4-bit crypto S-boxes: Generation with irreducible polynomials over Galois field GF(2^4) and cryptanalysis.

Sankhanil Dey[1] and Ranjan Ghosh[2],
sdrpe_rs@caluniv.ac.in[1], rghosh47@yahoo.co.in,
Institute of Radio Physics and Electronics, University of Calcutta[1,2],
92 A P C Road, Kolkata-700009[1,2].

Abstract. 4-bit crypto S-boxes play a significant role in encryption and decryption of many cipher algorithms from last 4 decades. Generation and cryptanalysis of generated 4-bit crypto S-boxes is one of the major concerns of modern cryptography till now. In this paper 48, 4-bit crypto S-boxes are generated with addition of all possible additive constants to the each element of crypto S-box of corresponding multiplicative inverses of all elemental polynomials (EPs) under the concerned irreducible polynomials (IPs) over Galois field GF(2^4). Cryptanalysis of 48 generated 4-bit crypto S-boxes is done with all relevant cryptanalysis algorithms of 4-bit crypto S-boxes. The result shows the better security of generated 4-bit crypto S-boxes.

Keywords. Irreducible polynomials, Galois field, Finite field, Substitution boxes, 4-bit S-boxes.
Mathematics Subject Classification: 94A60, 11T71, 14G50, 68P25, 81P94.
Computing Classification System: 9.1.4.

1. Introduction.

In computer cryptography polynomials especially irreducible polynomials play a significant role from last two decades. Generation of 4-bit crypto S-boxes with polynomials over binary Galois field GF(2^4) is the matter of interest in this paper. In binary Galois field GF(2^4) polynomials with highest degree of variable, '4', are said as basic polynomials or BPs over Galois field GF(2^4). Polynomials over Galois field GF(2^4) with highest degree of variable less than four are termed as elemental polynomials or EPs over Galois field GF(2^4). Polynomials over Galois field GF(2^4) with highest degree 0 are said as constant polynomials or CPs over Galois field GF(2^4). BPs that contain two non-constant EPs as factors are said as reducible polynomials or RPs over Galois field GF(2^4). Rest of BPs are irreducible polynomials or IPs over Galois field GF(2^4) that must have CPs over Galois field GF(2^4) and itself as factors. In binary Galois field GF(2^4) there are (2^4 =)16 BPs over Galois field GF(2^4), (2^4 =)16 EPs over Galois field GF(2^4) in which (2^1 =)2 are CPs over Galois field GF(2^4) and 14 are non-constant EPs over Galois field GF(2^4). Among 16 BPs over Galois field GF(2^4) there are 13 RPs over Galois field GF(2^4) and 3 IPs over Galois field GF(2^4) [1][2][3][4].

4-bit crypto substitution boxes or crypto S-boxes are in study of cryptographers from the beginning of computer cryptography since late sixties. A 4-bit crypto S-box is an array of sixteen unique and distinct elements with value of them vary from 0 to f in hex. It must be noted that the values of each element must be unique and distinct. The highest value of an element in an 4-bit crypto S-box is f and lowest is 0 and they are arranged in sequential, partly sequential or non-sequential arrangement [5][6][7]. In 2 variants of Lucifer there are 4, 4-bit crypto S-boxes used where as in DES the number is 32 [8][9][10]. Each row in 8 DES crypto S-boxes is a 4 bit crypto S-box and in DES there are 32 rows in 8 crypto S-boxes so there are 32 4-bit crypto S-boxes available in DES algorithm.

In binary Galois field GF(2^4) there are 16 distinct EPs for which the decimal equivalent or DE of EPs vary from 0 to 15 in decimal. For each EP there is a multiplicative inverse or MI of that EP under a certain IP [1]. End of the day there 3 sets of 16 distinct MIs available over Galois field GF(2^4) under 3 IPs over Galois field GF(2^4). There are 16 additive constants from 0 to 15 are included over Galois field GF(2^4). Each additive constant is added to each of 16 MIs of set to construct a new 4-bit crypto S-box.

In this paper 48, 4-bit S-boxes are generated under IPs over Galois field GF(2^4). They are cryptanalyzed and a comparative study with 32 DES and 6 Lucifer 4-bit crypto S-boxes has been illustrated in the paper.

Generation of 48, 4-bit crypto S-boxes is noted in sec.2. Cryptanalysis of 4 Lucifer, 32 DES and 48 generated 4-bit S-boxes with discussion on results is given in sec.3. Conclusion and Acknowledgment are given in sec.4. and sec.5 respectively.

2. Generation of 48, 4-bit crypto S-boxes under 3 IPs over Galois field GF(2^4).

There are 16 BPs available over Galois field GF(2^4) among which 13 are RPs and 3 are IPs. There are also 16 EPs are available over Galois field GF(2^4) among which 2 are CPs and 14 are non-constant polynomials. DE of All EPs in a sequential order constitutes an identity crypto S-box. MIs under 3 IPs over Galois field GF(2^4) constitutes another 3 crypto S-boxes. 16 additive constants in each case one of which are added to each elements of an MI S-box constitutes another crypto S-box. So there are (16 × 3 =) 48 possible crypto S-boxes can be generated under 3 IPs over Galois field GF(2^4). BPs over Galois field GF(2^4) are described and listed in subsec. 2.1. EPs over Galois field GF(2^4) are described and listed in subsec. 2.2. RPs and IPs over Galois field GF(2^4) are described and listed in subsec. 2.3. MIs of EPs under IP (x4+x+1) with (DE = 19) are described and listed in subsec. 2.4. At last 16 additive S-boxes are generated from S-box of MI with addition of 16 additive S-boxes one at a time are described and listed in subsec.2.5.

