $\mathbb{F}_{2^n}$ if $ad + bc \neq 0$. The properties of $S_{new21}(x)$ can be found in Table 17.

2.2 An Improved S-Box Structure

The properties of $S_{APA}(x)$ and $S_{new20}(x)$ are greatly enhanced relative to AES-like S-box. In [17], the authors found an 8-bit S-box with better properties (see Table 17). However, the structure $S_{new20}(x)$ has not been further explored. We propose a new structure as an extension of $S_{new20}(x)$ and study the properties of such structures.

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an n-bit S-box. For $x \in \mathbb{F}_{2^n}$, the algebraic expression of $F(x)$ is

$$F(x) = (\alpha + \beta)(\boldsymbol{A}x + \beta)^{-1} + \gamma, \tag{1}$$

where $\alpha \neq \beta$, and $\alpha, \beta, \gamma \in \mathbb{F}_{2^n}$, the matrix $\boldsymbol{A}$ is an invertible matrix in $\mathbb{F}_2^{n\times n}$, the inverse of 0 is 0, that is $F(\boldsymbol{A}^{-1}\beta) = \gamma$.

In the following, the n-bits S-box in Eq. (1) is denoted by $F_{new}^n(x)$. If $\gamma = 0x01$ then $F_{new}^8(x) = S_{new20}(x)$, because

$$S_{new20}(x) = \begin{cases} \dfrac{\boldsymbol{A}x + \alpha}{\boldsymbol{A}x + \beta} = \dfrac{\boldsymbol{A}x + \beta + \alpha + \beta}{\boldsymbol{A}x + \beta} = (\alpha + \beta)(\boldsymbol{A}x + \beta)^{-1} + 1 & \text{if } \boldsymbol{x} \neq \boldsymbol{A}^{-1}\beta \\ 0x01 & \text{if } \boldsymbol{x} = \boldsymbol{A}^{-1}\beta \end{cases},$$

so it is obvious that $S_{new20}(x)$ is a special case of F_{new}^n.

3 Affine Invariant Properties of F_{new}^n

The S-boxes generated by Eq. (1) have the same properties in some respects. In this section, we study its affine invariants.

The number of invertible matrix [26] in $\mathbb{F}_2^{n\times n}$ is $|GL(n, \mathbb{F}_2)| = \prod_{k=0}^{n-1}(2^n - 2^k)$, then the total number of n-bit S-boxes in F_{new}^n can be obtained.

Proposition 1 (The number of F_{new}^n). *Let α, β and $\gamma \in \mathbb{F}_{2^n}$, then the upper bound on the number of S-boxes that can be generated by Eq. (1) is*

$$2^{2n}(2^n - 1)\prod_{k=0}^{n-1}(2^n - 2^k).$$

Table 1. Different parameters generate the same S-box.

α	1	2	3	4	5
β	10	7	13	14	4
$\boldsymbol{A}$	(10, 3, 7, 11)	(11, 1, 3, 7)	(1, 2, 3, 12)	(7, 12, 1, 3)	(13, 15, 6, 8)
α	6	7	8	9	10
β	9	3	15	5	8
$\boldsymbol{A}$	(12, 13, 2, 4)	(6, 14, 5, 15)	(3, 4, 12, 1)	(9, 7, 11, 10)	(8, 5, 15, 6)
α	11	12	13	14	15
β	2	1	11	6	12
$\boldsymbol{A}$	(2, 6, 8, 13)	(4, 8, 13, 2)	(14, 11, 10, 9)	(15, 9, 14, 5)	(5, 10, 9, 14)

Remark 1. In fact, for $n = 2, 3, 4$ and any fixed γ, an S-box generated by Eq. (1) will be repeated $2^n - 1$ times for all invertible matrix $\boldsymbol{A} \in \mathbb{F}_2^{n\times n}$, for all $\alpha \in \mathbb{F}_{2^n}$ and $\beta \in \mathbb{F}_{2^n}$ in our experiments. We find that the number of different S-boxes in F_{new}^n is $2^{2n}|GL(n, \mathbb{F}_2)|$ for $n = 2, 3, 4$. So we have a guess: the number of different S-boxes generated by Eq. (1) is $2^{2n}|GL(n, \mathbb{F}_2)|$ for $n \geq 2$.

