International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-10)

Research Article | **October 2015**

A New AES S-box Construction Based on the Logistic Maps

Salim Ali Abbas
Department of Computer Science, College of Education,
Al-Mustansirya University, Baghdad, Iraq

Abstract—

The S-box is an important part in AES algorithm because it only nonlinearity function in the above algorithm, the choice of S-box determines whether the AES algorithm is strength or weakness. Actually, there is no practical attack on the S - box of the original AES, while a new S-box is constructed based on the chaotic logistic maps in this paper for making the fixed S-box able to be dynamic S-box and for increasing the complexity of S-box construction to resistance to any possible attack on the fixed S-box as well as to increase the key space and key sensitivity of the AES algorithm. The experimental results denote that the new S-box has an avalanche effect better than the original S-box in addition to the large key space and key sensitivity of the proposed system..

Keywords— AES, S-box, InvS-box, AVAL

I. INTRODUCTION

The Advanced Encryption Standard is one of most popular symmetric block cipher algorithm designed by two young Belgian, John Daemen and Vincent Rijmen in1998. The AES cipher was announced by the NIST to take the place of the old Data Encryption Standard as new Advanced Encryption Standard. The AES according to the FIPS publication 197 [1] that described more details of AES by The NIST has a plaintext with fixed block size of 128 bits, the data have passed through 10, 12 and 14 rounds, this number of rounds determined by flexible key sizes of 128 bits, 192 bits and 256 bits, respectively.

The AES designed to agree with principles of Substitution-Permutation Network mechanism. Thus it involves some of operations during the encryption and decryption; these operations take 4×4 matrix called the state array which represents 16 byte of data as input. There are four basic operations used over the encryption process to encrypt the plain text which are: Sub-bytes using the Substitution Box (S-box), Shifting Rows, Mixing Columns and XOR'ing with Round Key.

At the decryption process, the inverse of the later stages will be used to decrypt original data which are: InvSubBytes, InvShiftRows, and InvMix-Columns. The sub- keys for each round that used in encryption and decryption processes will be created by using an operation called the key schedule operation [2].

Several searches have been made in the literature toward enhance the AES S-box. So that two Vietnamese researchers and one French researcher are preprocessing the S-box of original AES with Gray code transformation which is special way to represent the binary numbers. The purpose of their method is to improve the algebraic complexity of S-box construction to increase resistance to any possible attacks [3]. Also the proposed system in [4] utilizes both of AES block cipher and RC4 stream cipher to construct new key dependent AES S-box based on key schedule procedure of RC4 algorithm, existing affine transformation of the normal AES S-box and the cipher key. Thereafter rotate the new S-box for substitution bytes stage in each round based on the result of XOR'ing all current round key bytes. As presented in their methodology, it provides high level of security, complexity and requires more time than original AES as well as its dependency on the cipher key. Whilst, the proposed method in [5] uses the first of each round sub key to generate a new AES S-box for each round by XOR'ing each S-box byte with the first byte of the current round key. However, during the decryption process, the same procedure will be used to generate the S-box table which involves XOR operation between the cells of the S-box table and the first cell of the round key, and then find the inverse of S-box table (InvS-box). According to the result of the avalanche effect test which compares between the modified AES and the original AES, the modified AES is more efficient than original AES. While the original AES beats on the modified AES in the speed test. This paper focuses on the S-box construction of the AES algorithm and proposes a new dynamic S-box has more avalanche effect and complexity than the original S-box based on the two logistic chaotic maps.

II. S-BOX OF THE AES ALGORITHM

The Sub-Byte function uses a substitution table (S-box) to substitute the bytes of state array. The byte substitution step used to increase the security level of AES algorithm because it agrees with nonlinearity requirement [6]. The way to implement the Sub-Byte step is corresponding each byte value in 4×4 matrix of data (state array) with the index value of S-box table that shown in Table (1). To explain the Sub-byte operation we will take the first byte of the state array as obtained in Figure (1) which is 95, and make this value as index to the S-box table where (X=9 and Y=5

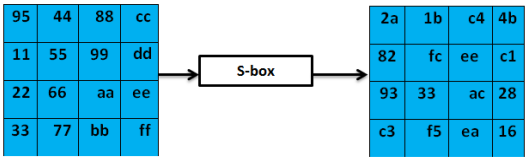


Figure (1): The Bytes Substitution operation.