2.1 Basic polynomials (BPs) over Galois field GF(2^4). Polynomials over Galois field GF(2^4) with degree of highest degree term 4 is termed as basic polynomials or BPs over Galois field GF(2^4). Total number of terms in BPs are (4+1 = highest degree +1= extension of Galois field +1 =) 5. For Galois field GF(2^4) the table of BPs with their decimal equivalents (DEs), polynomial presentation and binary coded number (BCN) [Number obtained from coefficients considering highest degree term as MSB and lowest degree term as LSB and also coefficients of terms absent are 0] presentation are given in table.1. The range of DEs of BPs over Galois field GF(2^4) is (2^4≤DE≤2^5-1) 16≤DE≤31, and total number of BPs are (2^4=) 16.

Table.1. List of BPs over Galois field GF(2^4)

Row	DEs	Polynomials	BCNs
1	16	x^4	10000
2	17	x^4+1	10001
3	18	x^4+x	10010
4	19	x^4+x+1	10011
5	20	x^4+x^2	10100
6	21	x^4+x^2+1	10101
7	22	x^4+x^2+x	10110
8	23	x^4+x^2+x+1	10111
9	24	x^4+x^3	11000
A	25	x^4+x^3+1	11001
B	26	x^4+x^3+x	11010
C	27	x^4+x^3+x+1	11011
D	28	$x^4+x^3+x^2$	11100
E	29	$x^4+x^3+x^2+1$	11101
F	30	$x^4+x^3+x^2+x$	11110
G	31	$x^4+x^3+x^2+x+1$	11111

2.2 Elemental polynomials (EPs) over Galois field GF(2^4). Polynomials over Galois field GF(2^4) with degree of highest degree term less than 4 is termed as elemental polynomials or EPs over Galois field GF(2^4). Maximum number of terms in EPs are (4 = highest degree= extension of Galois field) 4 and minimum 1. For Galois field GF(2^4) the table of EPs with their decimal equivalents (DEs), polynomial presentation and binary coded number (BCN) [Number obtained from coefficients considering highest degree term as MSB and lowest degree term as LSB and also coefficients of terms absent are 0] presentation are given in table.1. The range of DEs of EPs over Galois field GF(2^4) is (0≤DE≤2^4) 0≤DE≤15, and total number of BPs are (2^4=) 16. The polynomials 0 [00000] and

1[00001] are termed as constant polynomials or CPs over Galois field GF(2^4) since they carries only constant terms in it. They are not in our interest in this study.

Table.2. List of EPs over Galois field GF(2^4)

Row	DEs	Polynomials	BCNs
1	0	0	00000
2	1	1	00001
3	2	X	00010
4	3	x+1	00011
5	4	x^2	00100
6	5	x^2+1	00101
7	6	x^2+x	00110
8	7	x^2+x+1	00111
9	8	x^3	01000
A	9	x^3+1	01001
B	10	x^3+x	01010
C	11	x^3+x+1	01011
D	12	x^3+x^2	01100
E	13	x^3+x^2+1	01101
F	14	x^3+x^2+x	01110
G	15	x^3+x^2+x+1	01111

2.3 Reducible polynomials (RPs) and Irreducible Polynomials (IPs) over Galois field GF(2^4). Reducible polynomials have two non-constant EPs as its factor. Polynomial multiplication of two EPs must be an RP. Rests of polynomials that have it self and constant polynomials as factor are termed as irreducible polynomials or IPs. In table.3. below all reducible polynomials are listed in column RPs and DEs of RPs are listed in column DEs (RPs) with their BCNs in column BCNs (RPs). The corresponding two non-constant EP factors are given in column Factors. BPs that are not present in the table follows are IPs and here DE of IPs are 19, 25, 31 i.e. they are 3 in number.

Row	Factors	RPs	DEs (RPs)	BCNs (RPs)
1	$x.\ x^3$	x^4	16	10000
2	$x.\ (x^3+1)$	x^4+x	18	10010
3	$x.\ (x^3+x)$	x^4+x^2	20	10100
4	$x.\ (x^3+x+1)$	x^4+x^2+x	22	10110
5	$x.\ (x^3+x^2)$	x^4+x^3	24	11000
6	$x.\ (x^3+x^2+1)$	x^4+x^3+x	26	11010
7	$x.\ (x^3+x^2+x)$	$x^4+x^3+x^2$	28	11100
8	$x.\ (x^3+x^2+x+1)$	$x^4+x^3+x^2+x$	30	11110
9	$(x+1).\ x^3$	x^4+x^3	24	11000
10	$(x+1).\ (x^3+1)$	x^4+x^3+x+1	27	11101
11	$(x+1).\ (x^3+x)$	$x^4+x^3+x^2+x$	30	11110
12	$(x+1).\ (x^3+x+1)$	$x^4+x^3+x^2+1$	29	11101
13	$(x+1).\ (x^3+x^2)$	x^4+x^2	20	10100
14	$(x+1).\ (x^3+x^2+1)$	x^4+x^2+x+1	23	10111
15	$(x+1).\ (x^3+x^2+x)$	x^4+x	18	10010
16	$(x+1).\ (x^3+x^2+x+1)$	x^4+1	17	10001
17	$x^{2\cdot}x^2$	x^4	16	10000
18	$x^2\ .\ (x^2+1)$	x^4+x^2	20	10100
19	$x^2\ .\ (x^2+x)$	x^4+x^3	24	11000
20	$x^2\ .\ (x^2+x+1)$	$x^4+x^3+x^2$	28	11100
21	$(x^2+1)\ .\ (x^2+1)$	x^4+1	17	10001
22	$(x^2+1)\ .\ (x^2+x)$	$x^4+x^3+x^2+x$	30	11110

