A method for constructing dynamic S-boxes based on fractional transformation

Hoang Duc Tho[1*], Pham Quoc Hoang[1], Nguyen Thi Thu Nga[2], Pham Van Quoc[3]

[1]Academy of Cryptographic Techniques, Viet Nam Government Information Commission, 144 Chien Thang, Thanh Tri, Hanoi, Vietnam;
[2]Graduate University of Sciences and Technology, Vietnam Academy of Science and Technology, 18 Hoang Quoc Viet, Ha Noi, Viet Nam.
[3]VNU University of Science, 334 Nguyen Trai, Thanh Xuan, Hanoi, Vietnam.
[*]Corresponding author: thohd@actvn.edu.vn
Received 24 Sep. 2024; Revised 12 Nov. 2024; Accepted 12 Dec. 2024; Published 25 Dec. 2024.
DOI: https://doi.org/10.54939/1859-1043.j.mst.100.2024.113-119

ABSTRACT

This article describes the method for constructing a dynamic S-box based on fractional transformation on a finite field. The article shows the conditions of S-box, such as S-box is bijective. After that, the article describes S-box properties: nonlinearity, linear approximation probability, differential approximation probability, and algebraic degree. The paper proves that some important cryptographic properties of S-box based on fractional transformation are independent of coefficients a,b,c, d. Based on this, we propose an encryption algorithm with a dynamic S-box.

Keywords: S-box; Fractional transformation; Nonlinearity; Differential probability; Linear probability; Dynamic S-box.

1. INTRODUCTION

S-box plays an important role in block ciphers. In many block ciphers, S-boxes are unique nonlinear parts. Some S-boxes are randomly generated, for example, S-boxes in GOST 28147-89 and in GOST R 34.12-2015. The formula of some S-boxes, such as S-boxes in algorithm DES, is not known. Some S-boxes are generated by algebraic methods such as S-boxes of AES, APA, Gray, Skipjack, Xyi and Residue Prime. The AES S-box is constructed using a combination of the inversion map and an affine transformation. The APA S-box, on the other hand, is designed using a composition of an affine surjection, a power function, and another affine surjection. The Gray S-box is derived from the AES S-box by applying an additional transformation involving binary Gray codes. S-boxes in AES, APA and Gray have nonlinearity equal to 112. For several years, research on the S-box has been based on fractional transformation [3, 5]. In this article, we research S-box based on fractional transformation on GF(2^n). We analyze cryptographic properties of new S-box such as nonlinearity, differential probability, linear probability, and algebraic degree.

2. DEFINITIONS AND PRELIMINARIES

In this section, we introduce some basic definitions.

A function $f: F_2^n \to F_2$ is Boolean function.

We have a definition of vectorial Boolean function $F: F_2^n \to F_2^m$:

$$F(x) = (f_1(x), f_2(x), \dots, f_m(x))$$

with $x = (x_1, x_2, \dots, x_n) \in F_2^n$ and f_i with $1 \le i \le m$ are coordinate Boolean functions.

A S-box $n \times n$ bit is a vectorial Boolean function $S: F_2^n \to F_2^n$.

Nonlinearity of $F: F_2^n \to F_2^n$ is $NL(F)$:

$$NL(F) = 2^{n-1} - \frac{1}{2} max_{v \in F_2^{m*} w \in F_2^n} \left| \sum_{x \in F_2^n} (-1)^{v \cdot F(x) + wx} \right|$$

With $u \cdot v = \sum_i u_i v_i$ is a scalar product.

According to [1], we have inequality: $NL(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. "=" occurs if and only if F is bent function.

Algebraic degree of Boolean function. A coordinate $F_2^n \to F_2$ can be represented in the Algebraic Normal Form (ANF):

$$g(x_1, x_2, \dots, x_n) = a_0 \oplus \sum_{1 \leq i \leq n} a_i x_i \oplus \sum_{1 \leq i < j \leq n} a_{i,j} x_i x_j \oplus \oplus a_{1,2,\dots,n} x_1 x_2 \dots x_n$$

with $a_0, a_i, a_{ij}, \dots, a_{1,2,\dots,n} \in F_2$. S-box $n \times m$ is a map $S: F_2^n \to F_2^m$ and has coordinate functions (S_1, S_2 , ..., S_m). The degree of Boolean function g: $deg(g)$ is a degree of polynomial in ANF. The degree of S-box is minimal of a linear combination of the coordinate Boolean function of S-box:

$$deg(S) = min\{deg\ (c_1 f_1 \oplus c_2 f_2 \oplus \dots \oplus c_m f_m)\}$$

Differential Approximation Probability of S-box.

