Advances and Applications in Mathematical Sciences
Volume 21, Issue 10, August 2022, Pages 5935-5946

NEW DESIGN OF S BOX BASED ON GALOIS FIELD OF ODD CHARACTERISTIC AND ANALYSIS OF ITS CRYPTOGRAPHIC ATTRIBUTES

P. ABOOBACKER[1] and M. VIJI[2]

[1]Govt. Engineering College
Palakkad-678633, Kerala, India

[2]Department of Mathematics
St. Thomas' College (Autonomous)
Thrissur-680001, Kerala, India
E mail: vijigeethanjaly@gmail.com

Abstract

Block ciphers like Advanced Encryption Standard (AES) employs Nyberg design to construct S box over the Galois field $GF(2^n)$ of even characteristic. This construction is based on binary number system that has only two states 0 or 1. In this paper, we adopt Nyberg design combined with affine power map to construct S boxes on ternary logic. The construction exploits algebraic properties of Galois field $GF(3^n)$, an extension field of $GF(3)$ of odd characteristic. The complexity of the affine map with the extended degree of freedom of the states makes the construction algebraically strong. The proposed S box is of profound quality which is analogous what is characteristically appeared in the existing literature and is having cryptographic traits better than that of binary based construction.

1. Introduction

S Boxes are the heart of the symmetric algorithms which perform substitution. They are the nonlinear components of a block cipher which follows substitution permutation networks. In block ciphers the enhancement of cryptographic strength of a cipher can be achieved by boosting the nonlinear relation between the plaintext and cipher text, and between the

2020 Mathematics Subject Classification: 94A60.
Keywords: S box, Ternary number, Galois field.
[1]Corresponding author; E-mail: backer83@gmail.com
Received May 4, 2021; Accepted July 11, 2022

plaintext and the key (confusion) and also by dissipating the statistics of the plaintext (Diffusion) [1]. S box has a vital role in the security of symmetric block ciphers. The strength of such ciphers depends on the strength of S box.

The computer works on the principles of binary number system which has only two states true or false (on or off). As the states in the many valued logic increases, the algorithms based on many valued logic expand the freedom of choices in block transformations. The development of theory of many valued logic have helped in the emergence of cryptographic algorithms for data security [2]. So, it is promising to think out of the box and develop new cryptographic algorithms based on many valued states.

Ternary logic strengthens the understanding of the concept of confusion and diffusion in research point of view. Even the substitution of a block of small length offers high level of confusion in cryptographic algorithms which is established on ternary logic when compared to those of binary logic. When computation capacity is not a constrain, the algorithms based on many valued logic illuminate the thoughts of the cryptographic community. The quantum computation accelerates the growth of cryptographic algorithms based on ternary logic. S boxes which is the extension of Nyberg construction to Galois field of odd characteristic was discussed in [3].

Bijectivity, nonlinearity, imbalance, strict avalanche criterion and zero correlation are some of the important characteristics of an S box. But it's hard to find an S box which satisfies all this characteristic simultaneously. In this paper we constructed S boxes based on ternary logic and the cryptographic properties are analyzed. It opens new vistas to mathematically secure ciphers based on many valued logic.

2. Preliminaries

Finite fields of order $GF(p^n)$ plays a vital role in designing block symmetric cryptographic algorithms. The method of construction of such a field is addressed in the theorem 4.1 [4]. It claims that.

Theorem 1. *For a prime p and monic irreducible polynomial* $p(x)$ *in* $Fp[x]$ *of degree n, the ring* $Fp[x]/(p(x))$ *is a finite field of order* p^n.

So the construction of $GF(p^n)$ needs a monic irreducible polynomial over $GF(p)$. The number of irreducible polynomials and number of primitive polynomials over $GF(p)$ of degree n is obtained from the formula [5, p.26]. The formula to find the number of irreducible polynomials is

$$\| I_n \| = \frac{1}{n} \sum_{d/n} \mu(d) p^{\frac{n}{d}} \tag{1}$$

and the number of primitive polynomials is,

$$\| P_n \| = \frac{1}{n} \phi(p^n - 1). \tag{2}$$

Cryptographic primitives which are based on ternary number system are operating on extension field $GF(3^n)$ of $GF(3)$. The Galois Field $GF(3^n)$ is constructed by choosing an irreducible(primitive) polynomial over $GF(3)$. When $p = 3$ there are 27 irreducible and 12 primitive polynomials. The elements in the field can be expressed as polynomials of degree at most $n-1$ with coefficients in $GF(3)$. That is,

$$GF(3^n) = \{a_{n-1}x^{n-1} + \ldots a_1 x + a_0,\ a_i \in GF(3),\ i = 0, 2, \ldots, n\}.$$

The elements also expressed as $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$, where $a_i \in \{0, 1, 2\}$.