23	$(x^2+1) . (x^2+x+1)$	x^4+x^3+x+1	27	11011
24	$(x^2+x) . (x^2+x)$	x^4+x^2	20	10100
25	$(x^2+x) . (x^2+x+1)$	x^4+x	18	10010
26	$(x^2+x+1) . (x^2+x+1)$	x^4+x^2+1	21	10101

Table.3. List of RPs over Galois field GF(2^4).

List of IPs over Galois field GF(2^4) is given in table 4. Below,

Row	Irreducible Polynomials (IPs)	DE of IPs	BCN(IPs)
1	x^4+x+1	19	10011
2	x^4+x^3+1	25	11001
3	$x^4+x^3+x^2+x+1$	31	11111

Table.4. List of IPs over Galois field GF(2^4).

2.4 Multiplicative inverses (MIs) of all EPs under IP (x^4+x+1) or DE of IP 19 Galois field GF(2^4). MI of a particular non-constant EP is determined by multiplication of non-constant EP with rest of the EPs and division of product by IP. If for a certain division the residue is 1 then the two EPs are said as MIs of each other under IP (x^4+x+1) over Galois field GF(2^4). The equation can be described in mathematics as follows,

Mathematical procedure. (EP×MI)% (x^4+x+1) =1.

List of MIs of 16 EPs under IP (x^4+x+1) is given in table.5.

DE(EPs)	EPs	DE(MIs)	MIs
0	0	**0**	0
1	1	**1**	1
2	X	**9**	x^3+1
3	$x+1$	**E**	x^3+x^2+x
4	x^2	**D**	x^3+x^2+1
5	x^2+1	**B**	x^3+x+1
6	x^2+x	**7**	x^2+x+1
7	x^2+x+1	**6**	x^2+x
8	x^3	**F**	x^3+x^2+x+1
9	x^3+1	**2**	X
A	x^3+x	**C**	x^3+x^2
B	x^3+x+1	**5**	x^2+1
C	x^3+x^2	**A**	x^3+x
D	x^3+x^2+1	**4**	x^2
E	x^3+x^2+x	**3**	$x+1$
F	x^3+x^2+x+1	**8**	x^3

Table.5. List of MIs of 16 EPs under IP (x^4+x+1).

2.5 Additive S-boxes from S-box of MIs under IP (x^4+x+1). There are 16 additive elements over Galois field GF(2^4). They are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. It is intend to add each additive element to 16 MIs of 16 EPs to obtain 16 different crypto S-boxes. Although 16 set of MIs are also form a crypto S-box. The MI S-box and 16 additive MI S-boxes are shown in table.6. below,

Row	Addtv el.	**Original S-box**-019edb76f2c5a438
1	0	**S-box**-019edb76f2c5a438
2	1	**S-box**-12afec8703d6b549
3	2	**S-box**-23b0fd9814e7c65a
4	3	**S-box**-34c10ea925f8d76b
5	4	**S-box**-45d21fba3609e87c
6	5	**S-box**-56e320cb471af98d
7	6	**S-box**-67f431dc582b0a9e
8	7	**S-box**-780542ed693c1baf

9	8	**S-box**-891653fe7a4d2cb0
10	9	**S-box**-9a27640f8b5e3dc1
11	A	**S-box**-ab3875109c6f4ed2
12	B	**S-box**-bc498621ad705fe3
13	C	**S-box**-cd5a9732be8160f4
14	D	**S-box**-de6ba843cf927105
15	E	**S-box**-ef7cb954d0a38216
16	F	**S-box**-f08dca65e1b49327

Table.6. Additive S-boxes under IP (x^4+x+1) over Galois field GF(2^4).

3. Cryptanalysis of 32 DES, 4 Lucifer (2 variants) and 48 generated 4-bit crypto S-boxes and there comparative study and also the best possible 4-bit crypto S-boxes.

In beginning of this section discussion procedure of cryptanalysis algorithms are discussed in brief in subsec.3.1. Later in this section the results of cryptanalysis of 32 DES 4-bit S-boxes and 4 S-boxes of 2 variants of Lucifer are discussed in brief in subsec.3.2 and 3.3 respectively. In subsec.3.4 results of cryptanalysis of 16 additive S-boxes under each IP over Galois field GF(2^4) are discussed in brief. A comparative analysis of the above results is discussed in subsec.3.5.

