IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

A New Approach towards Confusion Analysis of S-boxes using Truncated Differential Cryptanalysis

Avijit Datta[1*], Dipanjan Bhowmik[2], Sharad Sinha[3]

[1, 2, 3] University of North Bengal, West Bengal, India

[*]Corresponding Author: avijit.go2avi@gmail.com, Tel.: +91-9775802114

Available online at: www.ijcseonline.org

Accepted: 12/Jan/2019, Published: 31/Jan/2019

***Abstract*—** SAC matrices have been implemented for S-boxes of DES and AES to implement a higher order differential analysis, known as truncated differentials. This new approach will help us to find the vulnerability to attacks. After getting the original outputs corresponding to the input strings, inputs to s-boxes of DES and AES are then truncated in two parts, strings (**a, b**), of equal bit length Then each bit of both **a** and **b** is changed one after the other to get the new input and its corresponding output. Using all outputs of every possible input, SAC matrices are generated for statistical and truncated differential analysis to reach the conclusion.

***Keywords*—** Truncated Differential; S-box; SAC; Higher order differential; Cryptanalysis; Cryptology; Differential Cryptanalysis

I. INTRODUCTION

The Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are the well known and most widely used cryptosystem developed by IBM in the mid 70's. The method which analyzes the effect of differences in plaintext pairs on the differences of generated ciphertext pairs is called Differential Cryptanalysis. In $n-$ iterated cryptosystem, iterations are called a round and the cryptosystem is called $n-round$ cryptosystem. A function of the output of previous round and a *subkey* which is a key dependent value calculated using a key scheduling algorithm is called the *round function*.

For a given plaintext $P = (P^L, P^R)$ and round keys (r) $K_1, K_2, \ldots., K_r$ the ciphertext $C = (C^L, C^R)$ has been generated which is computed in r rounds [1]. The differential attacks can take place on the calculated differences between these pair of plaintexts and its corresponding ciphertext with a non-uniform probability distribution.

Conventional differential is a difference of two bit-strings of the same length. A differential that predicts only parts of an n-bit value is called truncated differential [1]. Let **(a, b)** be an $i-$round differential. If a' is a subsequence of a and b' is subsequence of b, then $(\boldsymbol{a'}, \boldsymbol{b'})$ is called an $i-$round truncated differential.

In this paper, a new way of implementing truncated differential on generated SAC matrices of every possible input and corresponding output of S-boxes of DES and AES is proposed and the vulnerability towards the attacks on these S-boxes is statistically analyzed.

Section I contain the introduction of the work, section II contain related works of the proposed work, section III is contained discussion on differential attacks and truncated differential, section IV defining designing of S-box and SP network, section V is about the proposed method, section VI contain a brief experimental result, section VII and VIII is included the discussion and conclusion respectively.

II. RELATED WORK

In this section some of the related works on differential cryptanalysis has been included to facilitate future discussions.

Xuejia Lai discussed the higher order derivatives and differential cryptanalysis in [2]. His definition on higher order derivative is:

Let, $(S, +)$ and $(T, +)$ be Abelian groups. For a function $f : S \longrightarrow T$, the derivatives of the f at point $a \in S$ is defined as

$$\Delta_{\boldsymbol{a}} \boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{f}(\boldsymbol{x} + \boldsymbol{a}) - \boldsymbol{f}(\boldsymbol{x}) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

The derivatives of f is a function from S to T which define the $i-th$ derivative of f at $(a_1, a_2, \ldots., a_i)$ as

$$\Delta^{i}_{a_1, a_2, \ldots., a_i} \boldsymbol{f}(\boldsymbol{x}) = \Delta_{\boldsymbol{a}} \left(\Delta^{i-1}_{a_1, a_2, \ldots., a_{i-1}} \boldsymbol{f}(\boldsymbol{x})\right) \quad \ldots\ldots\ldots\ldots\ldots (2)$$

where $\Delta^{i-1}_{a_1,a_2,\ldots,a_{i-1}} f(x)$ being the $(i-1)-th$ derivative of f.

The derivatives for binary functions are computed with the group of bitwise XOR operations denoted by $\oplus$.

The differential and probability of a differential is defined as a couple of $(\mathbf{a},\mathbf{b})$ and $P(\Delta\, y = b|\, \Delta\, x = a)$.