In the decryption process, the InvS-box table will be used to implement Inverse Sub-Byte operation. To explain this operation, take the first byte in the substituted state that shown in Figure (1) which is (2a) and correspond it with index of InvS-box in Table (2), then set the value of that index (95) as first byte of the state array.

Table (1): Matching of (95) with its value in the AES S-box table

x \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FC	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	C5	F1	71	D8	31	15
3	04	C7	23	E3	18	96	O5	9A	07	12	80	C2	CB	27	B2	75
4	09	83	2C	1A	1B	6C	5A	A0	52	3B	D6	B3	29	C3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BC	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	B9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	CC	5F	97	44	17	C4	A7	7C	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	CC	B8	14	DC	5C	0B	DB
A	C0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	C4	79
B	C7	C8	37	6D	8D	D5	4C	A9	FC	56	F4	CA	65	7A	AC	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3C	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9C
E	C1	F8	98	11	69	D9	8E	94	9B	1C	87	C9	CC	55	28	DF
F	8C	A1	89	0D	BF	C6	42	68	41	99	2D	0F	B0	54	BB	16

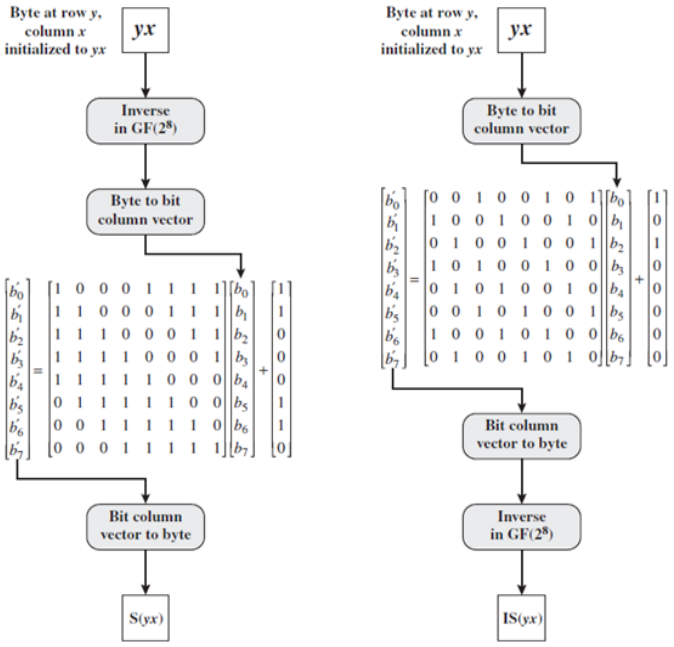
.

The table of S-box was constructed by taking the inverse of multiplicative in the GF (2^8) and affine transformation, respectively as obtained in [2]. The element (00) is its own inverse. Affine transformation involves the multiplication of arrays followed by XOR'ing of vectors, as shown in Figure (2.a).

The way of building InvS-box table similar to that used in S-box table but substituting the affine transformation with its inverse and perform The inverse of affine transformation before apply the multiplicative inversion, as shown in Figure (2. b).

Table (2): Matching of (2a) with its value in the AES Inv S-box table.

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



a) Calculation of byte at row y, column x of S-box.

b) Calculation of byte at row y, column x of InvS-box.

Figure (2): Construction both of S-box and InvS-box [27].

III. CHAOTIC LOGISTIC MAP

The noticeable properties of chaotic systems which are sensitivity to the control parameters values and initial conditions, unpredictability and their capability of generating random numbers made them used over the last years in much cryptosystems [7]. The one-dimensional logistic map is a simple non-linear chaotic map that shows random behavior. Which is proposed by Pierre Verhulst in 1845, and it becomes more popular where it was exploited by the biologist Robert M. May in 1979 [8]. The logistic map equation is expressed as below [9]:

$$x_{n+1} = \lambda . x_n . (1 - x_n) \quad (1)$$

Where λ is the control parameter which affects the chaotic behavior and it is positive number and takes values up to 4, the initial value is xn which takes number in the interval (0, 1) and n is the number of rounds.