3.1 Cryptanalysis procedure. 'No.elr' shows number of existing linear relations out of 64 possible linear relations in a 4-bit crypto S-box. 'No.8' shows number of 8s in linear approximation table or LAT. 'N0.dif' shows number of 0s in difference distribution table or DDT and 'N8.dat' shows number of 8s in differential approximation table or DAT [15][16]. The procedures are discussed as follows,

In difference distribution table there are 256 cells, i.e. 16 rows and 16 columns. Each row is for each input difference varies from 0 to f in hex. Each column in each row represents each output difference varies from 0 to f in hex for each input difference. 0 in any cell indicates absence of that output difference for subsequent input difference. Such as 0 in a cell of DDT means for input difference 0 the corresponding output difference is absent. If numbers of 0s are too low or too high it supplies more information regarding concerned output difference. So an S-box is said to be immune to this cryptanalytic attack if number of 0s in DDT is close to 128 or half of total cells or 256. In the said example of 1st DES 4-bit S-box total numbers of 0s in DDT are 168. That is close to 128. So the S-box is said to be almost secure from this attack. [6][7]

As total number of balanced 4-bit BFs increases in Difference Analysis Table or DAT the security of S-box increases since balanced 4-bit BFs supplies at most uncertainty. Since Number of 0s and 1s in balanced 4-bit BFs are equal i.e. they are same in number means determination of each bit has been at most uncertainty. In the said example of 1st DES 4-bit S-box total numbers of 8s in DAT are 36. That is close to 32 half of total 64 cells. So the S-box has been said to be almost less secure from this attack.[6][7]

In linear approximation table or LAT there are 256 cells for 256 possible 4-bit linear relations. The count of 16 4-bit binary conditions to satisfy for any given linear relation is put into the concerned cell. 8 in a cell indicate that the particular linear relation is satisfied for 8, 4-bit binary conditions and remain unsatisfied for 8, 4-bit binary conditions. That is at most uncertainty. In the said example of 1st DES 4-bit S-box total numbers of 8s in LAT is 143. That is close to 128. So the S-box is said to be less secure from this attack.

The value of $^{n}C_{r}$ is maximum when the value of r is ½ of the value of n (when n is even). Here the maximum number of linear approximations is 64. So if the total satisfaction of linear equation is 32 out of 64 then the number of possible sets of 32 linear equations is the largest. That means if the total satisfaction is 32 out of 64 then the number of possible sets of 32 possible linear equations is $^{64}C_{32.}$ That is maximum number of possible sets of linear equations. If the value of total number of linear relations is closed to 32 then it is more cryptanalysis immune. Since the number of possible sets of linear equations are too large to calculate. As the value goes close to 0 or 64 it reduces the sets of possible linear equations to search, that reduces the effort to search for the linear equations present in a particular 4-bit crypto S-box. In this example total satisfaction is 21 out of 64. Which means the given 4-bit S-Box is not a good 4 bit crypto S-box or not a good crypt analytically immune 4-bit crypto S-box.

If the value of total number of existing linear relations for a 4-bit crypto S-box is 24 to 32, then the lowest numbers of sets of linear equations are 250649105469666120. This is a very large number to investigate. So the 4-

bit crypto S-box is declared as a good 4-bit crypto S-box or 4-bit crypto S-box with good security. If it is between 16 through 23 then the lowest numbers of sets of linear equations are 488526937079580. This not a small number to investigate in today's computing scenario so the S-boxes are declared as medium 4-bit crypto S-box or 4-bit crypto S-box with medium security. The 4-bit crypto S-boxes having existing linear equations less than 16 are declared as poor 4-bit crypto S-Box or vulnerable to cryptanalytic attack [6][7].

'No.sac', 'N2sac', 'N3sac' and 'Nalsac' gives total number times four 4-bit BFs of the concerned S-box satisfies 4 simple first order SAC, 6, 2nd order HO-SAC, 4, 3rd order HO-SAC and 16, 1st, 2nd, 3rd, and 4th order HO-SAC respectively.

3.2 Discussion on cryptanalysis of 32 4-bit crypto S-boxes of Data Encryption Standard or DES. Data Encryption Standard or DES algorithm contains 8 S-boxes with four rows in each S-box. Each row in DES S-box is a 4-bit crypto S-box of DES algorithm. The results of cryptanalysis of 32 DES 4-bit crypto S-box is given in table.7. and results are discussed in discussion below,

DES S-boxes	No.elr	No.8	N0.ddt	N8.dat	No.sac	N2sac	N3sac	Nalsac
e4d12fb83a6c5907	21	143	168	36	7	15	11	36
0f74e2d1a6cb9538	29	143	168	36	7	17	9	36
41e8d62bfc973a50	23	138	168	36	8	15	11	36
fc8249175b3ea06d	25	154	166	42	10	20	12	42
f18e6b34972dc05a	24	132	162	30	6	12	9	30
3d47f28ec01a69b5	21	143	166	30	8	12	7	30
0e7ba4d158c6932f	31	143	166	21	4	10	6	21
d8a13f42b67c05e9	20	126	168	36	8	12	12	36
a09e63f51dc7b428	17	133	162	30	7	12	8	30
d709346a285ecbf1	22	133	168	30	7	13	8	30
d6498f30b12c5ae7	23	151	166	21	6	9	4	21
1ad069874fe3b52c	28	158	174	30	6	11	10	30
7de3069a1285bc4f	22	136	168	36	8	16	10	36
d8b56f03472c1ae9	22	136	168	36	8	16	10	36
a690cb7df13e5284	20	136	168	36	8	16	10	36
3f06a1d8945bc72e	22	136	168	36	8	16	10	36
2c417ab6853fd0e9	25	137	162	30	6	14	8	30
eb2c47d150fa3986	20	143	166	36	8	16	9	36
421bad78f9c5630e	30	130	160	27	6	11	7	27
b8c71e2d6f09a453	21	134	166	18	3	7	6	18
c1af92680d34e75b	30	141	159	36	8	16	10	36
af427c9561de0b38	29	127	164	36	7	15	11	36
9ef528c3704a1db6	24	127	168	18	5	7	5	18
432c95fabe17608d	24	130	162	30	6	12	9	30
4b2ef08d3c975a61	26	134	168	30	7	13	8	30
d0b7491ae35c2f86	27	145	166	30	7	14	7	30
14bdc37eaf680592	28	137	168	36	8	16	10	36
6bd814a7950fe23c	25	135	173	0	0	0	0	0
d2846fb1a93e50c7	23	144	161	30	8	14	7	30
1fd8a374c56b0e92	20	147	174	27	9	12	4	27
7b419ce206adf358	27	132	166	18	5	7	5	18
21e74a8dfc90356b	28	138	168	39	8	16	12	39