With $a \in F_2^n$

$$\Delta_{S,a}: F_2^n \to F_2^n$$

x: $S(x) \oplus S(x \oplus a) = b$ *and* $Diff(S) = max_{a \in F_2^n \{0\}, b \in F_2^m} |\Delta_{S,a}^{-1}(b)|$.

We have a definition of Differential Approximation Probability:

$$DP = \frac{\#\{x \in X | S(x) + S(x \oplus \Delta x) = \Delta y\}}{2^n} = \frac{Diff(F)}{2^n}$$

$\Delta x, \Delta y$ are input and output differential. DP is small, algorithm is good against differential analysis.

Linear Approximation Probability is defined as follows:

$$LP = max_{\Gamma_x, \Gamma_y \neq 0} \left| \frac{\#\{x.\Gamma_x = S(x).\Gamma_y\}}{2^n} - \frac{1}{2} \right|$$

Γ_x, Γ_y are input and output masks.

3. GENERATION S-BOX BASED ON FRACTIONAL LINEAR TRANSFORMATION

S-box 8x8 bit is based on GF(2^8). In AES, the irreducible polynomial is

$$\eta(x) = x^8 + x^4 + x^3 + x + 1$$

In this article, we chose an irreducible polynomial is

$$\eta(x) = x^8 + x^6 + x^5 + x^4 + 1$$

S-box is generated by following the formula $g(t) = \frac{at+b}{ct+d}$, with coefficients $a, b, c, d \in GF(2^8)$. We will show the conditions of a, b, c, d such that g exists and is a bijective.

Condition $g(t)$ nonlinear is $c \neq 0$, because if $c = 0$, then

$$g(t) = \frac{at + b}{d} = d^{-1}at + d^{-1}b$$

$g(t)$ is an affine map.

Condition of c, d such that g exists is $ct + d \neq 0, t \neq c^{-1}(-d)$.

Suppose that $t_1 \neq t_2$ such follow:

$$\frac{at_1 + b}{ct_1 + d} = \frac{at_2 + b}{ct_2 + d}$$

$$\leftrightarrow (at_1 + b) \cdot (ct_2 + d) = (at_2 + b) \cdot (ct_1 + d)$$

$$\leftrightarrow act_1t_2 + adt_1 + bct_2 + bd = act_1t_2 + adt_2 + bct_1 + bd$$
$$\leftrightarrow adt_1 + bct_2 - adt_2 - bct_1 = 0$$
$$\leftrightarrow (ad - bc) \cdot (t_1 - t_2) = 0$$

Because $t_1 \neq t_2$, so

$$\frac{at_1 + b}{ct_1 + d} = \frac{at_2 + b}{ct_2 + d}$$
$$\leftrightarrow ad - bc = 0$$

So linear transformation is bijective, when $ad - bc \neq 0$.

We can generate a S-box by the formula

$$g(t) = \frac{at + b}{ct + d} \quad a, b, c, d, t \in GF(2^8)$$

with conditions: $c \neq 0, ad - bc \neq 0$.

In [5], a = 29 = 00011101, b = 15 = 00001111, c = 8 = 00001000, d = 9 = 00001001. Với t = 47, $8 \cdot 47 + 9 = 0 \; mod \; \eta(x)$, with $\eta(x) = x^8 + x^6 + x^5 + x^4 + 1$, we have $g(t)$ such as:

$$g(t) = \frac{29t + 15}{8t + 9}; t \neq 47$$
$$g(t) = 149; t = 47$$

We have a S-box in the next tables.

Table 1. *The values of S-Box.*

$t \in Z_{2^8}$	$t \in GF(2^8)$	$g(t)$
0	00000000	124
1	00000001	18
…	…	…
255	11111111	138

We have built the program and calculated the S-box. The values of the S-box are shown in Fig. 1.

124	18	154	77	3	216	99	81	117	91	112	125	88	32	10	96
227	253	141	194	235	5	111	9	122	37	206	233	156	72	53	51
184	7	20	239	102	22	166	210	192	97	226	27	12	248	79	149
69	59	196	220	132	109	94	168	234	84	15	108	120	52	142	14
25	90	151	205	93	0	26	171	217	41	1	67	224	197	21	198
130	174	231	161	199	153	76	6	144	170	246	221	43	232	29	219
61	229	191	242	195	95	137	225	157	75	39	119	44	98	104	87
115	89	56	110	160	42	31	249	169	222	146	11	245	238	136	247
54	139	200	8	36	46	126	218	121	165	105	16	58	35	135	164
207	230	2	243	63	123	214	80	68	55	183	114	107	208	62	163
252	145	116	250	13	204	127	228	187	113	49	86	159	83	152	244
180	193	57	173	133	128	150	30	40	190	255	240	237	155	85	175
162	47	134	50	60	28	186	177	33	202	176	19	70	209	24	178
71	38	212	48	201	172	129	143	215	188	181	147	158	65	101	100
251	179	182	203	140	223	66	254	64	23	45	189	17	213	131	4
73	211	167	74	78	148	236	185	92	241	82	103	118	106	34	138

