S-boxes generated using Affine Transformation giving Maximum Avalanche Effect

Chandrasekharappa T.G.S., Prema K.V. and Kumara Shama
Department of Electronics and Communication Engineering
Manipal Institute of Technology
Manipal - 576104 INDIA

tgscmpl@gmail.com

Abstract:

The Advanced Encryption Standard (AES) was published by National Institute of Standards and Technology (NIST) in November 2001, to replace DES (Data Encryption Standard) and Triple DES. The S-box (Substitution box) used in AES is designed to be resistant to known cryptanalytic attacks [1][2]. The property of the S-box is that the output cannot be described as a simple mathematical function of the input. The S-box is designed to provide good avalanche effect. The Avalanche Criteria of S-box depends on the generator matrix A used in affine transformation to construct the S-box. This paper investigates the construction of S-boxes by affine transformation which satisfy maximum Avalanche Criteria.

Keywords: **Affine transformation, AES algorithm, Irreducible polynomial, Avalanche Criteria, S-box.**

1. Introduction:

The S-box, constructed in AES algorithm uses the Affine transformation

$$y = Ax \oplus C \mod m(x) \qquad (1).$$

where A is an 8 x 8 matrix with entries in GF(2) and C is a column matrix in GF(2), m(x) is an irreducible polynomial in GF(2^9). The entries used in A matrix are

$$[f8_h; 7c_h, 3e_h, 1f_h, 8f_h, c7_h, e1_h, f1_h]^T \text{ and } C = [63_h]^T \qquad (2)$$

To be useful as S-box generator, matrix A should be non-singular. We can generate approximately 2^{63} such non-singular matrices with each irreducible polynomials. The polynomials that result in non-singular matrices are bound by $[01; 02; 04; 08; 10; 20; 40; 80]^T$ on lower end and $[fe_h, 7f_h, bf_h, df_h, ef_h, f7_h, fb_h, fd_h]^T$ on higher end.

As per Avalanche criteria a one bit change in input should result in at least 50% changes in the output bits. A cryptographic function which satisfies above condition is said to be satisfying Strict Avalanche Criteria if and only if a one bit change in input should result in exactly 50% change in the output bits [4][6]. In this work we construct different S-boxes using Affine transformation and different irreducible polynomials for GF(2^8) and test them for Avalanche Criteria property.

The rest of the paper is organized as follows. In second section, the S-box construction using Affine transformation is briefed. Section three deals with calculation of Avalanche Criteria for the S-boxes. Section four classifies the polynomials into different difference distribution vectors. Section five gives the possible S-boxes which results in Avalanche Criteria of more than 50% .
In section six the experimental results are discussed. Section seven concludes the paper.

2. S-box generation using Affine Transformation:

The steps involved in generating a S-box for AES algorithm, using an Affine transformation are as follows:

Step 1. S-box is a 16_16 matrix. Initialize the _rst row with [00]; [01]; [02]:::[0f], second row with [10]; [11]; [12]:::[1f] and so on with last row as [f0]; [f1]; [f2]:::[ff].

Step 2. Map each byte into its multiplicative inverse with any one of the irreducible polynomials m(x), with [00] mapped to itself.

Step 3. Using Affine transformation in equation(1) , construct S-box with polynomials given in equation(2). The corresponding S-box is shown in Table1.It is possible to construct different S-boxes using different A (A must be a non-singular matrix), C and irreducible polynomials m(x).

3. Avalanche Criteria calculation for the S-boxes generated by affine transformation:

For a given function f, the Avalanche Criteria is given by

$$S_i(f) = \sum_{x \in GF(2^8} f(x) \oplus f(x \oplus e_i \qquad (3)$$

where e_i's the vector having only one entry as '1' in the i^{th} position, $S_i(f)$ are called difference distribution vectors of f. In this case $y = Ax \oplus C \mod m(x) \qquad (1).$

$$(x, y, f(x)) \in GF(2^8) \quad and \quad i \in (1,2,3...8)$$

It is shown in [3][4][5] that 'f' satisfies the SAC if and only if $S_i(f) = 2^{n-1} = 128$ for all $i \in (1,2,\ldots 8)$. Table2 shows the Avalanche criteria values calculated for the S-box of AES algorithm shown in Table1.