Table.7. Cryptographic analysis of 32 DES 4-bit crypto S-boxes.

Discussion. In table.7. out of 32 DES S-boxes 1 have 17, 3 have 21, 4 have 22, 1 have 23, 3 have 24, 3 have 25, 1 have 26, 2 have 27, 3 have 28, 2 have 29, 2 have 30 and 1 have 31 existing linear relations i.e. 24 S-boxes out of 32 are less secure from this attack and 8 out of 32 are immune to this attack. Again out of 32 DES S-boxes 1 have 126, 2 have 127, 2 have 130, 1 have 132, 2 have 133, 2 have 134, 1 have 135, 4 have 136, 2 have 137, 2 have 138, 1 have 141, 5 have 143, 1 have 144, 1 have 145, 1 have 147, 1 have 151, 1 have 154 and 1 have 158 8s in LAT. That is All S-boxes are less immune to this attack. Again out of 32 DES S-boxes 1 have 159, 1 have 160, 1 have 161, 4 have 162, 1 have 164, 8 have 166, 13 have 168, 1 have 173 and 2 have 174 0s in DDT. That is all S-boxes are secured from this attack. At last out of 32 DES S-boxes 1 have 0, 3 have 18, 2 have 21, 2 have 27, 10 have 30, 12 have 36, 1 have 39 and 1 have 42 8s in DAT i.e. they have been less secure to this attack. The comparative analysis has proved that linear approximation analysis is the most time efficient cryptanalytic algorithm for 4-bit S-boxes. In 'nosac' the lowest value is 0 and maximum value is 10 where in 'n2sac', 'n3sac' and 'nalsac' lowest values are 0, 0, 0 and maximum values are 16, 12 and 39 respectively. But numbers of optimum as well as better result i.e. 16 for 'nosac' is absent, close to 24 for 'n2sac', close to 16 for 'n3sac' and close to 64 for 'nalsac' has been very less in numbers. So the 32 DES 4-bit S-boxes are observed to be less secure.

3.2 Discussion on cryptanalysis of 4, 4-bit crypto S-boxes of 2 variants of Lucifer. 2 variants of Lucifer one by feistel [7], and one by Sorkin [8] contain total 4 crypto S-boxes. The cryptanalysis of the concerned 4, crypto S-boxes is shown in table.8. and the result is also discussed below.

Lucifer S-boxes	No.elr	No.8	N0.ddt	N8.dat	No.sac	N2sac	N3sac	Nalsac
F-3085124fd9ce6ba7	25	132	163	36	8	16	9	36
F-8d16c4fb325e907a	31	115	154	36	10	12	11	36
S-cf7aedb026319458	25	132	163	36	8	16	9	36
S-72e93b04cd1a5f85	28	58	151	18	6	5	7	18

Table.8. Cryptographic analysis of 4, 4 bit crypto S-boxes of 2 variants of Lucifer.

Discussion. In table.8. out of 4, 4-bit Crypto S-boxes 2 have 25, 1 have 28 and 1 have 31 existing linear relations i.e all 4 crypto 4-bit S-boxes are almost secure from this attack. Again out of 4, 4-bit crypto S-boxes, 2 have 132, 1 have 115 and 1 have 58 8s in LAT i.e. 3 4-bit crypto S-boxes out of four are secure from this attack and one is a poor 4-bit crypto S-box from the angle of this attack. Again out of 4, 4-bit crypto S-boxes 2 have 163, one have 154 and one have 151 0s in DDT so all of four S-boxes are seen to secure from the attack. From the angle of this attack 3 have 36 and one have 18 8s in DAT so all of four 4-bit crypto S-boxes are less secure to this attack.

Now first S-box in table.8. has 8 out of total 16 SFO SAC satisfaction, 16 out of total 24 2nd order MHO SAC satisfaction, 9 out of total 16 3rd order MHO SAC satisfaction, 36 out of total 64 all MHO SAC satisfaction so from this angle it is a poor 4-bit crypto S-box from this angle.

Now second S-box in table.8. has 10 out of total 16 SFO SAC satisfaction, 12 out of total 24 2nd order MHO SAC satisfaction, 11 out of total 16 3rd order MHO SAC satisfaction, 36 out of total 64 all MHO SAC satisfaction so from this angle it is a almost good 4-bit crypto S-box from this angle.