Biham and Shamir in "Differential Cryptanalysis of DES-like Cryptosystems" [3] introduced differential cryptanalysis on DES considering the iterative rounds based on S-boxes, bit permutations, arithmetic operations and the exclusive-OR operations.

Kaisa Nyberg in [4] discussed differentially uniform mapping for cryptography with other cryptographic properties like large distance from affine functions, high nonlinear order and efficient computability. Special attention has been focused on the nonlinearity properties of round functions and it seems that the security of the cryptosystem may be increased by increasing the size of S-boxes or may be by replacing the set of small parallel substitution by one large transformation with desirable properties.

Nyberg and Knudsen in [5] have shown that DES-like iterated ciphers are provably resistant against differential attacks.

It is shown in [6] that perfect non-linear mappings from $GF(2)^m \longrightarrow GF(2)^n$ only exist for an even m and $m \geq 2n$ and they can be included in DES-like ciphers with expansion mappings that double the block length.

Truncated differential has been introduced by Knudsen in [1]. Truncated differentials are differentials where only a part of difference in the cipher text can be predicted. He showed some examples of Feistel block ciphers that are secure against differential attacks [21] but vulnerable to the differential attack using truncated differentials and higher order differentials.

In [7], truncated differential cryptanalysis has been done to ensure security of E2. They evaluated the security against the attacks using truncated differentials with bitwise differentials.

An improved truncated differential cryptanalysis of KLEIN [8] has been introduced by Rasoolzadeh, Shahram, et al. KLEIN is a type of light weighted block cipher which has three variants, namely KLEIN-64, -80, -96 with having 12, 16 and 20 rounds, respectively. It has an SPN structure which combines 4-bit S-boxes with AES's MixColumn.

Truncated differential cryptanalysis has also been done for Camellia block cipher, which was cooperatively designed by NTT and Mitsubshi Electric Corporation and submitted to NESSIE by S. Lee, S. Hong et.al [9]. They presented truncated differential cryptanalysis for the modified Camellia with 7 rounds and found 8-bit key with 3.2^{81} plaintexts and for Camellia with 8 rounds they found 16-bit key with 3.2^{82} plaintexts.

Forrié R. [17] has introduced a Boolean function $f(\underline{x})$ with n bits input and one bit output. Walsh-transform has shown to be very useful for the statistical analysis of properties of Boolean function. According to [17], a Boolean function $f(\underline{x})$ fulfills the SAC if and only if, for all $i \in \{1,2,\ldots\ldots,n\}$, its Walsh-transform

$$\hat{F}(\underline{w}),\ \underline{w} = [w_1, w_2, \ldots\ldots, w_n], \qquad \ldots\ldots\ldots\ldots (3)$$

fulfills

$$\sum_{\underline{w}\in Z_2^n}(-1)^{w_i}.\hat{f}^2(\underline{w}) = 0, \qquad \ldots\ldots\ldots\ldots (4)$$

where Z_2^n denotes the *n*-dimensional vector space over the finite field GF(2). Theorem stated here proves that a Boolean function fulfils the SAC if and only if it is 50% dependent on each of its input bits.

Definition 1 [17]: A function $\hat{f} : Z_2^n \longrightarrow \{1,-1\}$ $(resp. Z_2^n \longrightarrow \{1,0\})$ is said to be 50% dependent on its i-th input bit x_i if and only if any two $n-tuples$ $\underline{x}$ and $\underline{x_i}$ that differ only in bit i are mapped onto two different values with probability $1/2$ and onto the same value with the same probability $1/2$.

Or formally,

$$\sum_{\underline{x}\in Z_2^n} \hat{f}(\underline{x}) \,.\, \hat{f}\left(\underline{x} \oplus \underline{c_i}\right) = \mathbf{0} \qquad \ldots\ldots\ldots\ldots (5)$$

for {1,-1} – valued functions, and

$$\sum_{\underline{x}\in Z_2^n} \hat{f}(\underline{x}) \oplus\ \hat{f}\left(\underline{x} \oplus \underline{c_i}\right) =\ \mathbf{2^{n-1}} \qquad \ldots\ldots\ldots\ldots (6)$$

for {1,0} – valued functions.

Thus a Boolean function fulfils the SAC if and only if it is 50% dependent on each of its input bits.

The sufficient condition for a function to be 50% dependent on one or more of its input bits can be extracted from the following theorem.