3. Design Principle of *S* box

The cipher algorithms use two S boxes, one for encryption and the other, inverse for decryption. An S box is a permutation of the elements of the corresponding Galois field. Thus, the mechanism to construct an S box is to find a permutation which satisfies almost all characteristics that is expected for an ideal S box. The structure of the pro-posed S box is adapted from AES S box [6, 7] which follows Nyberg design [8] combined with affine map of the form $S(x) = Ax^{-1} + B$, A is an invertible 8×8 matrix and B is 8×1 matrix over $GF(2)$. In our construction we used the algebraic structure

$S(x) = Ax^7 + B$, where A is an invertible matrix and B is a column matrix over $GF(3)$ with suitable order. The power mapping $x^7 \mod (p(x))$ gives a bijective map over all finite field domains that we used for construction. We constructed four bijective S boxes of size 9, 27, 81 and 243. The Avalanche effect, nonlinearity, imbalance and input output correlation of each S box is computed.

3.1. S box size 9

The S box of size 9 is a permutation of elements in the Galois field $GF(3^2)$. We constructed the field using the irreducible polynomial $p(x) = x^2 + x + 2$ of order two. So the elements are polynomial of degree 1 with coefficients in $GF(3)$ which in turn can be expressed as a_1a_0, where a_0 and a_1 are members in $GF(3)$ as a ternary vector. In our construction we used

$$A = \begin{bmatrix} 0 & 1 \\ 2 & 1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 \\ 2 \end{bmatrix},$$

A is a nondegenerate matrix and B is a column matrix over $GF(3)$. Table 1. is the ternary representation of the proposed S box. It has two components f_1f_2.

Table 1. S box -9.

(a_1, a_0)	00	01	02	10	11	12	20	21	22
$S = f_1(a_1, a_0) f_2(a_1, a_0)$	12	10	11	22	21	01	02	20	00

That is, $S_9 = \{12\ 10\ 11\ 22\ 21\ 01\ 02\ 02\ 00\}$.

3.1.1. Cryptographic characteristics of Proposes S box 6

The propagation criterion and strict avalanche criterion of many valued component functions was described as in [9, 10, 11]. The S box has two component ternary functions. The Table 2. is the calculated values of derivatives of each three valued two component functions at a vector u computed using the formula given in [10, 11].

$$D_u f(x) = (f(x \oplus_q u) - f(x)) \bmod (q), \tag{3}$$

where $\oplus_q$ is the modular q operation. The probability of 0's, 1's and 2's in each component are given in the Table 3. The expected value to satisfy strict avalanche criterion is 0.33.

Table 2. Derivative of component functions.

D_{01}		D_{10}		D_{20}		D_{02}	
f_1	f_2	f_1	f_2	f_1	f_2	f_1	f_2
0	1	1	0	0	2	2	0
0	1	1	1	0	2	1	0
0	1	2	0	0	2	2	2
0	2	1	0	1	2	2	0
1	0	0	2	0	1	2	2
2	1	0	2	2	0	1	0
2	1	1	0	0	1	2	0
1	0	2	0	1	2	0	1
0	2	1	1	2	0	0	1

Table 3. Measures of Strict avalanche Criterion of component functions.

u	01		10		02		20	
	f_1	f_2	f_1	f_2	f_1	f_2	f_1	f_2
0's	0.56	0.22	0.22	0.56	0.56	0.22	0.22	0.56
1's	0.22	0.56	0.56	0.22	0.22	0.22	0.22	0.22
				0.22	0.22	0.56	0.56	0.22
2's	0.22	0.22	0.22					

The values are deviated from the expected value with a standard deviation 0.16. The input output correlation matrix is calculated using the formula given in [12, p.378]

$$\rho_{xy} = \frac{\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{\sqrt{\sum_{i=1}^{n} x_i^2 - (\frac{1}{n}\sum_{i=1}^{n} x_i)}\sqrt{\sum_{i=1}^{n} y_i^2 - (\frac{1}{n}\sum_{i=1}^{n} y_i)^2}}. \quad (4)$$

The matrix P_1 computed according to the formula (5) for the s box of size 9 is

$$P_1 = \begin{bmatrix} 0.2 & 0.2 \\ 0.3 & 0.7 \end{bmatrix}.$$

It is clear that only one pair of input output vector is having more than 50 percentage and all other pairs are having weak correlation.