Example 1. Let $n = 4$, $\gamma = 7$, the S-box [10,15,9,8,14,5,12,4,1,13,7,2,6,11,0,3] can be generated by 15 different parameters $(\boldsymbol{A}, \alpha, \beta)$ in Table 1. It is important to note that the value of $\boldsymbol{A}$ in Table 1 indicates the four row vectors of matrix $\boldsymbol{A}$. For example, $\boldsymbol{A} = (1, 2, 3, 12)$ means the first row of $\boldsymbol{A}$ is [0, 0, 0, 1], the second row is [0, 0, 1, 0], the third row is [0, 1, 0, 0] and the last row is [1, 1, 0, 0]. This S-box uses the finite field $\mathbb{F}_{2^4} = \mathbb{F}_2[t]/(t^4 + t + 1)$.

In order to prove the equivalence of F_{new}^n and x^{-1} in $\mathbb{F}_{2^n}$, we introduce Lemma 1.

Lemma 1. *Let $a, b \in \mathbb{F}_{2^n}$, then there exists one matrix $\boldsymbol{A}$, s.t. $ab = \boldsymbol{A}\boldsymbol{b}$, where $\boldsymbol{A}$ is an invertible matrix in $\mathbb{F}_2^{n\times n}$.*

The above result means that the multiplication in the finite field $\mathbb{F}_{2^n}$ can be expressed in the form of an affine transformation.

Proposition 2 (Affine Equivalent). *All n-bit S-boxes in F_{new}^n are affine equivalents.*

Proof. Let $x \in \mathbb{F}_{2^n}$, then

$$x^{-1} \sim \boldsymbol{A}^{'}(\boldsymbol{A}x + a)^{-1} + b, \tag{2}$$

where $\boldsymbol{A}, \boldsymbol{A}^{'}$ are invertible matrices in $\mathbb{F}_2^{n\times n}$, $a, b \in \mathbb{F}_{2^n}$.

It is easy to find that Eq. (2) and Eq. (1) are affine equivalents for the same irreducible polynomial in $\mathbb{F}_{2^n}$, if and only if

$$\begin{cases} a = \beta \\ b = \gamma \\ \boldsymbol{A}^{'}(\boldsymbol{A}x + a)^{-1} = (\alpha + \beta)(\boldsymbol{A}x + \beta)^{-1}. \end{cases} \tag{3}$$

Table 2. Representatives of 16 classes of optimal 4-bit S-boxes [16].

Class	Distributions of S-boxes
G_0	0, 1, 2, 13, 4, 7, 15, 6, 8, 11, 12, 9, 3, 14, 10, 5
G_1	0, 1, 2, 13, 4, 7, 15, 6, 8, 11, 14, 3, 5, 9, 10, 12
G_2	0, 1, 2, 13, 4, 7, 15, 6, 8, 11, 14, 3, 10, 12, 5, 9
G_3	0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 5, 3, 10, 14, 11, 9
G_4	0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 9, 11, 10, 14, 5, 3
G_5	0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 11, 9, 10, 14, 3, 5
G_6	0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 11, 9, 10, 14, 5, 3
G_7	0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 14, 11, 10, 9, 3, 5
G_8	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 9, 5, 10, 11, 3, 12
G_9	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 3, 5, 9, 10, 12
G_{10}	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 5, 10, 9, 3, 12
G_{11}	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 10, 5, 9, 12, 3
G_{12}	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 10, 9, 3, 12, 5
G_{13}	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 9, 5, 11, 10, 3
G_{14}	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 11, 3, 9, 5, 10
G_{15}	0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 11, 9, 3, 10, 5

According to Lemma 1, the Eq. (3) always holds. That is

$$F^n_{new}(x) \sim x^{-1},$$

then all n-bit S-boxes in F^n_{new} are affine equivalents. □

Remark 2. For $n = 4$, all S-boxes in F^4_{new} are affine equivalent to G_3 (see in Table 2). The upper bound on the number of S-boxes that affine equivalent to G_3 is 104, 044, 953, 600 ($= 20160 \times 20160 \times 16 \times 16$), and the upper bound on the number of S-boxes of F^4_{new} is 82, 575, 360 ($= 20160 \times 2^{12}$). So F^4_{new} is a subset of G_3 equivalence class.