Theorem 1 [17]: If for some non-zero $\underline{c} \in Z_2^n$ and for all $\underline{w} \in Z_2^n$

$$\hat{f}^2\,(\underline{w}) = \hat{f}^2(\underline{w} \oplus \underline{c}) \qquad \ldots\ldots\ldots\ldots (7)$$

holds, and if $\underline{c}$ has Hamming weight m ($c_1 = c_1 = \cdots = c_m, 1 \leq m \leq n$), then $\hat{f}(\underline{x})$ is 50% dependent on the input bits $x_1, x_2, \ldots, x_m$.

III. DIFFERENTIAL ATTACKS AND TRUNCATED DIFFERENTIAL

If we consider a Feistel cipher with block size $2n$ with r rounds then the round function g is:

$$g: GF(2)^n \times GF(2)^n \times GF(2)^m \rightarrow GF(2)^n \times GF(2)^n$$

$$\boldsymbol{g(X,Y,Z) = (Y, f(Y,Z) + X)} \quad \ldots\ldots\ldots\ldots (8)$$

where f can be any function accepting two parameters, n bits and m bits and producing n bits. For any given plaintext $P = (P_L, P_r)$, the differential attacks exploit the difference of certain plaintexts and the difference of corresponding ciphertexts with non-uniform probability distribution.

The number of times the right key is counted over the number of times a random key is counted is called signal to noise ratio [1] and can be represented as:

$$\boldsymbol{S/N = \frac{|K| \times p}{\gamma \times \lambda}} \quad \ldots\ldots\ldots\ldots\ldots\ldots (9)$$

where p is the probability of differential used in the attack, |K| is the number key, γ is the key suggested for each pair of plaintext and λ is the ratio of non-discarded pairs to all pairs. If $S/N \leq 1$ then a differential attack will not succeed [3].

For generic differential attack on $2n$ Fiestel cipher, the prediction is done on n bits of ciphertext. The differential that predicts only a part of n bits is called truncated differential. Attackers have more freedom in choosing plaintexts or ciphertexts when using the truncated differential. So, ensuring strength and security against truncated differential analysis can provide a more strict evaluation of the security against differential cryptanalysis [7].

IV. Design of an S-box and SP Network

To get the advantages for attack on cryptosystem, cryptanalyst can collect information about statistical properties if strict avalanche criterion (SAC) or avalanche variable independence requirement is not satisfied [11].

To satisfy both SAC and avalanche variable independence requirement, a cryptographic transformation has been discovered as substitution boxes or S-boxes. An S-box should randomly select potentially invertible and single output bit function that satisfies SAC. Moreover when each input bit is complemented, the resulting avalanche variables are pair-wise independent [11]. The S-box that satisfies both of these properties is referred as perfect S-box.

As the heart of modern cryptography, Claude Shannon [12] proposed the Substitution Permutation (SP) network, and to confirm the confidentiality of bits of data in encryption or decryption of SP network, three basic steps has been described in [13] as:

a. Subkey is X-ORed with input data bits.

b. A substitution function $S_i : \mathbb{Z}_{2^n} \rightarrow \mathbb{Z}_{2^m}$ replaces n bits of data to increase confusion with lookup tables called S-boxes.

c. Permutation function shuffles the bits to cause diffusion within the data.

Fig. 1 shows a substitution permutation network with 3 rounds. S-boxes can be considered as Boolean mapping from $\{0,1\}^m \rightarrow \{0,1\}^n$ in the form $n \times n$. S-boxes are also the only non-linear form of operation in an encryption process.

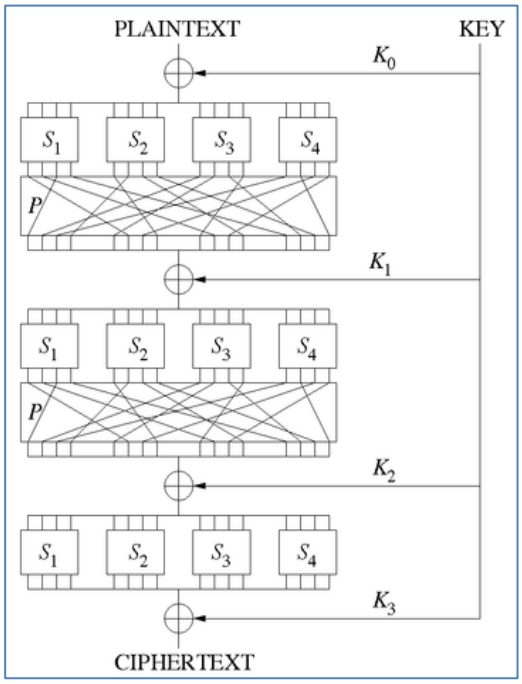

Fig. 1: SP Network with 3 rounds

V. Proposed Method

In [14][15], two different approaches have been presented, where confusion of S-boxes has been discussed statistically.