As a measure of nonlinearity, the notion of nonlinearity distance of valued logic functions was introduced in [13]. The nonlinearity distance of the component p-valued functions on n variables and their Vilenkin-Cherstenson transform ants is related by the formula given in [13]

$$NL = \begin{cases} p^n - Max\,|Wi| & p > 2 \\ p^{n-1} - \frac{1}{2} Max\,|Wi| & p = 2 \end{cases}. \quad (5)$$

Wi is vector of Vilenkin-Chrestenson spectrum of i^{th} component function of the S box, $Wi = f_i \cdot V^*$, where V^* is the conjugate of Vilenkin-Cherstenson transform matrix. For this computation the component function f and the matrix are translated in to complex exponential form using the unique transformation,

$$\{0, 1, 2\} \to \{e^{\frac{2\prod i}{3}0}, e^{\frac{2\prod i}{3}1}, e^{\frac{2\prod i}{3}2}\}.$$

The matrix V is obtained by the recursive formula [14],

$$V_{3^k} = \begin{bmatrix} V_{3^k} & V_{3^k} & V_{3^k} \\ V_{3^k} & V_{3^k}+1 & V_{3^k}+2 \\ V_{3^k} & V_{3^k}+2 & V_{3^k}+1 \end{bmatrix}, \text{ where } V_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}.$$

The nonlinearity of the S box is the minimum of the nonlinearity of the

component functions. The nonlinearity distance of the proposed s box of size 9 is $NL = 3$.

The imbalance of 3 valued (ternary) function was introduced in [15] which is

$$\Delta_f = | n_0 . e^{\frac{2\prod i}{3}0} + n_1 . e^{\frac{2\prod i}{3}1} + n_2 . e^{\frac{2\prod i}{3}2} |, \tag{6}$$

where n_i, $i = 0, 1, 2$ are respectively the number of 0's, 1's and 2's in the component function $f(x)$ as x varies over all possible values. The computation yields zero imbalance for the proposed S box.

3.2. S box size 27

The S box of order 27 is a permutation of elements of $GF(3^3)$. The construction make use of the field constructed using the irreducible polynomial $p(x) = x^3 + 2x^2 + 1$ of order 3. The elements in the field are polynomials of degree at most three, consequently the ternary representation has three components $a_2a_1a_0$. The decimal representation of the field elements contains numbers from 0 to 26. In this construction we used the invertible matrix A and shift vector C,

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 0 & 2 \\ 0 & 2 & 0 \end{bmatrix} \text{ and } C = \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}.$$

The constructed S box in its ternary representation is depicted as the set S_{27}. The ternary blocks from 000 to 222(0 to 26) can be substituted by the values in the set.

S_{27} = {120 020 221 110 111 022 102 100 210 222 001 122 011 112 012

010 002 000 212 021 201 211 200 121 101 202}.

The propagation criterion (avalanche effect) of the components of the S box is computed, the values at each component coming close to the expected value 0.33 of an ideal S box. The absolute deviation of the values from 0.33 is 0.09. The measure of nonlinearity shows that the nonlinearity distance of the

S box is $NL = 18$, higher than the $NL = 11.412$, of the S box constructed by Kim's Scheme [8]. The input output correlation matrix is,

$$P_2 = \begin{bmatrix} 0.17 & 0 & 0.33 \\ 0 & 0.33 & 0 \\ 0.17 & 0.33 & 0.17 \end{bmatrix}.$$

It is observed that there are three 0's and all other values are below 0.5 with a maximum of 0.33. Each component three valued function of the S box is having zero imbalance.

3.3. *S* box size 81

The construction of S box of order 81 utilize algebraic manipulations over the Galois field $GF(3^4)$ in order to produce a permutation of the elements in the field. The field $GF(3^4)$ is constructed as an extension field of $GF(3)$ by picking an irreducible polynomial $p(x) = x^4 + x^3 + 2$ of degree 4 over $GF(3)$. So the elements are polynomials of degree 11 at most 4. The 4×4 invertible matrix A and the shift matrix C used for the construction is

$$A = \begin{bmatrix} 0 & 1 & 2 & 0 \\ 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 1 & 2 & 0 & 1 \end{bmatrix} \text{ and } C = \begin{bmatrix} 2 \\ 0 \\ 2 \\ 1 \end{bmatrix}.$$

The constructed S box, S_{81} is bijective, without any fixed point and with lengthy cycles. Ternary representation of the elements in $GF(3^4)$ and hence in the S box has four ternary components $a_3a_2a_1a_0$.