Remark 3. For $n = 8$, all S-boxes in F^8_{new} are affine equivalent to AES S-box. In fact, it is easy to find from the proof of Proposition 2 that

$$F^8_{new}(x) \sim S_{new20}(x) \sim S_{new21}(x) \sim S_{APA}(x) \sim S_{AES}(x) \sim x^{-1},$$

where $x \in \mathbb{F}_{2^8}$.

The nonlinearity [19] represents the degree of correlation between the S-box and the linear function.

Proposition 3 (Nonlinearity). *The nonlinearity of F^n_{new} is*

$$\mathcal{NL}(F^n_{new}) = 2^{n-1} - 2^{\frac{n}{2}},$$

where n is even.

Table 3. Proposed 4-bit S-box.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F^4_{this}(x)$	13	15	10	6	7	14	9	8	0	5	11	4	3	1	2	12

Differential uniformity [18] describes whether S-boxes can resist differential attacks.

Proposition 4 (Differential Uniformity). *The differential uniformity of* F^n_{new} *satisfies*

$$\mathcal{U}(F^n_{new}) \leq 4$$

Proof. The differential uniformity is an affine invariant, and we have proved that $F^n_{new} \sim S_{APA}$, then the proof is given in [13]. □

Remark 4. In fact, it can be seen from the experiment that

$$\mathcal{U}(F^n_{new}) = \begin{cases} 2 \text{ if } n \text{ is odd,} \\ 4 \text{ if } n \text{ is even.} \end{cases}$$

In general, the higher the algebraic degree [5] of the S-box, the stronger the resistance to algebraic attacks.

Proposition 5 (Algebraic degree). *The algebraic degree of* F^n_{new} *is*

$$Deg(F^n_{new}) = n - 1.$$

4 Proposed S-Box Performance Analysis

We will analyze the characteristics of the proposed S-box in this section from the aspects of Strict Avalanche Criterion (SAC), distance to SAC, periodicity, algebraic complexity and Bit Independence Criterion (BIC).

In the practical encryption algorithm, 4-bit and 8-bit S-boxes are the most commonly used S-boxes. In this section, we focus on the properties of a 4-bit S-box and an 8-bit S-box.

For $n = 4$, we have tested all parameters $(\boldsymbol{A}, \alpha, \beta, \gamma)$. The number of matrices $\boldsymbol{A}$ is 20160 and there are 5,160,960 different S-boxes in total. Finally, we find 131 S-boxes with good properties. Table 3 is a 4-bit S-box proposed by this paper denoted by F^4_{this}, whose parameters are $\boldsymbol{A} = (9, 7, 10, 5)$ and $(\alpha, \beta, \gamma) = (7, 13, 3)$. In addition, F^4_{this} uses the finite field $\mathbb{F}_{2^4} = \mathbb{F}_2[t]/(t^4 + t + 1)$.

For $n = 8$, considering that the number of matrices A is too large to calculate, we just tested all the cyclic invertible matrices (the number is 128), and find 158 S-boxes with good properties. Table 4 is an 8-bit S-box our proposed denoted by F^8_{this}, which parameters are $\boldsymbol{A} = (32, 64, 128, 1, 2, 4, 8, 16)$ and $(\alpha, \beta, \gamma) = (34, 251, 1)$.

F^4_{this} and F^8_{this} will be analyzed in the following section.

Table 4. Proposed 8-bit S-box.

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

4.1 Strict Avalanche Criterion

Strict avalanche criterion (SAC) [25] is a indicator that must be considered in S-box design. In fact, SAC is a diffusion criterion. It requires the S-box satisfy that the probability that any single bit reversed in the input will result in a change in each output bits is 0.5. Therefore, SAC can be described as: Let $F = (f_0, f_1, \ldots, f_{n-1})$ be an S-box, for any $a \in \mathbb{F}_2^n$, and $wt(a) = 1$, satisfies $\sum_{x \in \mathbb{F}_2^n} f_i(x) \oplus f_i(x \oplus a) = 2^{n-1}$, $i \in \{0, 1, \cdots, n-1\}$. We have tested the SAC of the two S-boxes $F^4_{this}(x)$ and $F^8_{this}(x)$, and the results are shown in Table 5 and Table 6, respectively.