In first approach [14], the SAC (Strict Avalanche Criterion) matrix has been generated in comparison to the original ciphertext. In this approach, all elements of DES S-boxes and AES S-box take inputs individually and the SAC matrix is generated from the original ciphertext along with ciphertexts generated from the every one alternative bit alteration of the original inputs. By using the generated SAC matrix, the vulnerability of every bit of the ciphertext has been statistically computed and discussed.

In the other approach [15], the SAC matrix was generated with original ciphertext and ciphertexts of every two alternative bit alteration of original inputs. The method has been used for all 8 S-boxes of DES and the S-box of AES.

In this work, the truncated differential cryptanalysis approach has been implemented on S-boxes of DES and S-box of AES with a new proposal of the statistical analysis on the generated SAC. The proposed method has been compared with the conclusion of 2-bit approach [15] of confusion analysis of S-box.

The truncated differential cryptanalysis in this paper involves the following:

1) Analysis of frequency of every bit column-wise and its various avalanche effects from the generated SAC using truncated approach.

2) Coefficient variance analysis of generated SAC.

3) Analysis of frequency of various differential values from the generated SAC.

The SAC was introduced by Webster and Tavares in [16] and according to them SAC can be defined as: "If a function is to satisfy SAC, then each of its output bit should change with a probability of one half whenever a single input bit x is complemented to $\overline{x}$."

Using the V-vector (Vulnerability Vector) [18],[20], the proposed algorithm is as below:

A. Proposed Algorithm: Confusion Analysis of S-boxes using Truncated Differential Cryptanalysis

Input: S-box with length n, where n is the number of bits.

Step1: Choose a random number P, within the range of the S-box, where $P \in \mathbb{Z}_2^n$. Find the corresponding output value of S-box:

$$C = S(P)$$

Step 2: Change the P_is to find their corresponding output values C_is.

P_i may be generated by:

- Truncating the original input P of same size in $P(a, b)$ and getting two parts of P as P_a and P_b.
- Change the every individual bit of both P_a and P_b, for every iteration.
- Then concatenate P_a and P_b, in every iteration, to generate P_i.

Step 3: SAC matrix has to be created by $S_i = C_i \oplus C$, which to be included in the i^{th} row of a matrix of size $m \times n$, where m is the number bits of P and n is the number of bits of C.

Step 4: Find the count of $1s$ in each column of generated SAC matrix.

B. S-box structure of DES

The structure of S-box of DES is given in Fig. 2. The number of S-boxes in DES is 8 with the structure of 4×16 and values ranging from $(0)_{10}$ to $(15)_{10}$. For any 6-bit input, with the ranging value, each S-box of DES generates 4 bits of output.

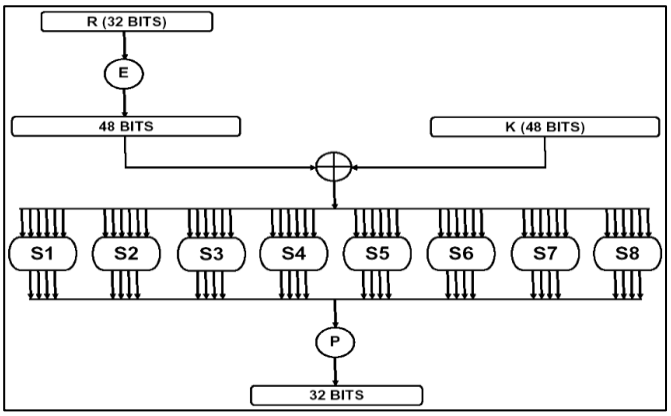

Fig. 2: S-boxes of DES

$S = matrix\ 4 \times 16, values\ from\ 0\ to\ 15$

$B\ (6\ bit\ input) = \boldsymbol{b_1} b_2 b_3 b_4 b_5 \boldsymbol{b_6}$

$\boldsymbol{b_1 b_6} \rightarrow r = row\ of\ the\ matrix\ (2\ bits: 00,01,10,11)$