Now third S-box in table.8. has 8 out of total 8 SFO SAC satisfaction, 16 out of total 24 2nd order MHO SAC satisfaction, 9 out of total 16 3rd order MHO SAC satisfaction, 36 out of total 64 all MHO SAC satisfaction so from this angle it is a poor 4-bit crypto S-box from this angle.

Now first S-box in table.8. has 8 out of total 6 SFO SAC satisfaction, 5 out of total 24 2nd order MHO SAC satisfaction, 7 out of total 16 3rd order MHO SAC satisfaction, 36 out of total 64 all MHO SAC satisfaction so from this angle it is a very poor 4-bit crypto S-box from this angle.

3.3. Discussion on cryptanalysis of 48, 4-bit crypto S-boxes generated under 3 IPs over Galois field GF(2^4). A discussion on results of 16 generated 4-bit crypto S-boxes under IP x^4+x+1 with DE 19 is shown in subsec. 3.3.1. Again a discussion on results of 16 generated 4-bit crypto S-boxes under IP x^4+x^3+1 with DE 25 is shown in subsec. 3.3.2 and a discussion on results of 16 generated 4-bit crypto S-boxes under IP $x^4+x^3+x^2+x+1$ with DE 31 is shown in subsec. 3.3.3.

3.3.1 Discussion on results of 16 generated 4-bit crypto S-boxes under IP x^4+x+1 with DE 19 over Galois field GF(2^4). In this subsection a detailed discussion on cryptanalysis of 16, 4-bit crypto S-boxes generated after addition of 16 additive elements 0 to f in hex to each element of MI S-box, under IP x^4+x+1 with DE 19 over Galois field GF(2^4) one at a time for one additive S-box. The result of application of cryptanalysis algorithms of 4-bit crypto S-boxes on 16 generated 4-bit crypto S-boxes are shown in table.9. below and results are discussed in the following discussion section in brief.

Ad.el.	S-boxes un IP 19	No.elr	No.8	N0.ddt	N8.dat	No.sac	N2sac	N3sac	Nalsac
0	019edb76f2c5a438	23	117	150	36	08	14	11	36
1	12afec8703d6b549	31	121	155	36	7	14	11	36
2	23b0fd9814e7c65a	22	135	157	36	9	16	9	36
3	34c10ea925f8d76b	39	128	157	27	5	11	9	27
4	45d21fba3609e87c	27	115	150	36	10	12	12	36
5	56e320cb471af98d	37	125	155	36	8	14	11	36
6	67f431dc582b0a9e	29	132	157	36	10	15	8	36
7	780542ed693c1baf	34	125	157	27	5	10	9	27
8	891653fe7a4d2cb0	23	117	150	36	8	14	11	36
9	9a27640f8b5e3dc1	31	121	155	36	7	14	11	36
A	ab3875109c6f4ed2	22	135	157	36	9	16	9	36
B	bc498621ad705fe3	39	128	157	27	5	11	9	27
C	cd5a9732be8160f4	27	115	150	36	10	12	12	36
D	de6ba843cf927105	37	125	155	36	8	14	11	36
E	ef7cb954d0a38216	29	132	157	36	10	15	8	36
F	f08dca65e1b49327	34	125	157	27	5	10	9	27

Table.8. Cryptographic analysis of 16, 4 bit crypto S-boxes under IP (x^4+x+1) with DE 19 over Galois field GF(2^4).

Discussion. Out of total 16 4-bit crypto S-boxes 2 have 22, 2 have 23, 2 have 27, 2 have 29, 2 have 31, 2 have 34, 2 have 37 and 2 have 39 existing linear relations i.e. all of 16 4-bit crypto S-boxes are secure from this cryptanalytic attack. Again out of total 16 4-bit crypto S-boxes 2 have 115, 2 have 117, 2 have 121, 4 have 125, 2 have 128, 2 have 132 and 2 have 135 8s in LAT i.e. they are secure from linear cryptanalysis of 4-bit S-boxes. Now out of total 16 4-bit crypto S-boxes 4 have 150, 4 have 155 and 8 have 157 0s in DDT i.e. from this attack they are quite secure too. Again out of total 16 4-bit crypto S-boxes 4 have 27 and 12 have 36 8s in DAT i.e. they are in secure region of this attack.

S-boxes with additive element 0 to F in hex has a range 5 to 10 out of total 16 SFO SAC satisfactions, 10 to 16 out of total 24 2nd order MHO SAC satisfaction, 8 to 12 out of total 16 3rd order MHO SAC satisfaction, 27 to 36 out of total 64 all MHO SAC satisfaction so they are poor 4-bit crypto S-boxes from only SFO SAC angle but good secure 4-bit crypto S-boxes from MHO SAC angle.

3.3.2 Discussion on results of 16 generated 4-bit crypto S-boxes under IP x^4+x^3+1 with DE 25 over Galois field GF(2^4). In this subsection a detailed discussion on cryptanalysis of 16, 4-bit crypto S-boxes generated after addition of 16 additive elements 0 to f in hex to each element of MI S-box, under IP x^4+x^3+1 with DE 25 over Galois field GF(2^4) one at a time for one additive S-box. The result of application of cryptanalysis algorithms of 4-bit crypto S-boxes on 16 generated 4-bit crypto S-boxes are shown in table.10. below and results are discussed in the following discussion section in brief.