Table 5. SAC of F^4_{this}.

Reverse	Bit 3	Bit 2	Bit 1	Bit 0
0001	8	8	8	8
0010	12	8	8	8
0100	8	8	4	8
1000	8	8	8	8

Table 6. SAC of F^8_{this}.

Reverse	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
00000001	132	124	140	128	120	120	128	124
00000010	124	124	124	124	120	120	120	128
00000100	128	132	124	144	132	120	120	120
00001000	124	132	140	128	128	136	136	128
00010000	128	132	132	120	132	128	136	136
00100000	136	124	132	140	124	132	128	136
01000000	136	116	124	128	128	124	132	128
10000000	128	140	116	124	120	128	124	132

Remark 5. For F^4_{this}, we find that 4 occurs 1 time, 8 occurs 14 times and 12 occurs 1 time. For F^8_{this}, 116 occurs 2 times, 120 occurs 10 times, 124 occurs 14 times, 128 occurs 15 times, 132 occurs 11 times, 136 occurs 7 times, 140 occurs 4 times and 144 occurs 1 time.

In generally, the mean value of the SAC matrix is often used to represent the SAC property. However, this expression does not completely account for the SAC of the S-box. For example, 4 and 12 respectively appear once in Table 5, and their effects cancel each other out, resulting in the mean value of SAC is 8.

Describing the diffusion properties of the S-box, distance to SAC is better than the mean value of SAC. The distance to SAC [25] is the sum of bias that the elements in the SAC matrix with respect to 2^{n-1}. That is, let $F = (f_0, f_1, \ldots, f_{n-1})$ be an S-box, for any vectors $x \in \mathbb{F}_2^n$, $a = (a_{n-1}, a_{n-2}, \cdots, a_0) \in \mathbb{F}_2^n$, and $wt(a) = 1$, then

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

One S-box F satisfies SAC if and only if DSAC$(F) = 0$, that is all elements in the SAC matrix is 2^{n-1}.

S-boxes with good diffusion criterion should have a small DSAC. The DSAC values of F^4_{this} and F^8_{this} are shown in Table 7 and Table 8, respectively.

Table 7. DSAC and mean of SAC of 4-bit S-boxes.

	Distance to SAC	Mean of SAC
Optimal value	0	8
F^4_{this} (Table 3)	8	8
PRESENT [3]	32	10
Piccolo [20]	44	8.25
TWINE [23]	28	9.25
QARMA [1]	24	6.5
KLEIN [11]	24	9.5
GIFT [2]	40	10

Table 8. DSAC and mean of SAC of 8-bit S-boxes.

		Distance to SAC	Mean of SAC
Optimal value		0	128
F^8_{this} (Table 4)		324	128.06
AES [8]		432	129.25
SM4 [22]		492	127.94
FOX [14]		688	130.38
AIRA [15]	S_1	432	129.25
	S_2	488	126.88
CLEFIA [21]	S_1	848	138
	S_2	488	126.88
S_{APA} [7]		452	128.19
S_{new20} [17]		328	128.25
S_{new21} [10]		324	130.44

4.2 Periodicity

The periodicity of the S-box [24] is a property about the distribution. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an S-box. For $x \in \mathbb{F}_{2^n}$, the period of x is the smallest r such that $F^r(x) = x$.

A well-distributed S-box should have only one period path, that is the period of the S-box is 2^n. The input x is called a fixed point of S-box if there exist special period $r = 1$ for x. An S-box has a poor periodicity, if fixed points exist for it.

The periodicity of AES S-box is not optimal value, which possible periods are 2, 27, 59, 81 and 87. There is no fixed point in AES S-box, but the minimum period reaches 2. F^4_{this} and F^8_{this} have the largest period 2^n (see in Table 9 and Table 10, respectively).

Table 9. The periodicity of 4-bit S-boxes.

S-box	Periodicity
Optimal value	16
F^4_{this} (Table 3)	16
PRESENT [3]	2, 3, 4, 7
Piccolo [20]	3, 13
TWINE [23]	1, 3, 6
QARMA [1]	1, 2
KLEIN [11]	2
GIFT [2]	7, 9

Table 10. The periodicity of 8-bit S-boxes.