The logistic map characteristics depend on the number of the bifurcation parameter λ as shown in Figure (3) where the number of λ represents by horizontal axis and the number of xn represents by vertical axis. A detailed analysis of this bifurcation diagram leads to the following conclusions about the logistic map [8, 10]:

a. The same results will be appeared after several iterations if $\lambda \in$ [0, 3), which mean the chaotic behavior is evanesced.
b. The system appears periodicity if $\lambda \in$ [3, 3.57).
c. Most of the λ values after 3.57 or which $\in$ (3.57, 4] become a chaotic system with periodicity die out.

For that the chaotic behavior will increase the greater the value of the variable.

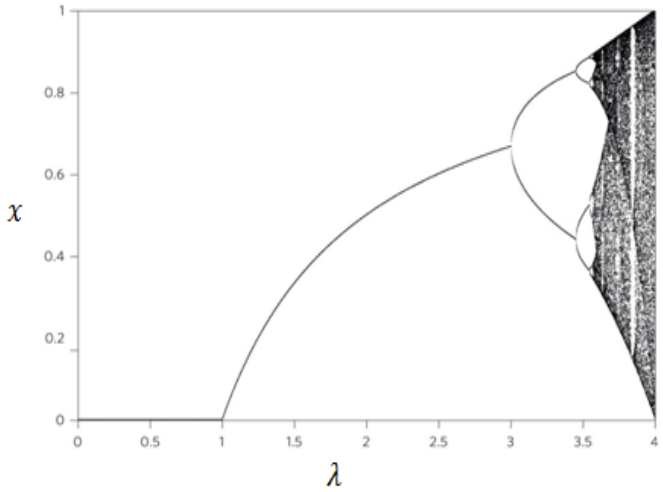


Figure (3): The bifurcation diagram for the logistic map [8].

IV. THE PROPOSED METHOD

The table of the new S-box consists of three different elements which are: take the multiplicative inverse over GF (2^8) followed by multiplying with chaos based Affine matrix and then addition with chaos vector. The rational for using chaos vector is to remove fixed point and to overmuch the S-box complexity. The new S-box is constructed by composing the following transformations.

a. Generate one byte (Y) based on the hexadecimal value of the division remainder of the last three digits of the logistic map output on 256 to speed up the process of generating S-box and due to the high changing in the last three numbers of outputs real values, then get the bit sequence of generating byte (Y) is (Y_7, Y_6, Y_5, Y_4, Y_3, Y_2, Y_1, Y_0), where (Y_0) is the least significant bit (LSB) and (Y_7) is the most significant bit (MSB).
b. Construct 8×8 matrix (Affine matrix) based on the shifting and rearranging operation for the generated byte (Y) as obtained in Figure (4). The shifting and arranging of the generated byte is shifting the sequence of bits (Y_7, Y_6, Y_5, Y_4, Y_3, Y_2, Y_1, Y_0) one bit to the left side, and continuances on the same a fashion to complete 8×8 matrix. In other words, shifting the original bits one bit to the left side for eight times.

$$\begin{bmatrix} Y0 & Y7 & Y6 & Y5 & Y4 & Y3 & Y2 & Y1 \\ Y1 & Y0 & Y7 & Y6 & Y5 & Y4 & Y3 & Y2 \\ Y2 & Y1 & Y0 & Y7 & Y6 & Y5 & Y4 & Y3 \\ Y3 & Y2 & Y1 & Y0 & Y7 & Y6 & Y5 & Y4 \\ Y4 & Y3 & Y2 & Y1 & Y0 & Y7 & Y6 & Y5 \\ Y5 & Y4 & Y3 & Y2 & Y1 & Y0 & Y7 & Y6 \\ Y6 & Y5 & Y4 & Y3 & Y2 & Y1 & Y0 & Y7 \\ Y7 & Y6 & Y5 & Y4 & Y3 & Y2 & Y1 & Y0 \end{bmatrix}$$