Figure 1. *S-Box based on [5].*

4. SECURITY ANALYSIS OF S-BOX BASED ON FRACTIONAL TRANSFORMATION

Proposition 1: Cryptographic properties of S-box $g(t) = \frac{at+b}{ct+d}$: nonlinearity, differential approximation probability, linear approximation probability and algebraic degree are independent of coefficients a, b, c, d.

Proof:

$$g(t) = \frac{at+b}{ct+d} = (at+b)(ct+d)^{-1}$$

Put $ct + d = z \to t = (z-d)c^{-1}$, we have:

$$g(z) = (a(z-d)c^{-1} + b)z^{-1} = (ac^{-1}z - adc^{-1} + b)z^{-1}$$

Put $ac^{-1} = p$, $-adc^{-1} + b = q$, we have:

$$g(z) = (pz+q)z^{-1} = pz \cdot z^{-1} + q \cdot z^{-1} = p \cdot 1 + q \cdot z^{-1}$$

$\leftrightarrow g(z) = q \cdot z^{-1} + p$, with $p, q \in GF(2^8)$.

S-box based on fractional transformation is affine equivalent with S-box based on inverse function.

$$S(z) = \begin{cases} 0, nếu\ z = 0 \\ z^{-1}, nếu\ z \neq 0 \end{cases}$$

So nonlinearity, differential approximation probability, linear approximation probability, algebraic degree of $g(z)$ are the same properties of $S(z)$. If coefficients a, b, c, d are changed, then nonlinearity, differential approximation probability, linear approximation probability are not changed.

In [4], some cryptographic properties of S-box based on the inverse map are shown. We show $Diff(g) = 4$ with n even. Put $\alpha, \beta \in F$ and $\alpha \neq 0$, we have the equation:

$$S(z+\alpha) + S(z) = \beta$$
$$\leftrightarrow (z+\alpha)^{-1} + z^{-1} = \beta$$

With $z \neq 0, z \neq \alpha$, we have:

$$\beta z^2 + \alpha\beta z - \alpha = 0$$

If $\beta = \alpha^{-1}$, then:

$\alpha^{-1}z^2 + \alpha \cdot \alpha^{-1} \cdot z - \alpha = 0$, multiplicate with α, we have :

$$z^2 + \alpha z - \alpha^2 = 0$$

Square both sides, and $z^2 = \alpha z + \alpha^2$, we have:

$$z(z^3 + \alpha^3) = 0$$

If n even, $(2^n - 1) \vdots 3$, put $d = \frac{2^n-1}{3}$, the equation has 4 roots $z = 0$, $z = \alpha$,$z = \alpha^{1+d}$, $z = \alpha^{1+2d}$, so S-box based on inverse function on $GF(2^n)$ with n even has Diff=4 (differential 4-uniform). According to [4], the algebraic degree of S-box based on an inverse map $\deg(S) = n - 1$, with $n = 8, \deg(S) = 7$, Nonlinearity $N(S) \geq 2^{n-1} - 2^{n/2}$.

So that, S-box based on fractional transformation has Diff=4 (with n even), $\deg(S) = n - 1$, and nonlinearity $N(g) \geq 2^{n-1} - 2^{n/2}$, with S-box 8×8: $N(g) \geq 2^7 - 2^4 = 112$.

We use the SageMath (https://sagecell.sagemath.org) program to evaluate these cryptographic properties of the S-box in Fig.1. The results are in complete agreement with the theoretical evaluation above.

5. PROPOSING A METHOD FOR CONSTRUCTING DYNAMIC S-BOXES BASED ON FRACTIONAL TRANSFORMATION

According to proposition 1, important cryptographic properties, such as nonlinearity, differential approximation probability, linear approximation probability, algebraic degree are not changed, when a, b, c, d are changed.

We choose irreducible polynomial on GF(2^8): $\eta(x) = x^8 + x^6 + x^5 + x^4 + 1$.

We modify AES algorithm with dynamic S-box. Propose original key of AES is K_0, the length of K_0 is 128/192/256 bits. After key expansion, we recieve $K_1, K_2, \dots, K_{N_r}$, with N_r is number of rounds 10/12/14.