S_{81} = {1021 1121 1200 2010 0202 2012 0002 0000 21110 0021 0200 1021 2212 0221 0001 1222 1012 1121 2021 1020 2112 1120 1221 1000 0100 2011 2121 2000 1111 0210 1011 0122 1112 0120 0212 2101 1110 1122 2002 2221 2202 1002 2222 1210 2211 0011 0220 2210 2201 2111 2020 1100 2022 1101 0012 2102 1201 2222 0211 2100 1001 2200 2220 2001 0102 2122 1212 1211 0020 0111 0022 0201 1202 0010 1220 2120 0101 1102 0121 1010 0110}.

The avalanche effect of each of the four components is computed and the values gets sharpened to the expected value of 0.33. The values deviate from

the expected value with an absolute deviation of 0.066. The input-output correlation matrix P_3 gives a positive sign as the maximum value of the correlation coefficient is 0.2. The nonlinearity distance of the S box is $NL = 54,$ much bigger than the $NL = 34.235$ of the S box of size 81 in [8].

$$P_3 = \begin{bmatrix} 0.1 & 0.2 & 0.1 & 0 \\ 0 & 0.1 & 0.2 & 0.2 \\ 0.1 & 0.1 & 0 & 0.1 \\ 0.1 & 0.1 & 0.1 & 0.1 \end{bmatrix}.$$

3.4. *S* box size 243

S box of size 243 is a permutation of the elements in the Galois field $GF(3^4)$ which we constructed using the irreducible polynomial $p(x) = x^5 + x^3 + 2x^2 + 1$ over $GF(3).$ Thus, the members of the field are polynomials of degree at most 4. The ternary representation has five components. The nondegenerate matrix and the shift matrix used for construction is

$$A = \begin{bmatrix} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 2 & 1 \\ 1 & 0 & 1 & 0 & 2 \\ 2 & 1 & 0 & 1 & 0 \end{bmatrix} \text{ and } C = \begin{bmatrix} 1 \\ 0 \\ 2 \\ 0 \\ 1 \end{bmatrix}.$$

The ternary Representation of the S box is obtained as,

S_{243} = {10201 11102 02000 12002 20020 20010 11100 20122 00112 01000 10100 01011 12201 01111 21101 02012 12210 22220 12102 22121 10002 21120 11212 11222 11201 22001 22021 21021 20220 21110 22011 01210 11120 10102 10200 10011 20110 10112 01201 01222 02202 11001 21000 02202 12222 00020 21100 22111 00202 11010 21021 01020 00010 20202 02120 22022 00212 00000 00121 10202 01121 12012 02222 20112 01021 02002 22112 00200 22112 00200 00122 20200 00022 22201 10020 02102 11210 21200 22210 12101 22200 22000 22100 20120 21111 01100 11011 10220 01012 01022 12021 11012 20001 21010 00210 11110 02210 12200 10222 22211 00110 10121 10101 21202 10111 02112 11020 00011 20102 12001 21102 02100 21122 22012 21221 11211 02101 02001 10010 00002

12220 10012 22110 21112 20222 12010 12211 22020 00220 02011 02220 02222 10021 01221 01220 00100 01112 21002 00001 21001 20211 00111 02010 11121 22102 12110 10110 21202 11220 11200 02122 20000 20201 20221 12221 11021 10211 02212 20012 01200 01110 12121 01102 00012 01002 10212 02110 22120 02021 02121 22002 11221 10011 20022 21020 20121 12112 10001 00021 02200 11111 00101 12120 21222 10210 12112 22122 12022 00222 20002 12100 12020 20021 12011 01122 20101 00221 22101 00211 12111 21211 12202 21011 02022 10221 00120 21220 11000 10022 11022 01010 00201 00102 02201 22202 12212 10000 12000 11101 02211 01001 02221 11002 01120 22010 01221 20212 11112 20111 22212 22221 21121 21210 21212 01101 20100 10122 02020 11122 20210 01212 21022 10120}.

The images of the elements from 0000 to 2222 (0 to 242 in decimal) is obtained when we move forward through the set S_{243}.

$$P_4 = \begin{bmatrix} 0 & 0 & 0 & 0.1 & 0.1 \\ 0 & 0 & 0.1 & 0 & 0 \\ 0 & 0 & 0.2 & 0.1 & 0 \\ 0 & 0.1 & 0.2 & 0.1 & 0 \\ 0.1 & 0 & 0 & 0 & 0.1 \end{bmatrix}.$$

Cryptographic characteristics of the S box is measured and it is found that the avalanche effect of the components is very close to that expected for an ideal S box. The deviation from the expected value reduced to 0.034. The input-output correlation matrix P_4 has 15 zeros and all other values are close to zero. That is, more than half of the input-output vectors are uncorrelated. The nonlinearity distance according to formula (5) of the proposed S box of size 243 is $NL = 204$.