Ad.el.	S-boxes un IP 25	No.elr	No.8	N0.ddt	N8.dat	No.sac	N2sac	N3sac	Nalsac
0	01c86f4e3dba2975	25	120	150	36	10	17	7	36
1	12d9705f4ecb3a86	33	150	159	36	10	16	8	36
2	23ea81605fdc4b97	25	132	157	36	10	15	9	36
3	34fb927160ed5ca8	27	128	152	36	9	15	10	36
4	450ca38271fe6db9	19	127	150	36	11	14	10	36
5	561db493820f7eca	25	141	159	36	10	16	8	36
6	672ec5a493108fdb	21	129	157	36	9	17	9	36
7	783fd6b5a42190ec	29	124	152	36	8	16	10	36
8	8940e7c6b532a1fd	25	120	150	36	10	17	7	36
9	9a51f8d7c643b20e	33	150	159	36	10	16	8	36
A	ab6209e8d754c31f	25	132	157	36	10	15	9	36
B	bc731af9e865d420	27	128	152	36	9	15	10	36
C	cd842b0af976e531	19	127	150	36	11	14	10	36

D	de953c1b0a87f642	25	141	159	36	10	16	8	36
E	efa64d2c1b980753	21	129	157	36	9	17	9	36
F	f0b75e3d2ca91864	29	124	152	36	8	16	10	36

Table.10. Cryptographic analysis of 16, 4 bit crypto S-boxes under IP (x^4+x^3+1) with DE 25 over Galois field GF(2^4).

Discussion. Out of total 16 4-bit crypto S-boxes 2 have 19, 2 have 21, 6 have 25, 2 have 27, 2 have 29 and 2 have 33 existing linear relations i.e. all of 16 4-bit crypto S-boxes are secure from this attack. Now out of total 16 4-bit crypto S-boxes 2 have 120, 2 have 124, 2 have 127, 2 have 128, 2 have 129, 2 have 132, 2 have 141 and two have 150 8s in LAT i.e. most of the S-boxes are secure but some of them are less secure from this attack. Again out of total 16 4-bit crypto S-boxes 4 have 150, 4 have 152, 4 have 157 and 4 have 159 0s in DDT i.e. they are secure from this attack. At last out of total 16 4-bit crypto S-boxes 16 have 36 8s in DDT i.e. they are secure from this attack too.

S-boxes with additive element 0 to F in hex has a range 8 to 11 out of total 16 SFO SAC satisfactions, 15 to 17 out of total 24 2nd order MHO SAC satisfaction, 8 to 10 out of total 16 3rd order MHO SAC satisfaction, 36 out of total 64 all MHO SAC satisfaction so they are good 4-bit crypto S-boxes from not only SFO SAC angle but also good secure 4-bit crypto S-boxes from MHO SAC angle.

3.3.3 Discussion on results of 16 generated 4-bit crypto S-boxes under IP x^4+x^3+x^2+x+1 with DE 31 over Galois field GF(2^4). In this subsection a detailed discussion on cryptanalysis of 16, 4-bit crypto S-boxes generated after addition of 16 additive elements 0 to f in hex to each element of MI S-box, under IP x^4+x^3+x^2+x+1 with DE 31 over Galois field GF(2^4) one at a time for one additive S-box. The result of application of cryptanalysis algorithms of 4-bit crypto S-boxes on 16 generated 4-bit crypto S-boxes are shown in table.11. below and results are discussed in the following discussion section in brief.

Ad.el.	S-boxes un IP 31	No.elr	No.8	N0.ddt	N8.dat	No.sac	N2sac	N3sac	Nalsac
0	01fa8659473edcb2	29	120	150	36	6	17	11	36
1	120b976a584fedc3	25	133	161	36	10	12	12	36
2	231ca87b6950fed4	30	131	157	36	9	13	13	36
3	342db98c7a610fe5	24	126	159	36	8	12	14	36
4	453eca9d8b7210f6	31	125	150	36	5	16	12	36
5	564fdbae9c832107	25	132	161	27	7	9	10	27
6	6750ecbfad943218	30	133	157	27	5	12	9	27
7	7861fdc0bea54329	26	128	159	36	6	14	13	36
8	89720ed1cfb6543a	29	120	150	36	6	17	11	36
9	9a831fe2d0c7654b	25	133	161	36	10	12	12	36
A	ab9420f3e1d8765c	30	131	157	36	9	13	13	36
B	bca53104f2e9876d	24	126	159	36	8	12	14	36
C	cdb6421503fa987e	31	125	150	36	5	16	12	36
D	dec75326140ba98f	25	132	161	27	7	9	10	27
E	efd86437251cba90	30	133	157	27	5	12	9	27
F	f0e97548362dcba1	26	128	159	36	6	14	13	36

Table.11. Cryptographic analysis of 16, 4 bit crypto S-boxes under IP (x^4+x^3+x^2+x+1) with DE 31 over Galois field GF(2^4).

Discussion. Now out of total 16 4-bit crypto S-boxes 2 have 24, 4 have 25, 2 have 26, 2 have 29, 4 have 30 and 2 have 31existing linear relations i.e. they are secure from this attack. Again out of total 16 4-bit crypto S-boxes 2 have 120, 2 have 125, 2 have 126, 2 have 128, 2 have 131, 2 have 132, 4 have 133 8s in LAT i.e. they are very much secure to this attack. Now out of total 16 4-bit crypto S-boxes 4 have 150, 4 have 157, 4 have 159 and 4 have 161 0s in DDT i.e. they are secure from this attack. At last out of total 16 4-bit crypto S-boxes 4 have 27 and 12 have 36 8s in DAT i.e. they are secure from this attack too.