		Periodicity
Optimal value		256
F^8_{this} (Table 4)		256
AES [8]		2, 27, 59, 81, 87
SM4 [22]		1, 2, 3, 6, 9, 24, 35, 56, 120
FOX [14]		1, 2, 8, 21, 94, 120
AIRA [15]	S_1	2, 27, 59, 81, 87
	S_2	2, 3, 9, 21, 36, 64, 121
CLEFIA [21]	S_1	4, 5, 17, 109, 116
	S_2	256
S_{APA} [7]		2, 12, 26, 176
S_{new20} [17]		256
S_{new21} [10]		256

Proposition 6. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an S-box. For $x \in \mathbb{F}_{2^n}$, $a \in \mathbb{F}_{2^n}$, the new S-box $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ has new distribution of periods.*

$$G(x) = \boldsymbol{I}_n F(x) + a,$$

where $\boldsymbol{I}_n$ is an $n \times n$ identity matrix.

Example 2. The periods of S-box $F_1(x) = [12, 5, 6, 11, 9, 0, 10, 13, 3, 14, 15, 8, 4, 7, 1, 2]$ are 2, 3, 4, 7. If $a = 3$, then the periods of new S-box $I_4F_1(x) + 3$ are 15 and 1. However, the S-box $F_2(x) = [11, 2, 15, 13, 0, 14, 4, 5, 6, 10, 7, 8, 9, 12, 3, 1]$ has periods 3, 5, 8. If $a = 6$, then the period of $I_4F_2(x) + 6$ can reach 16.

From Proposition 6, we know that the parameter γ is used to change the periodicity of S-boxes in Eq. (1).

4.3 Algebraic Complexity

An S-box can be uniquely represented as a univariate polynomial. Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be any n-bit S-box. The univariate polynomial representation of F is

$$F(X) = \sum_{i=0}^{n-1} u_i X^i,$$

where $u_i \in \mathbb{F}_{2^n}$. The number of terms of $F(X)$ is defined as the algebraic complexity [5].

The algebraic complexity of the S-box indicates the resistance to interpolation attacks. If the algebraic complexity of the S-box is too small, it may lead to efficient interpolation attacks [12].

The univariate polynomial $F(X) = \sum_{i=0}^{n-1} u_i X^i$ and the algebraic degree of S-box are related as follows [4]: $\mathrm{Deg}(S) = \max\{wt(i), u_i \neq 0\}$. This means that the maximum algebraic complexity is $2^n - 1$ for an n-bit S-box. The algebraic complexity data about F^4_{this} and F^8_{this} are shown in Table 11 and Table 12, respectively.

Table 11. The algebraic complexity of 4-bit S-boxes.

S-box	Algebraic complexity	Inverse Algebraic complexity
Optimal value	15	15
F^4_{this} (Table 3)	15	15
PRESENT [3]	14	13
Piccolo [20]	15	15
TWINE [23]	15	15
QARMA [1]	14	14
KLEIN [11]	14	14
GIFT [2]	15	12

Table 12. The algebraic complexity of 8-bit S-boxes.

		Algebraic complexity	Inverse Algebraic complexity
Optimal value		255	255
F^8_{this} (Table 4)		255	255
AES [8]		9	255
SM4 [22]		255	255
FOX [14]		247	246
AIRA [15]	S_1	9	255
	S_2	9	254
CLEFIA [21]	S_1	247	245
	S_2	253	255
S_{APA} [7]		254	255
S_{new20} [17]		255	254
S_{new21} [10]		255	254

One of the ways to obtain $F(X)$ is using lagrange interpolation in $\mathbb{F}_{2^n}$. The algebraic complexity of AES S-box is 9, which univariate polynomial is

$$S_{AES}(X) = 05X^{254} + 09X^{253} + f9X^{251} + 25X^{247} + f4X^{239} + 01X^{223} + b5X^{191} + 8fX^{127} + 63.$$

However, the algebraic complexity of the inverse of AES S-box is 255, so it is optimal in only one aspect. In fact, the upper bound on the algebraic complexity of AES-like S-boxes is 9 [7]. The algebraic complexity of F^4_{this} and F^8_{this} all reache the upper bound. The coefficients of univariate polynomial of F^8_{this} are shown in Table 13.