S-box for the first round, we use bytes of the first round key K_1 for a, b, c, d. We use transposition π_1:(1,...,16)→ (1, ...,16) to choice 4 bytes for a, b, c, d.

Table 2. *Transposition* $\boldsymbol{\pi_1}$.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15

With the transposition, a, b, c, d are the values of the second byte, 4th byte, 6th byte, 8th byte of K_1.

The conditions of S-box based on fractional transformation: $ad - bc \neq 0$ and $c \neq 0$.

If $ad - bc \neq 0$ or $c \neq 0$ are not satisfied, we use:

$$g(t) = \begin{cases} \dfrac{3t+1}{5t+7} & t \neq 47 \\ 114 & t = 47 \end{cases}$$

We propose a modified AES with a S-box that depends on the round key. Two sides secretly distribute the original key and N_r transpositions $\pi_1, \dots, \pi_{N_r}$. These transpositions define positions of bytes for coefficients a, b, c, d. The modified AES are shown in Fig.2.

We evaluate the number of S-boxes based on fractional transformation.

If $a = 0$, $g(t) = \frac{b}{ct+d} \rightarrow b \neq 0$. With $c \neq 0$, we have $ad - bc \neq 0$. Such that, with $a = 0$, we have 255 choices of b, 255 choices c, 256 choices d. With $a = 0$, we have 255.255.256 choices of fractional maps.

If $a \neq 0$, we have 255 choices of a, b has 256 variants, c has 255 variants (because $c \neq 0$), $ad - bc \neq 0 \rightarrow d \neq a^{-1}bc$, so d has 255 choices. In this case, we have 255.256.255.255 choices of fractional maps.

In both cases with one irreducible polynomial, the number of S-box based on a fractional map:

$$255.255.256 + 255.256.255.255 = 255.255.256.256 = 4261478400 \approx 2^{32}$$

We describe the security analysis of block cipher with a dynamic S-box depending on the key. The attackers don't know the S-box of cipher. Therefore, they need to use more data to determine the differential and linear traces. Moreover, it will be much more difficult for the attacker to perform other attacks.

Besides, the S-box is dynamic, but important cryptographic properties are not changed according to proposition 1. This is an advantage over dynamic methods based on chaotic mappings [7, 8]. Since chaotic mapping-based methods cannot preserve the good cryptographic properties of the S-box, these methods often weaken the good cryptographic properties of the S-box.

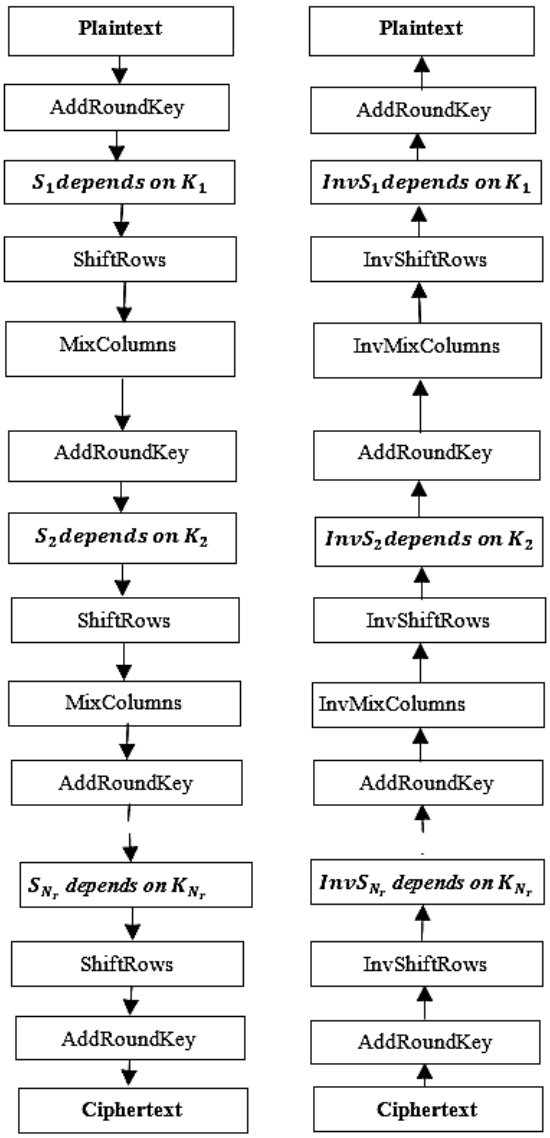

Figure 2. *Modified AES with dynamic S-box.*

With the algebraic attack, according to the authors in [9], the AES and our Modified AES can be defined by $SR(n, r, c, e)$, where:

– n is the number of (encryption) rounds;

– r is the number of "rows" in the rectangular arrangement of the input;

– c is the number of "columns" in the rectangular arrangement of the input;

– e is the size (in bits) of a word.