Figure (4): The constructed matrix.

c. Generate a new byte (Z) by using logistic map in the same above way, then it is represented by the vector (Sigmal vector) that arranged with the least significant bit first sorting as follows (Z_0, Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7).
d. In ascending sort and row by row starting with byte value {00} that mapped into itself to {FF}, find the multiplicative inverse for each byte in the Galois Field (2^8).
e. Each byte (X) after taking its multiplicative inverse in GF (2^8) consists of 8-bits (X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0), that will be sorted by least significant bit first sort and save them in a vector.
f. Multiplying the vector of bit sequence (X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7) with 8×8 matrix that constructed in (b). As shown in Figure (5).

$$\begin{bmatrix} X'0 \\ X'1 \\ X'2 \\ X'3 \\ X'4 \\ X'5 \\ X'6 \\ X'7 \end{bmatrix} = \begin{bmatrix} X0 \\ X1 \\ X2 \\ X3 \\ X4 \\ X5 \\ X6 \\ X7 \end{bmatrix} \begin{bmatrix} Y0 & Y7 & Y6 & Y5 & Y4 & Y3 & Y2 & Y1 \\ Y1 & Y0 & Y7 & Y6 & Y5 & Y4 & Y3 & Y2 \\ Y2 & Y1 & Y0 & Y7 & Y6 & Y5 & Y4 & Y3 \\ Y3 & Y2 & Y1 & Y0 & Y7 & Y6 & Y5 & Y4 \\ Y4 & Y3 & Y2 & Y1 & Y0 & Y7 & Y6 & Y5 \\ Y5 & Y4 & Y3 & Y2 & Y1 & Y0 & Y7 & Y6 \\ Y6 & Y5 & Y4 & Y3 & Y2 & Y1 & Y0 & Y7 \\ Y7 & Y6 & Y5 & Y4 & Y3 & Y2 & Y1 & Y0 \end{bmatrix}$$

Figure (5): Multiplying the input sequence against the constructed matrix.

Note: Actually, the multiply operation of the input sequence vector against the constructed matrix is logical AND between the input sequence (X) and matrix rows (R) followed by XOR'ing against each other for the result bits (B`) to find the final result (X`), as in following formula:

$X : X_0\ X_1\ X_2\ X_3\ X_4\ X_5\ X_6\ X_7$
$R_0 : Y_0\ Y_7\ Y_6\ Y_5\ Y_4\ Y_3\ Y_2\ Y_1$
$X`_0: B`_0\ B`_1\ B`_2\ B`_3\ B`_4\ B`_5\ B`_6\ B`_7$
$R_1 : Y_1\ Y_0\ Y_7\ Y_6\ Y_5\ Y_4\ Y_3\ Y_2$
$X`_1: B`_0\ B`_1\ B`_2\ B`_3\ B`_4\ B`_5\ B`_6\ B`_7$
$R_2 : Y_2\ Y_1\ Y_0\ Y_7\ Y_6\ Y_5\ Y_4\ Y_3$
$X`_2: B`_0\ B`_1\ B`_2\ B`_3\ B`_4\ B`_5\ B`_6\ B`_7$
$R_3 : Y_3\ Y_2\ Y_1\ Y_0\ Y_7\ Y_6\ Y_5\ Y_4$
$X`_3: B`_0\ B`_1\ B`_2\ B`_3\ B`_4\ B`_5\ B`_6\ B`_7$
$R_4 : Y_4\ Y_3\ Y_2\ Y_1\ Y_0\ Y_7\ Y_6\ Y_5$
$X`_4: B`_0\ B`_1\ B`_2\ B`_3\ B`_4\ B`_5\ B`_6\ B`_7$
$R_5 : Y_5\ Y_4\ Y_3\ Y_2\ Y_1\ Y_0\ Y_7\ Y_6$
$X`_5: B`_0\ B`_1\ B`_2\ B`_3\ B`_4\ B`_5\ B`_6\ B`_7$
$R_6 : Y_6\ Y_5\ Y_4\ Y_3\ Y_2\ Y_1\ Y_0\ Y_7$
$X`_6: B`_0\ B`_1\ B`_2\ B`_3\ B`_4\ B`_5\ B`_6\ B`_7$
$R_7 : Y_7\ Y_6\ Y_5\ Y_4\ Y_3\ Y_2\ Y_1\ Y_0$
$X`_7: B`_0\ B`_1\ B`_2\ B`_3\ B`_4\ B`_5\ B`_6\ B`_7$