S-boxes with additive element 0 to F in hex has a range 5 to 10 out of total 16 SFO SAC satisfactions, 9 to 17 out of total 24 2nd order MHO SAC satisfaction, 9 to 14 out of total 16 3rd order MHO SAC satisfaction, 27 to 36 out of total 64 all MHO SAC satisfaction so they are poor 4-bit crypto S-boxes from only SFO SAC angle but good secure 4-bit crypto S-boxes from MHO SAC angle.

3.5 Comparative analysis of Generated 48, 4-bit crypto S-boxes with existing 36, 4-bit crypto S-boxes. In existing 16 4-bit crypto S-boxes of Lucifer are almost secure in same manner than DES 4-bit crypto S-boxes. From four cryptanalysis algorithm it is clear that the 4-bit crypto S-boxes of Lucifer is defined in the same way as the 4-bit crypto S-boxes of DES. But the SAC results are better in 4-bit crypto S-boxes of Lucifer. However the generated 3 set of 16 4-bit crypto S-boxes have better result than the 4-bit crypto S-boxes of Lucifer and DES where 2nd set or 4-bit crypto S-boxes generated with addition of additive elements from 0 to F in hex to each element of MI S-box one at a time under IP x^4+x^3+1 with DE 25 over Galois field $GF(2^4)$ gives optimum result.

4. Conclusion. Here in this paper 48, 4-bit crypto S-boxes are generated under 3 IPs with DE 19, 25, 31 over Galois field $GF(2^4)$. On the contrary there are 36 4-bit crypto S-boxes exists in 2 variants of Lucifer and DES algorithm. The cryptanalysis of 32 DES, 4 Lucifer and 48, generated 4-bit crypto S-boxes proves that the generated 4-bit crypto S-boxes are better than 4-bit crypto S-boxes of DES and Lucifer. The 2nd set or 4-bit crypto S-boxes generated with addition of additive elements from 0 to F in hex to each element of MI S-box one at a time under IP x^4+x^3+1 with DE 25 over Galois field $GF(2^4)$ gives optimum result. So it can be concluded that the generated 48 4-bit crypto S-boxes are secure from the angle of crypto security.

5. Acknowledgement. For this exhaustive work I would like to acknowledge my supervisors Dr. Ranjan Ghosh, Associate Professor, Institute of Radio Physics and Electronics, University of Calcutta and Prof. (Dr.) Amlan Chakrabarti Dean, Faculty council of Post graduate Studies in Engineering and Technology, University of Calcutta for their continuous encouragement and help. I would also like to acknowledge Prof. (Dr.) Debatosh Guha Head Dept. Institute of Radio Physics and Electronics, University of Calcutta for providing me with the nice infrastructure.

References.

[1] Church R, Tables of irreducible polynomials for the first four prime moduli, The Annals of Maths., 2nd Series, vol. 36, no. 1, 198-209, Jan (1935) http://www.jstor.org/stable/1968675.

[2] JKM Sadique Uz Zaman, Sankhanil Dey, Ranjan Ghosh, An Algorithm to find the Irreducible Polynomials over Galois Field GF(p^m), January 2015,International Journal of Computer Applications 109(15):24-29,DOI:10.5120/19266-1012.

[3] Sankhanil Dey and Ranjan Ghosh, A new algorithm to search for irreducible polynomials with decimal equivalents of polynomials over Galois Field $GF(p^q)$, International Journal of Mathematics and Computation, Vol.29, Issue. #3, pp.110-122 , June 2018. CESER publishers.

[4] Junsoo Ha, Irreducible polynomials with several prescribed coefficients, Finite Fields and Their Applications, Volume 40, July 2016, Pages 10-25,https://doi.org/10.1016/j.ffa.2016.02.006.

[5] Adams, Carlisle, Tavares, Stafford, "The structured design of cryptographically good S-boxes", J. Cryptology (1990) 344 vol. 3, pp : 27-41.

[6] Dey, S. and Ghosh, R. (2018) A Review of Existing 4-Bit Crypto S-Box Cryptanalysis Techniques and Two New Techniques with 4-Bit Boolean Functions for Cryptanalysis of 4-Bit Crypto S-Boxes*. Advances in Pure Mathematics, **8**, 272-306. doi: 10.4236/apm.2018.83015.

[7] Dey Sankhanil and Ghosh Ranjan, "A Review of Cryptographic Properties of S-Boxes with Generation and Analysis of Crypto Secure S-Boxes", International Journal of Electronics and Information Engineering, vol.8, no.1, pp.49-73, DOI: 10.6636/ IJEIE.201803.8(1).06. Mar 2018.

[8] Data Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 46, National Bureau of Standards, Washington, DC (1977).

[9] Data Encryption Standard (DES), Federal Information Processing Standards Publication (FIPS PUB) 46-3, National Institute of Standards and Technology, Gaithersburg, MD (1999).

[10] Joan Daemen,Vincent Rijmen (2000), AES Proposal: Rijndael,http://csrc.nist.gov/encryption/aes/ Last Visited: 7th February 2001.