Table 13. The coefficients of univariate polynomial of F^8_{this}.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	e9	7e	5d	7b	52	7b	96	8e	11	2e	51	5b	43	0f	ae	0f
1	51	18	a8	d0	ff	1f	be	bd	b2	fb	5c	68	23	ac	56	2d
2	03	d8	57	be	a6	ff	eb	35	fc	17	63	87	95	44	45	70
3	34	b5	dc	75	f8	87	9d	d8	89	ee	14	68	b5	46	0b	9a
4	05	b4	06	aa	cb	66	9b	ef	af	e6	72	4c	fb	6c	33	1c
5	16	21	aa	e6	fd	cb	60	36	6e	05	05	61	ab	9a	0f	f2
6	7d	b4	01	54	6a	e0	14	85	f9	c0	76	32	16	cd	a7	53
7	0a	95	c5	79	dd	6b	d4	4e	6a	a4	93	1d	ca	9d	df	ab
8	f1	f5	64	58	29	91	c9	66	96	5a	f7	e7	e6	aa	95	88
9	f5	f7	c8	01	18	11	0e	a6	21	f5	66	82	14	bd	7f	e5
A	bb	85	f2	1c	4a	fe	a3	f9	2f	a4	63	78	82	fb	3e	62
B	e6	31	3e	3e	3f	ed	5b	43	e3	fd	d4	a1	8b	7e	97	a6
C	f3	c4	58	1f	a5	56	47	c4	a5	84	3c	9d	33	62	a8	a9
D	3f	33	70	14	38	11	4d	03	6b	51	5d	d4	67	92	a4	c7
E	7e	a1	15	f5	a4	86	b4	56	f8	7a	3a	2b	61	13	46	9c
F	e8	1c	e0	44	82	a5	fc	15	8f	19	39	cf	fa	42	33	00

and the univariate polynomial of F^4_{this} is

$$F^4_{this}(X) = 14X^{14} + 4X^{13} + 12X^{12} + 7X^{11} + 11X^{10} + 7X^9 + 10X^8 + 11X^7 + 13X^6 + 13X^5 + 11X^4 + 5X^3 + 15X^2 + 15X + 13.$$

4.4 Bit Independence Criterion

The bit independence criterion (BIC) means that the change in output bits is statistically independent when the input any bit changed. For a good S-box, the

correlation between output bits should be as small as possible. According to the definition of S-box BIC given in [9], we conducted a BIC test on the proposed S-boxes. The experimental results of F^4_{this} and F^8_{this} are shown in Table 14 and 15, respectively.

Table 14. The BIC of S-box F^4_{this}.

	$k=3$	$k=2$	$k=1$	$k=0$
$j=3$	1.0	0.5	0.5	**0.577**
$j=2$	0.5	1.0	0.5	**0.577**
$j=1$	0.5	0.5	1.0	**0.577**
$j=0$	**0.577**	**0.577**	**0.577**	1.0

Table 15. The BIC of S-box F^8_{this}.

	$k=7$	$k=6$	$k=5$	$k=4$	$k=3$	$k=2$	$k=1$	$k=0$
$j=7$	1.0	0.063	**0.126**	0.095	0.094	0.096	0.125	0.094
$j=6$	0.063	1.0	0.124	0.125	0.095	0.096	0.125	**0.126**
$j=5$	**0.126**	0.124	1.0	0.097	0.094	0.1	0.1	0.125
$j=4$	0.095	0.125	0.097	1.0	0.094	0.065	0.095	0.064
$j=3$	0.094	0.095	0.094	0.094	1.0	0.094	0.125	0.096
$j=2$	0.096	0.096	0.1	0.065	0.094	1.0	0.094	0.125
$j=1$	0.125	0.125	0.1	0.095	0.125	0.094	1.0	0.094
$j=0$	0.094	**0.126**	0.125	0.064	0.096	0.125	0.094	1.0

In Table 14 and 15, j and k denote the output bits of the S-box, the elements in the table are the maximum value of the correlation coefficient between j and k, when the input bits $a \in \mathbb{F}_{2^n}, wt(a) = 1$ are changed.

The BIC of the S-box is generally described by the maximum value of the BIC matrix for $j \neq k$, and the optimal value is 0. For the S-boxes F^4_{this}, the maximum BIC value is 0.577. For F^8_{this}, the maximum BIC value is 0.126.