Table 4. Cryptographic Characteristics of the S boxes.

Size of S box	Bijective/ Invertible	Fixed points	Imbalance	Avalanche effect (Deviation from expected value)	Nonlinearity Distance (NL)	Input output correlation	
						Min	Max
9	Yes	No	0	0.16	3	0.2	0.70

27	Yes	No	0	0.09	18	0	0.33
81	Yes	No	0	0.07	54	0	0.20
243	Yes	No	0	0.03	204	0	0.20

4. Conclusion

The role of an *s* box in a block cipher is to provide confusion. The ternary *S* box is advantageous and overriding over and above binary *s* box as it offers same level of confusion with fewer block length. The *S* box in AES is of size 256 substitute a block of 8 bits by another 8 bits, the ternary *S* box of size 243 offer almost same level of 15 confusion with substitution of block of length 5 trits. The primitives over ternary logic could be used in binary algorithm by converting the binary data to ternary vectors. The binary computers "Setun" and "Setun 70" that uses ternary data representation assures and convince the practicality of ternary technique. The analysis shows as the size of the *s* box increases there is a tendency to satisfy strict avalanche criterion and zero correlation property. The more complex algebraic structure of the proposed *s* boxes makes the cryptanalysis laborious. The nonlinearity and zero correlation properties are analogous to the existing designs. Thus, the constructed ternary *S* box is, therefore an invaluable and pioneering contribution for the posterity.

References

[1] C. E. Shannon, A mathematical theory of cryptography, Bell System Technical Journal 27(3) (1948), 379-423.

[2] O. N. Zhdanov and A. V. Sokolov, Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic, Far East Journal of Electronics and Communications 16(3) (2015), 573-589.

[3] O. N. Zhdanov and A. V. Sokolov, Extending Nyberg Construction on Galois Fields of Odd Characteristic, Radio electronics and Communications Systems © Aller-ton Press, Inc. 60(12) (2017), 538-544.

[4] R. Lidl and H. Niederreiter, Finite Fields (2nd ed., Encyclopedia of Mathematics and its Applications), Cambridge University Press., (1996).

[5] Carlos Cid, Sean Murphy and Matthew Robshaw, Algebraic Aspects of the Advanced Encryption Standard, Springer, Boston, MA (2005).

[6] Joan Daemen and Vincent Rijmen, The Design of Rijndael: AES-The Advanced Encryption Standard, Springer, Berlin (2002).

[7] A. G. Konheim, Cryptography: Primer, John Wiley and Sons, New York (1981).

[8] K. Nyberg, Differentially uniform mappings for cryptography, Advances in cryptology. Proc. of EUROCRYPT'93, Lecture Notes in Computer Science 765(55) (1994).

[9] Sokolov, Artem Zhdanov and Oleg, Avalanche characteristics of cryptographic functions of ternary logic. Radio Electronics, Computer Science, Control. 4 (2019), 177-185.

[10] A. V. Sokolov and O. N Zhdanov, Strict avalanche criterion of four valued functions as the quality characteristic of cryptographic algorithms strength, Siberian, Journal of Science and Technology 20(2) (2019), 183-190.

[11] A. V. Sokolov, Constructive method for the synthesis of nonlinear *S* boxes satisfying the strict avalanche criterion, Radio electron, Commun. Syst. 56(8) (2013), 415-423.

[12] O. N. Zhdanov and A. V. Sokolov, Algorithm of construction of optimal according to criterion of zero correlation non-binary S-boxes, Problems of physics, Mathematics and Technics 3(24) (2015), 94-97.

[13] A. V. Sokolov and N. I. Krasota, Very nonlinear permutations: synthesis method for S-boxes with maximal 4-nonlinearity, Proceeding of ONAT named after A. S. Popov. 1 (2017), 145-154.

[14] M. I. Mazurkov, A. V. Sokolov and N. A. Barabanov, Synthesis method for bent sequences in the Vilenkin-Chrestenson basis, Radio Electronics and Communications Systems 59(11) (2016), 510-517.

[15] A. V. Sokolov and O. N. Zhdanov, The class of perfect ternary arrays, System Analysis and Applied Information Science 2 (2018), 47-54.