Table 1 The AES S-box

	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	FE	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	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	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	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1E	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Table 2 Avalanche Criteria for the AES S-box in Table1.

	S8	**S7**	**S6**	**S5**	**S4**	**S3**	**S2**	**S1**
00000001	128	116	124	116	144	116	132	132
00000010	136	128	116	124	128	144	124	120
00000100	128	136	128	144	120	128	132	132
00001000	140	128	136	128	116	120	136	136
00010000	136	140	128	128	132	116	128	116
00100000	136	136	140	120	120	132	132	116
01000000	124	136	136	120	132	120	136	136
10000000	132	124	136	124	136	132	144	132

In this S-box generation the A matrix is constructed with the polynomials from eqn.(2). From the difference distribution vectors[3] it is found that , the polynomials f8 and e3 belongs to S_7, 7c and 3e to 6, 8f and f1 to S_5, c7 to S_4 and 1f to S_3. The respective Avalanche Criteria values ≥ 128 are 2 x 7 + 2 x 6 + 2 x 5 + 1 x 4 + 1 x 3 = 43 . It follows that the total number of entries

which give Avalanche Criteria value ≥ 128 are 43 out of total 64 entries in Avalanche Criteria Table2, which is 71.88% .

Now consider the A matrix which consists of 8 x 8 entries $\in$ GF(2) , treating each row as a polynomial entry of one byte $\in$ GF(2^8) , test for the Avalanche Criteria of each entry. Table3 shows the number of polynomials that satisfies the difference distribution vectors of S, for irreducible polynomial $11b_h$.

Table 3 Number of polynomials satisfy S.

S_8	S_7	S_6	S_5	S_4	S_3	S_2	S_1
04	26	54	61	67	35	08	01

Consider all the four polynomials from S_8 which gives Avalanche Criteria ≥ 128 in 8 places. Select remaining four polynomials from group S_7, such that A matrix generated from all the 8 polynomials is a non-singular matrix. The polynomial from group S_7 give Avalanche Criteria ≥ 128 in 7 places. The total number of entries which satisfy Avalanche Criteria are 8 x 4+7 x 4 = 60, out of 64 entries and it is 93.75% .

It is possible to select four polynomials at a time out of 26 available polynomials from group S_7, after selecting all four polynomials from group S_8. Now $26C_4 = 14950$ possible combinations are there to construct 8 x 8 A matrices. It is found that only 4915 combinations will give non-singular matrices. It is possible to construct at most 4915 S-boxes which give 93.75%

Avalanche Criteria with irreducible polynomial $m(x)=11b_h[3]$.

As on example consider the first four polynomials 22_h, 25_h, $4a_h$ and 95_h from group S_8 and remaining four polynomials 04_h, 09_h, 12_h and $f8_h$ from group S_7 and construct the A matrix and any arbitrary constant $C = c5_h$. The respective S-box and its Avalanche Criteria are shown in Table4 and Table5 respectively.

Table 4 The AES S-box which gives 93.75% Avalanche Criteria.

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

Table 5 Avalanche Criteria for the AES S-box in Table 4.

	S8	**S7**	**S6**	**S5**	**S4**	**S3**	**S2**	**S1**
00000001	140	132	136	140	140	132	132	128
00000010	132	136	140	132	132	132	128	136
00000100	136	140	132	140	132	128	136	128
00001000	132	132	140	128	128	136	120	140
00010000	140	140	128	128	136	120	132	136
00100000	140	128	128	136	120	132	136	136
01000000	128	128	136	132	132	136	140	124
10000000	132	136	132	140	136	140	132	132

4. Classification of polynomials based on irreducible polynomials for maximum Avalanche Criteria.

There are 30 irreducible polynomials in GF(2^9) and they are $11b_h$, $11d_h$, $12b_h$, $12d_h$, 139_h, $13f_h$, $14d_h$, $15f_h$, 163_h, 165_h, 169_h, 171_h, 177h, $17b_h$, 187_h, $18b_h$, $18d_h$, $19f_h$, $1a3_h$, $1a9_h$, $1b1_h$, $1bd_h$, $1c3_h$, $1cf_h$, $1d7_h$, $1dd_h$, $1ef_h$, $1f3_h$, the different distribution vectors of 'f' are tabulated in Table6. Table 6 Number of polynomials satisfies different S_j for irreducible polynomials m(x).