$b_2 b_3 b_4 b_5 \rightarrow c$

$= column\ of\ matrix\ (0,1,\ldots,15)$

$C\ (output) = Binary\ representation\ S(r, c)$

C. S-box structure of AES

The structure of S-box of AES is shown in Fig. 3. There is a single non-linear S-box in AES with matrix structure 16×16.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig. 3: S-boxes of AES

$S = matrix\ 16 \times 16, in\ octal\ value\ 0\ to\ F$

$B\ (8\ bit\ input) = b_1 b_2 b_3 b_4 \boldsymbol{b_5 b_6 b_7 b_8}$

$b_1 b_2 b_3 b_4 \rightarrow r = row\ of\ the\ matrix\ for\ output$

$\boldsymbol{b_5 b_6 b_7 b_8} \rightarrow c = column\ of\ the\ matrix\ for\ output$

$C\ (8\ bit\ output) = octal\ value\ S(r, c)$

VI. EXPERIMENTAL RESULTS

A. *Coefficient Variance (CV) Analysis of Generated SAC of S-boxes of DES using Truncated Differential Method*

By following the proposed algorithm, using truncated plaintext $P(a, b)$, a SAC matrix has been generated for every possible input of every S-box of DES. The $1s$ of every column output of S-boxes have been counted and the sum of $1s$ of every column is being identified as V-vector (**V**ulnerability Vector) and computed for all 64 possible inputs and corresponding outputs of the 8 S-boxes. Some of the generated SAC matrices has been given in Table 1.0 and 2.0 and are compared with tables 1.1, 2.1 and 1.2, 2.2 which are generated from 2-bit [15] and 1-bit [14] alteration methods. The line graph of frequencies of V-vector for all 8 S-boxes of DES is showed in Fig. 4.

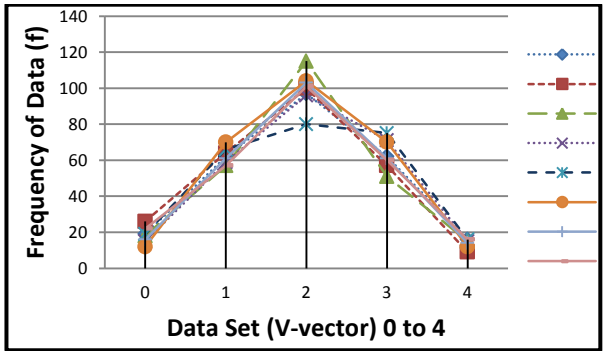

Fig. 4: Line Graph of Frequencies of V-vector for S-boxes of DES

TABLE 1.0 – SAC MATRIX OF INPUT '0' TO 'S-BOX 0' USING TRUNCATED DIFFERENTIAL APPROACH

SAC Matrix of Input - 0			
1	1	1	0
0	1	0	1
1	0	0	1
1	1	0	1
V-vector of Input - 0			
3	3	1	3

TABLE 1.1 – SAC MATRIX OF INPUT '0' TO 'S-BOX 0' USING 2-BIT ALTERATION APPROACH

SAC Matrix of Input - 0			
1	1	1	0
1	0	1	0
1	0	1	0
1	0	1	0
1	0	1	0
1	1	1	0
V-vector of Input - 0			
6	2	6	0

TABLE 1.2 – SAC MATRIX OF INPUT '0' TO 'S-BOX 0' USING 1-BIT ALTERATION APPROACH

SAC Matrix of Input - 0			
1	0	1	0
1	1	0	1
1	1	0	0
0	0	1	1
1	0	1	0
1	1	1	0
V-vector of Input - 0			
5	3	4	2

TABLE I.

TABLE 2.0 – SAC MATRIX OF INPUT '0' TO 'S-BOX 1' USING TRUNCATED DIFFERENTIAL APPROACH

SAC Matrix of Input – 0			
1	0	1	0
0	1	0	0
1	1	0	0
1	1	1	1
V-vector of Input – 0			
3	3	2	1

TABLE 2.1 – SAC MATRIX OF INPUT '0' TO 'S-BOX 1' USING 2-BIT ALTERATION APPROACH

SAC Matrix of Input – 0			
1	1	0	0
1	1	1	0
1	1	1	0
1	1	1	0
1	1	1	0
1	1	1	1
V-vector of Input – 0			
6	6	5	1