g. Add sorted bits of byte (Z) with the final result bits of previous step ($X`_0$, $X`_1$, $X`_2$, $X`_3$, $X`_4$, $X`_5$, $X`_6$, $X`_7$). At the end rearrange the result vector with the most significant bit first sorting (MSB), as obtained in Figure (6).

$$\begin{bmatrix} X'0 \\ X'1 \\ X'2 \\ X'3 \\ X'4 \\ X'5 \\ X'6 \\ X'7 \end{bmatrix} = \begin{bmatrix} X'0 \\ X'1 \\ X'2 \\ X'3 \\ X'4 \\ X'5 \\ X'6 \\ X'7 \end{bmatrix} \oplus \begin{bmatrix} Z0 \\ Z1 \\ Z2 \\ Z3 \\ Z4 \\ Z5 \\ Z6 \\ Z7 \end{bmatrix}$$

$[X`_0\ X`_1\ X`_2\ X`_3\ X`_4\ X`_5\ X`_6\ X`_7] = [X`_7\ X`_6\ X`_5\ X`_4\ X`_3\ X`_2\ X`_1\ X`_0]$

Figure (6): The addition operation for the vectors and rearrange the result.

V. AVALANCHE EFFECT CRITERION (AVAL) FOR FMAES S-BOX

The avalanche effect criterion (AVAL) means that a significantly change will happen in the output bits, if only one bit is changed [4, 5]. Thus, it is an important property for block cipher algorithms. This test will be applied on the original AES S-box and FMAES S-box which constructed when the initial conditions of the logistic maps are (X0 = 0.1, Y0 = 0.1) and its parameters are (r1 = 3.8, r2 = 3.8) that shown in Table (3), while its inverse is shown in Table (4). However, the initial clear text is (00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF) and the cipher key is (01 23 45 67 89 AB CD EF 01 23 45 67 89 AB CD EF).

$$\text{AVAL} = \frac{\textit{number of bits flipped bits in cipher text}}{\textit{number of bits in cipher text}} \quad \ldots (2)$$

The comparison result between the original S-box and the new S-box indicates that the proposed method provides high degree of the avalanche effect than the original method as shown in Table (5) and Table (6).

Table (3): The new S-box table.

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

Table (4): The InvS-box table of new S-box.

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

Table (5): AVAL measure of the original AES S-box.

Index of changed bit	Clear text	Encrypted text	AVAL
0	00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF	49 8d dc 37 00 91 17 16 3a 5e 3f f1 fb ac 1b 36	
1	00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FE	6c 33 4c 75 3a f7 8f d6 23 ce 0e ec c5 3d c1 01	0.4375
45	00 11 22 33 44 55 66 77 88 99 BA BB CC DD EE FF	a0 c1 d3 7b c6 b4 28 29 b2 30 76 4a 26 28 03 2f	0.4922
128	80 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FE	f8 16 93 30 3d 59 7d 2f 3e 40 71 c7 49 54 10 b4	0.4688

Table (6): AVAL measure of the new AES S-box.