Table6

m(x)	**S_8**	**S_7**	**S_6**	**S_5**	**S_4**	**S_3**	**S_2**	**S_1**	**S_0**
11b	04	26	54	61	67	35	08	00	01
11d	01	20	53	86	60	27	07	01	01
12b	10	26	44	72	66	20	07	08	03
12d	03	21	56	79	57	26	11	02	01
139	03	24	60	68	55	32	11	02	01
13f	01	27	59	72	53	28	10	05	01
14d	10	25	47	79	43	33	12	05	02
15f	08	27	37	63	89	24	07	00	01
163	04	34	42	68	63	32	10	02	01
165	10	25	47	79	43	33	12	05	02
169	03	21	56	79	57	26	11	02	01
171	01	20	53	86	60	27	07	01	01
177	05	22	43	81	68	31	05	00	01
17b	09	21	60	60	58	31	12	04	01
187	00	18	62	71	72	27	05	00	01
18b	04	11	49	93	72	24	02	00	01
18d	04	34	42	68	63	32	10	02	01
19f	00	24	50	79	69	27	06	00	01
1a3	04	11	49	93	72	24	02	00	01
1a9	10	26	44	72	66	20	07	08	03
1b1	04	26	54	61	67	35	08	00	01
1bd	09	21	60	60	58	31	12	04	01
1c3	00	18	62	71	72	27	05	00	01
1cf	01	32	51	59	70	36	05	01	01
1d7	02	20	67	60	64	34	08	00	01
1dd	05	22	43	81	68	31	05	00	01
1ef	01	32	51	59	70	36	05	01	01
1f3	00	24	50	79	69	27	06	00	01
1f5	08	27	37	63	89	24	07	00	01
1f9	01	27	59	72	53	28	10	05	01

From the above Table6 it is observed that there are 8 irreducible polynomials which have more than 8 polynomials that satisfy the maximum Avalanche Criteria. The irreducible polynomials $12b_h$, $14d_h$, 165_h, and $1a9_h$ have 10 polynomials each, $17b_h$, and $1bd_h$ have 9 polynomials each and $15f_h$ and $1f5_h$ have 8 polynomials each, from which maximum Avalanche Criteria can be achieved. It is found that the matrices constructed from the respective polynomials of irreducible polynomials $15f_h$ and $1f5_h$ are singular matrices. It is also verified that all the generator matrices constructed from $12b_h$ and $1a9_h$ are singular one. Matrices constructed from irreducible polynomials $17b_h$ and $1bd_h$, that is totally 2 x $9C_8$ = 18 are also singular, and only 2 x 5 = 10 are non-singular. Similarly the matrices constructed from remaining two irreducible polynomials $14d_h$ and 165_h, there are only 2 x 20 = 40 non-singular, out of 2 x $10C_8$ = 90 . Hence in total it is possible to construct 10 + 40 = 50, S-boxes from affine transformation, those satisfy maximum

Avalanche Criteria. The polynomials which give $S_8 > 8$ for different irreducible polynomials m(x) are tabulated in Table 7.

Table 7 The polynomials give $S_8 > 8$

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
15F	22	24	2C	48	59	65	91	B2	-	-
1F5	3C	56	67	9E	AB	CF	D5	EA	-	-
17B	05	0A	15	6B	6D	82	B5	D7	DA	-
1BD	36	3F	6D	7E	9B	9F	B7	DB	FD	-
12B	49	58	63	8F	93	AC	B1	C2	C7	E1
14D	0D	1B	24	37	52	6F	86	92	A9	DF
165	08	0E	10	21	28	43	51	87	C0	E0
1A9	04	09	12	25	2D	4B	71	96	97	E2

5. Construction of S-boxes which give 100% Avalanche Criteria.

As it was discussed in section 4, polynomials with irreducible polynomials $17b_h$, $1bd_h$, $14d_h$ and165_h only give non-singular matrices. With the above irreducible polynomials, the possible combination of the polynomials which give non-singular matrices are discussed below.