TABLE 2.2 – SAC MATRIX OF INPUT '0' TO 'S-BOX 1' USING 1-BIT ALTERATION APPROACH

SAC Matrix of Input – 0			
1	1	1	1
0	1	1	0
1	0	0	1
0	1	1	1
1	1	1	0
1	1	0	0
V-vector of Input – 0			
4	5	4	3

B. *Experimental Results for DES S-Boxes*

The experimental results of proposed test are in Table 3:

TABLE 3 – EXPERIMENTAL RESULTS OF PROPOSED TEST ON S-BOXES OF DES

S-box	Observed Mean	Variance	Standard Deviation	Coefficient of Variance
1	1.976563	1.030701	1.405903	0.711287
2	1.839844	0.993881	1.356408	0.737241
3	1.953125	0.935303	1.397542	0.715542
4	2.046875	0.974365	1.43069	0.698963
5	2.044719	1.097519	1.418351	0.705044
6	1.953125	0.872803	1.397542	0.715542
7	1.980469	0.948837	1.407291	0.710585
8	1.964844	1.049545	1.401729	0.713405

C. Coefficient Variance (CV) Analysis of Generated SAC of S-box of AES using Truncated Differential Method

By following the proposed algorithm, using truncated plaintext $P(a, b)$, a SAC matrix has been generated for S-box of AES. 1s of every column output of S-box has been counted and the sum of 1s of every column, is being identified as V-vector (**V**ulnerability Vector), has calculated for some example inputs and corresponding outputs of the S-box. Some of the generated SAC matrices has given below in Table 4.0 and 5.0 and are compared with tables 4.1, 5.1 and 4.2, 5.2 which are generated from 2-bit [15] and 1-bit [14] alteration method. The line graph of frequencies of V-vector for all inputs using S-box of AES is showed in Fig. 5.

TABLE 4.0 – SAC MATRIX OF INPUT 11000011TO AES S-BOX USING TRUNCATED DIFFERENTIAL APPROACH

Input : 11000011							
Original Output : 00101110							
0	1	0	0	1	1	0	0
1	1	1	0	1	0	0	0
0	0	0	0	0	1	1	1
0	1	0	0	1	0	1	0
V-vector of input 11000011							
1	3	1	0	3	2	2	1

TABLE 4.1 – SAC MATRIX OF INPUT 11000011TO AES S-BOX USING 2-BIT ALTERATION APPROACH

Input : 11000011							
Original Output : 00101110							
1	0	0	0	0	1	0	0
1	1	1	1	0	1	0	1
1	1	1	1	0	0	1	0
0	1	0	0	0	1	1	0
0	1	1	1	0	1	0	1
0	1	0	1	1	0	0	1
0	1	0	0	0	1	0	1
V-vector of input 11000011							
3	6	3	4	1	5	2	4

TABLE 4.2 – SAC MATRIX OF INPUT 11000011TO AES S-BOX USING 1-BIT ALTERATION APPROACH

Input : 11000011							
Original Output : 00101110							
1	1	1	0	0	1	0	1
0	0	0	1	0	0	1	1
1	1	1	0	1	1	1	0
1	0	0	1	1	0	0	1
1	1	1	0	0	0	0	0
0	0	1	1	1	0	0	1
1	0	0	0	0	1	1	1
1	1	0	1	1	0	1	0
V-vector of input 11000011							
6	4	4	4	4	3	4	5

TABLE 5.0 – SAC MATRIX OF INPUT 10101010TO AES S-BOX USING TRUNCATED DIFFERENTIAL APPROACH

Input : 10101010							
Original Output : 10101100							
0	1	1	0	1	1	0	0
1	1	0	1	0	1	1	1
0	0	1	1	1	0	1	1
0	0	0	1	0	1	0	1
V-vector of input 10101010							
1	2	2	3	2	3	2	3

TABLE 5.1 – SAC MATRIX OF INPUT 10101010 TO AES S-BOX USING 2-BIT ALTERATION APPROACH

Input : 10101010							
Original Output : 10101100							
1	1	1	1	1	1	0	1
1	0	0	0	1	0	1	1
0	1	0	0	0	1	1	1
1	1	0	0	1	0	0	0
1	1	0	1	1	0	1	1
0	1	1	0	1	1	1	0
0	0	1	0	1	1	0	0
V-vector of input 10101010							
4	5	3	2	6	4	4	4