5 Comparison with Some Known S-boxes

In Table 16 and Table 17, we list F^4_{this} and $F_{this}8$ for all properties in this paper, then compared with the S-boxes in some public algorithms or proposed by other scholars. After comparison, it is clear that F^4_{this} and $F_{this}8$ are the best results at present.

Finally, we check the affine equivalence class of the S-boxes. For 4-bit S-boxes in Table 16, it can be seen that only the S-box of GIFT is not optimal. For 8-bit S-boxes in Table 17, it can be seen that the S-boxes with good linear and differential properties are all affine equivalent to AES S-box.

Table 16. Comparison of F^4_{this} with other S-boxes.

	PRESENT [3]	Piccolo [20]	TWINE [23]	QARMA [1]	KLEIN [11]	GIFT [2]	F^4_{this}	Optimal
Nonlinearity	4	4	4	4	4	6	**4**	4
Differential Uniformity	4	4	4	4	4	4	**4**	4
Algebraic Degree	3	3	3	3	3	3	**3**	3
Mean of SAC	10	8.25	9.25	6.5	9.5	10	**8**	8
Distance to SAC	32	44	28	24	24	40	**8**	0
Possible periods	2, 3, 4, 7	3, 13	1, 3, 6	1, 2	2	7, 9	**16**	16
Algebraic Complexity	14	15	15	14	14	15	**15**	15
InverseAlgebraic Complexity	13	15	15	14	14	12	**15**	15
Maximal BIC	1	0.577	0.577	0.577	0.577	1	**0.577**	0
Affine equivalent (see in Table 2)	G_0	G_8	G_3	G_9	G_4	NOT Equivalent	$\boldsymbol{G_3}$	

Table 17. Comparison of F^8_{this} with other S-boxes.

	AES [8]	SM4 [22]	FOX [14]	AIRA [15]		CLEFIA [21]		S_{APA} [7]	S_{new20} [17]	S_{new20} [10]	F^8_{this}	Optimal
				S_1	S_2	S_1	S_2					
Nonlinearity	112	112	96	112	112	100	112	112	112	112	**112**	120
Differential Uniformity	4	4	16	4	4	10	4	4	4	4	**4**	4
Algebraic Degree	7	7	6	7	7	6	7	7	7	7	**7**	7
Mean of SAC	129.25	127.94	130.38	129.25	128.75	138	126.88	128.19	128.25	130.44	**128.06**	128
Distance to SAC	432	492	688	432	400	848	488	452	328	324	**324**	0
Possible periods	2, 27, 59 81, 87	1, 2, 3, 6 9, 24, 35 56, 120	1, 2, 8, 21 94, 120	2, 27, 59 81, 87	2, 3, 9, 21 36, 64, 121	4, 5, 17 109, 116	256	2, 12 26, 176	256	256	**256**	256
Algebraic Complexity	9	255	247	9	9	247	253	254	255	255	**255**	255
Inverse Algebraic Complexity	255	255	246	255	254	245	255	254	254	254	**255**	255
Maximal BIC	0.134	0.135	0.377	0.134	0.134	0.333	0.132	0.129	0.126	0.129	**0.126**	0
Affine equivalence with AES S-box	YES	YES	NO	YES	YES	NO	YES	YES	YES	YES	**YES**	

6 Conclusion

In this paper, we propose a new S-box structure to improve the existing 4-bit and 8-bit S-boxes. The new structure gives more possibilities for improving the Strict avalanche criterion (SAC), distance to SAC, the bit independence criterion (BIC), algebraic complexity, inverse algebraic complexity, and periodicity while maintaining good differential and linear properties. By comparing them with the S-boxes in public algorithms and other improved S-boxes, it can be observed that F^4_{this} and F^8_{this} in this paper have better properties.

Acknowledgements. The first author and the second author were supported in part by the Sichuan Science and Technology Program (No. 2021ZYD0011, 2020JDJQ0076).