Then full AES-128 (and Modified AES-128) is equivalent to $SR(10, 4, 4, 8)$. In general, equations for AES can be easily established and the number of equations and variables for different variants are given by [9]:

$$(6n + 1)rce + 2nre + rce$$

Since when the S-box changes, the system of equations will have to be re-established. Therefore, the number of equations required with our modified AES will be

$$2^{32}((6n+1)rce + 2nre + rce)$$

Thus, the algebraic attack resistance of our modified AES is significantly increased.

6. CONCLUSIONS

In this article, the method of constructing dynamic S-boxes with fractions based on formulas is considered. The conditions for fractional mapping exist and the proposed S-box to be bijective are indicated. Also, the article shows that the mapping based on fractions is affine equivalent to the inverse mapping. This allows us to evaluate some of the S-box's cryptographic properties based on Nynberg's inverse mapping in [4]. The article also shows some cryptographic characteristics of S-boxes based on fractional mapping are independent of the coefficients a, b, c, d. Finally, we have proposed a dynamic S-box generation method that preserves some important cryptographic properties with coefficients a, b, c, d calculated from the round key of the cipher. We also show that the algebraic attack resistance of this proposed algorithm is significantly increased. The proposed dynamic method has an advantage over chaotic mapping-based methods in that it preserves the important cryptographic properties of the S-box.

Acknowledgement: *This work has been supported by Academy of Cryptography Techniques*.

REFERENCES

[1]. Claude Carlet, Cunsheng Ding "*Nonlinearities of S-boxes*", Finite Field and Their Applications, (2007).
[2]. L. Cui, Y. Cao "*A new Sbox structure named affine-power-affine*" International journal of Inovative Computing, Information and Control, (2007).
[3]. Iqtadar Hussain, Tariq Shah, M.A. Gondal, W.A Khan "*Construction of Cryptographically Strong 8x8 S-boxes*", World Applied sciences journal, (2011).
[4]. Kaisa Nyberg "*Differentially uniform mappings for cryptography*", Springer-Velag, Berlin Heidelberg, (1994).
[5]. Shabieh Farwa, Tariq Shah, Lubna Idress "*A highly nonlinear S-box based on a fractioanal linear transformation*" Springer plus, (2016)
[6]. Webster AF, Tavares SE "*On the design of Sboxes*", Crypto85, Springer, Berlin, (1986).
[7]. F. J. Luma1, H. S. Hilal and A. Ekhlas, "*New Dynamical Key Dependent S-Box based on chaotic maps*", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 4, Ver. IV, pp. 91-101, (2015).
[8]. Chao Yang, Xia Wei, Cong Wang, "*S-Box Design Based on 2D Multiple Collapse Chaotic Map and their Application in Image Encryption*", Entropy, (2021).
[9]. C. Cid, S. Murphy and M.J.B. Robshaw, *"Small-scale variants of the AES,"* Fast Software Encryption: 12th International Workshop (FSE 2005), Paris, France, Lecture Notes in Computer Science, vol. 3557, pp. 145–162, Berlin: Springer, (2005).

TÓM TẮT

Một phương pháp xây dựng S-hộp động dựa trên biến đổi phân số

Bài báo mô tả phương pháp xây dựng S-hộp động dựa trên phép biến đổi phân số trên trường hữu hạn, chỉ ra các điều kiện của S-box, chẳng hạn như S-box là song ánh. Sau đó, mô tả các thuộc tính của S-box: phi tuyến, xác suất xấp xỉ tuyến tính, xác suất xấp xỉ vi sai, bậc đại số. Bài báo chứng minh rằng, một số tính chất mật mã quan trọng của S-box dựa trên phép biến đổi phân số là không đổi với các hệ số a, b, c, d do tương đương aphin với hộp thế dạng ánh xạ nghịch đảo trên trường hữu hạn. Trên cơ sở đó chúng tôi đề xuất cải tiến thuật toán mã hóa AES với S-box động. Thuật toán mã hóa cải tiến có ưu điểm là khả năng kháng tấn công đại số có thể được cải thiện. Ngoài ra, phương pháp làm động hộp thế được đề xuất cũng không làm giảm đi những tính chất mật mã tốt quan trọng của hộp thế. Vì vậy, phương pháp đề xuất có ưu điểm hơn so với phương pháp làm động dựa trên ánh xạ chaotic.

Từ khóa: S-box; Biến đổi phân số; Phi tuyến tính; Xác suất vi phân; Xác suất tuyến tính; S-box động.