With m(x) = $17b_h$, 5 matrices can be constructed excluding the polynomials 05_h, $0a_h$, $6d_h$, $d7_h$, da_h in each case. Similarly with m(x) = $1bd_h$, 5 matrices can be constructed excluding the polynomials $3f_h$, $6d_h$, $7e_h$, $9b_h$, $b7_h$ in each case. In the case, m(x) = $14d_h$, 20 matrices can be constructed excluding the following pairs of polynomials for each case, (92_h,49_h), (49_h,df_h), (86_h,49_h), (86_h,df_h), ($6f_h$,49_h), ($6f_h$,df_h), (52_h,$6f_h$), (52_h,86_h), (52_h,92_h), (52_h,49_h),(52_h,df_h),(24_h,$6f_h$), (24_h,86_h), (24_h,92_h), (24_h,49_h), (24_h,df_h), ($0d_h$,24_h), ($0d_h$,52_h), ($0d_h$,49_h), ($0d_h$,df_h). Similarly in the case of m(x) = 165_h, 20 more matrices can be constructed

excluding the following pairs of polynomials for each case, ($c0_h$,$e0_h$), (87_h,$c0_h$), (87_h,$e0_h$), (51_h,$c0_h$), (51_h,$e0_h$), (28_h,51_h), (28_h,87_h), (28_h,$c0_h$), (10_h,28_h), (10_h,$c0_h$), (10_h,$e0_h$), ($0e_h$,28_h), ($0e_h$,$c0_h$), ($0e_h$,$e0_h$), (08_h,$0e_h$), (08_h,10_h), (08_h,28_h), (08_h,51_h), (08_h,87_h), (08_h,$e0_h$) (Refer Table7).

Construct an A matrix selecting anyone set of 8 polynomials among the above 4 irreducible polynomials m(x). Using equation (1), construct the S- box, C may be any constant from 00_h to ff_h, which will not change the Avalanche Criteria property. Calculate the Avalanche Criteria for each S- box as explained in Section 3.

Consider an example with irreducible polynomial $14d_h$ with 8 polynomials [$0d_h$, $1b_h$, 24_h, 37_h, 52_h, $6f_h$, 86_h, 92_h, $a9_h$,df_h]^T to construct the A matrix, from which S- box is generated using C = 97_h and the respective Avalanche Criteria values are calculated and tabulated as in Table8 and Table9 respectively. From the Avalanche Criteria Table 9 it is observed that all the 64 entries are ≥ 128, that is 64/64 = 100%

Table 8 The AES S-box which gives 100% Avalanche Criteria.

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

Table 9 Avalanche Criteria for the AES S-box in Table 8

	S_8	S_7	S_6	S_5	S_4	S_3	S_2	S_1
00000001	136	144	132	132	140	128	140	132
00000010	144	132	128	128	144	132	136	136
00000100	132	128	136	132	128	136	144	132
00001000	128	132	132	136	136	132	132	136
00010000	132	136	144	132	136	136	128	132
00100000	136	132	136	136	128	132	132	128
01000000	132	136	128	132	136	128	136	128
10000000	136	132	136	128	136	128	132	136.

6. Results.

All the possible fifty S-boxes and their respective Avalanche Criteria's are generated and tested. By changing the row positions of the individual polynomials in A matrix, 8! of S-boxes were constructed and tested for Avalanche Criteria. It is found that in all the cases the Avalanche Criteria is maximum. One of the S- box and the corresponding Avalanche Criteria are tabulated in Table8 and Table9 .The Avalanche criteria for the following affine transformation with different A matrix, C and irreducible polynomials m are shown in Table10 toTable13.