Index of changed bit	Clear text	Encrypted text	AVAL
0	00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF	68 fe 1c d1 77 a9 08 cb 0a 61 1e 50 f9 95 dc 4c	
1	00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FE	22 d6 95 36 9a 8a 30 20 d7 ce 5c 7c ef a7 c9 d0	0.4844
45	00 11 22 33 44 55 66 77 88 99 BA BB CC DD EE FF	88 cf 49 2b 98 0b 94 ec 8c c4 77 2c ee dc 01 13	0.5391
128	80 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FE	6b 30 c6 a5 84 63 d1 a9 56 bc 70 ce b0 df ae 8d	0.5234

VI. KEY ANALYSIS

a. Key Space

In addition to the key space of the AES algorithm which is (2^{128}, 2^{192} or 2^{256}), the logistic maps that used for S-box construction provide additional key space for the AES algorithm. The two logistic maps provide two real initial conditions and two real control parameters, where each one of them represented by 64 bits. Therefore, the modified AES has large key space than the original AES so that it has (2^{384}, 2^{448} or 2^{512}) as key space.

b. Key Sensitivity

Any slight change for the secret key will lead to another cipher text quite different from the previous cipher text for example when the plain text (00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF), cipher key (01 23 45 67 89 AB CD EF 01 23 45 67 89 AB CD EF), the initial conditions of the logistic maps are (X0 = 0.1, Y0 = 0.1) and its parameters are (r1 = 3.8, r2 = 3.8), the cipher text will be (49 8d dc 37 00 91 17 16 3a 5e 3f f1 fb ac 1b 36). However, when the plain text (00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF), cipher key (01 23 45 67 89 AB CD EF 01 23 45 67 89 AB CD EF) and the control parameters of the logistic maps are (r1 = 3.8, r2 = 3.8) but the logistic maps initial conditions are(X0 = 0.1, Y0 = 0.2), the cipher text will be (97 a9 97 27 46 de 3c fd e8 77 52 2f 71 5b 5c 83).

VII. CONCLUSION

Actually, the S-box is core of the AES algorithm because it only nonlinearity element in the AES algorithm. In another hand, the remarkable properties of the chaotic maps make them more suitable for the cryptography purposes. Thus, the proposed method focuses on the AES S-box to construct a new S-box based on logistic maps. As well as its complexity and its ability to change depending on the user input, the new S-box has an avalanche effect better than the original S-box. Hence the new S-box is more secure than the AES S-box in the resistance against the differential and linear cryptanalysis.

In addition to the advantages of the new S-box, the modified AES with new S-box provides large key space and key sensitivity than the original AES algorithm.

and then replace the values of the state bytes with the values of S-box bytes that referred by X and Y.

REFERENCES

[1] National Institute of Standards and Technology, "Advanced Encryption Standard", NIST FIPS PUB 197, November 2001.

[2] Christof Paar and Jan Pelzl, "Understanding Cryptography, A Textbook for Students and Practitioners", Springer, 2009.

[3] M.T. Tran, A.D. Duong and D.K. Bui, "Gray S-box for Advanced Encryption Standard", International Conference on Computational Intelligence and Security, IEE, December 2008.

[4] S. Shivkumar and G. Umamaheswari, "Performance Comparison of Advanced Encryption Standard (AES) and AES key dependent S-box - Simulation using MATLAB", Process Automation, Control and Computing (PACC), IEEE, July 2011.

[5] S. Sabah, F. Nejad and A. Jam, "Analysis of Avalanche Effect on Advance Encryption Standard by Using Dynamic S-Box Depends on Rounds Keys", International Conference on Computational Science and Technology, IEEE, August 2014.

[6] William Stallings,"Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Prentice Hall publishing ,2011.

[7] M. G. Avasare and V. V. Kelkar, "Image Encryption using Chaos Theory", International Conference on Communication, Information & Computing Technology (ICCICT), IEEE, 2015.

[8] M. Mohammad Maqableh, " Analysis and Design Security Primitives Based on Chaotic Systems for eCommerce", Ph.D Thesis, University of Durham, School of Engineering and Computing Sciences,UK, 2012.

[9] Hossam Eldin H. Ahmed and Ayman H. Abd El-aziem, "Image Encryption Using Development of Chaotic Logistic Map Based on Feedback Stream Cipher", Recent Advances In Telecommunications, Informatics And Educational Technologies, Egypt, 2014.

[10] S. N. Al Saad and E. Hato, "A Speech Encryption based on Chaotic Maps", International Journal of Computer Applications, May 2014.