References

1. Avanzi, R.M.: The QARMA block cipher family. IACR Trans. Symmetric Cryptol. **2017**(1), 4–44 (2017). https://doi.org/10.13154/tosc.v2017.i1.4-44
2. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Yu., Sim, S.M., Todo, Y.: GIFT: a small present. In: Fischer, W., Homma, N. (eds.) CHES 2017. LNCS, vol. 10529, pp. 321–345. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66787-4_16
3. Bogdanov, A., et al.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74735-2_31
4. Canteaut, A.: Lecture Notes on Cryptographic Boolean Functions. Inria, Paris, France (2016)

5. Carlet, C.: Vectorial Boolean Functions for Cryptography. Boolean Models Methods in Mathematics (2006)
6. Cui, J., Huang, L., Zhong, H., Chang, C., Yang, W.: An improved AES S-box and its performance analysis. Int. J. Innov. Comput. Inf. Control **7**(5), 2291–2302 (2011)
7. Cui, L., Cao, Y.: A new S-box structure named affine-power-affine. Int. J. Innov. Comput. Inf. Control **3**(3), 751–759 (2007)
8. Daemen, J., Rijmen, V.: AES proposal: Rijndael. Gaithersburg, MD, USA (1999)
9. Detombe, J., Tavares, S.: Constructing large cryptographically strong S-boxes. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 165–181. Springer, Heidelberg (1993). https://doi.org/10.1007/3-540-57220-1_60
10. Eddahmani, S., Mesnager, S.: A suitable proposal of s-boxes (inverse-like) for the AES, their analysis and performances. In: Stănică, P., Mesnager, S., Debnath, S.K. (eds.) ICSP 2021. CCIS, vol. 1497, pp. 49–63. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-90553-8_4
11. Gong, Z., Nikova, S., Law, Y.W.: KLEIN: a new family of lightweight block ciphers. In: Juels, A., Paar, C. (eds.) RFIDSec 2011. LNCS, vol. 7055, pp. 1–18. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-25286-0_1
12. Jakobsen, T.P., Knudsen, L.R.: Attacks on block ciphers of low algebraic degree. J. Cryptol. **14**(3), 197–210 (2001). https://doi.org/10.1007/s00145-001-0003-x
13. Jinomeiq, L., Baoduui, W., Xinmei, W.: One AES S-box to increase complexity and its cryptanalysis. J. Syst. Eng. Electron. **18**(2), 427–433 (2007). https://doi.org/10.1016/S1004-4132(07)60108-X
14. Junod, P., Vaudenay, S.: FOX: a new family of block ciphers. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 114–129. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30564-4_8
15. Kwon, D., et al.: New block cipher: ARIA. In: Lim, J.-I., Lee, D.-H. (eds.) ICISC 2003. LNCS, vol. 2971, pp. 432–445. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24691-6_32
16. Leander, G., Poschmann, A.: On the classification of 4 bit S-boxes. In: Carlet, C., Sunar, B. (eds.) WAIFI 2007. LNCS, vol. 4547, pp. 159–176. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73074-3_13
17. Nitaj, A., Susilo, W., Tonien, J.: A new improved AES S-box with enhanced properties. In: Liu, J.K., Cui, H. (eds.) ACISP 2020. LNCS, vol. 12248, pp. 125–141. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-55304-3_7
18. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_6
19. Nyberg, K.: S-boxes and round functions with controllable linearity and differential uniformity. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 111–130. Springer, Heidelberg (1995). https://doi.org/10.1007/3-540-60590-8_9
20. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: *Piccolo*: an ultra-lightweight blockcipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 342–357. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23951-9_23
21. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (extended abstract). In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181–195. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74619-5_12

22. SM4: ISO/IEC 18033–3:2010/AMD 1:2021 information technology—security techniques—encryption algorithms—part 3: block ciphers—amendment 1: SM4 homepage. https://www.iso.org/standard/81564.html
23. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: *TWINE*: a lightweight block cipher for multiple platforms. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 339–354. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-35999-6_22
24. Wang, Y.B.: Analysis of structure of AES and its S-box. J. PLA Univ. Sci. Technol. (Nat. Sci.) (2002)
25. Webster, A.F., Tavares, S.E.: On the design of S-boxes. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 523–534. Springer, Heidelberg (1986). https://doi.org/10.1007/3-540-39799-X_41
26. Wilson, R.A.: The Finite Simple Groups. Springer, London (2009). https://doi.org/10.1007/978-1-84800-988-2