Table 10 Avalanche Criteria for A = $[1b_h, 24_h, 37_h, 52_h, 6f_h, 86_h, 92_h, df_h]^T$, c = $[b5_h]^T$ and m = $14d_h$

	S8	**S7**	**S6**	**S5**	**S4**	**S3**	**S2**	**S1**
00000001	144	132	132	140	128	140	128	132
00000010	132	128	128	144	132	136	132	136
00000100	128	136	132	128	136	144	128	132
00001000	132	132	136	136	132	132	136	136
00010000	136	144	132	136	136	128	132	132
00100000	132	136	136	128	132	132	144	128
01000000	136	128	132	136	128	136	136	128
10000000	132	136	128	136	128	132	128	136

Table 11 Avalanche Criteria for A = $[0e_h, 10_h, 21_h, 28_h, 43_h, 51_h, 87_h, c0_h]^T$, c = $[e8_h]^T$ and m = 165_h

	S8	**S7**	**S6**	**S5**	**S4**	**S3**	**S2**	**S1**
00000001	132	128	128	136	132	128	136	136
00000010	136	128	132	128	136	136	132	128
00000100	132	132	136	136	132	144	136	136
00001000	128	136	132	144	136	132	132	136
00010000	132	132	136	132	132	136	128	128
00100000	144	136	132	136	128	128	132	144
01000000	136	132	128	128	132	132	144	140
10000000	140	128	132	132	144	128	136	132

Table 12 Avalanche Criteria for A = [$0a_h$, 15_h, $6b_h$, $6d_h$, 82_h, $b5_h$, $d7_h$, da_h]^T , c = [$7e_h$]^T and m = $17b_h$

	S8	**S7**	**S6**	**S5**	**S4**	**S3**	**S2**	**S1**
00000001	136	136	128	140	128	128	128	132
00000010	136	144	128	132	136	128	132	128
00000100	144	144	132	128	136	128	132	128
00001000	144	132	132	128	136	132	132	128
00010000	132	132	132	128	144	132	128	132
00100000	132	128	128	132	144	132	136	132
01000000	128	144	136	132	132	128	132	132
10000000	144	132	132	132	132	136	136	128

Table 13 Avalanche Criteria for A = [36_h, $6d_h$, $7e_h$, $9b_h$, $9f_h$, $b7_h$, db_h, fd_h]^T , c = [$5d_h$]^T and m = $1bd_h$

	S8	**S7**	**S6**	**S5**	**S4**	**S3**	**S2**	**S1**
00000001	132	136	128	136	132	132	128	132
00000010	136	128	132	132	144	132	132	132
00000100	128	132	132	136	128	132	132	144
00001000	132	132	144	128	132	128	132	144
00010000	132	132	144	132	132	128	128	136
00100000	132	128	136	132	144	128	128	136
01000000	128	128	136	132	144	132	128	136
10000000	128	128	136	128	136	140	132	128

7. Conclusion

It is possible to construct the S-box which satisfy maximum Avalanche Criteria, There are only Four irreducible polynomials which give these S-boxes. In total it is possible to construct only 50 S-boxes that satisfies maximum Avalanche Criteria with affine transformation. It may be concluded that with any other combinations with any other irreducible polynomials, it is not possible to construct the S-boxes which satisfy the maximum Avalanche Criteria.

References:

[1] William Stallings, "Cryptography and Network Security Principles and Practices", Fourth
[2] Edition, Pearson, Prentice Hall, 2006.
[3] Daemen, J. and V. Rijmen, "The Design of RIJNDAEL- AES The Advanced Encryption
[4] Standard", Springer-Verlag, Berlin, 2002.
[5] Chandrasekharappa T G S, Prema K V, Kumara Shama, "Possible S-boxes generated from Affine transformation those satisfy Maximum Strict Avalanche Criteria, Proceedings of World Academy of Science, Engineering and Technology 60, pp.880-883 Dec. 2009.
[6] Elif Saygi, Zulfukar Saygi, Meltem SOnmezturan, Ali doganaksoy, Statistical approach on the number of SAC satisfying functions, IEEE transactions on computers, vol. 44. No. 9, September 1995.
[7] Rejane Forre, The strict avalanche criterion: spectral properties of Boolean Functions and an Extended De_nitio, Advances in cryptology-crypto 88, Lecture notes in computer science, volume 403, pp. 450-468 Springer-verlag.
[8] Isil VERGILI, Melek D. YUCEL, Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen n _ n S-boxes, Turk J Elec. Engin, VOL.9, NO.2 2001.