TABLE 5.1 – SAC MATRIX OF INPUT 10101010 TO AES S-BOX USING 1-BIT ALTERATION APPROACH

Input : 10101010							
Original Output : 10101100							
0	0	0	1	1	0	1	0
0	1	1	1	1	0	0	0
1	0	0	0	0	0	0	1
0	0	0	0	1	0	1	1
1	1	0	0	0	1	0	1
0	0	0	1	1	0	1	1
0	0	1	1	1	1	0	1
1	0	0	1	1	1	0	1
V-vector of input 10101010							
3	2	2	5	6	3	3	6

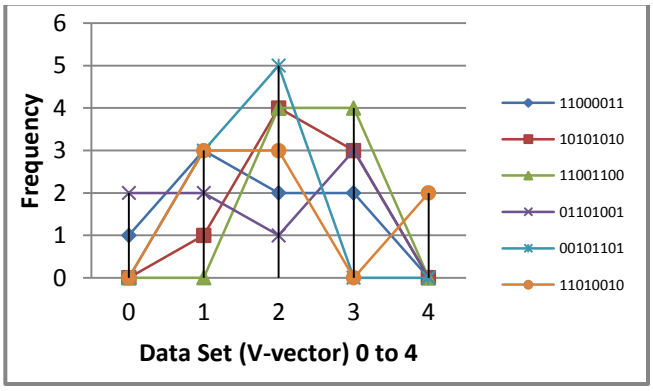

Fig. 5: Line Graph of Frequencies of V-vector for inputs using S-box of AES

D. *Experimental Results for AES S-Box*

The experimental results of proposed test on the S-box of AES are in Table 6:

TABLE 6 – EXPERIMENTAL RESULTS OF PROPOSED TEST USING AES S-BOX

Input	Observed Mean	Variance	Std. Deviation	Coefficient of Variance
$(195)_{10}$	1.625	0.984375	0.992157	0.610558
$(170)_{10}$	2.25	0.4375	0.661438	0.293972
$(204)_{10}$	2.5	0.25	0.5	0.2
$(105)_{10}$	1.625	1.484375	1.218349	0.749753
$(45)_{10}$	1.625	0.234375	0.484123	0.297922
$(210)_{10}$	2.125	1.359375	1.165922	0.548669

VII. DISCUSSION

By using the proposed algorithm, coefficient of variance has been calculated as a statistical measure of dispersion for the output corresponding to all possible inputs of every S-box of DES and six numbers of randomly chosen inputs to the single S-box of AES.

From the generated SAC matrix from each S-box of DES, the vulnerability vector (V-vector) has been calculated by summation of $1's$ of every column of SAC matrices and by using the data set ranging from 0 to 4 and it's frequency of appearance, the line graph has been plotted in Fig. 5. To calculate the coefficient of variance of every S-box, statistical mean, variance and standard deviation have also been calculated. It is found that the coefficient of variance (CV) ranges from 0.69 to 0.73, where CV < 1 and average coefficient of variance of S-boxes of DES is 71%.

Using the single S-box of AES, the V-vector has been calculated in same way and using data set ranging from 0 to 4 and it's frequency of appearance, the line graph has been plotted in Fig. 6. To calculate the coefficient of variance of the inputs using single S-box, statistical mean, variance and standard deviation have also been calculated. The coefficient of variance (CV) is found to range from 0.20 to 0.74 where CV < 1 and average coefficient of variance of S-boxes of DES is 45%.

VIII. CONCLUSION

Confusion and diffusion are the two major aspects to measure of the strength of a block cipher and there exist different methods to test diffusion and confusion characteristics of cryptographic algorithms. In this proposed method, to test the confusion characteristic, the truncated differential approach has been used to analyze statistically the occurrence of $1's$ of every column of SAC matrices of DES S-boxes and AES S-box.

For the both cases of AES and DES, the coefficient of variance (CV) is ranging from 0.69-0.73 and 0.2-0.74, respectively, which are in the lower end of the spectrum which indicating that performances of S-boxes of DES and AES are pretty good with respect to the proposed test using truncated differential approach. The average CV of DES and AES is 71% and 45%, respectively, which helps us to draw the conclusion that the performance of S-box of AES is better than the performance of S-boxes of DES.

The proposed truncated differential approach of testing of confusion characteristics of S-boxes will lead us to draw an algorithm of testing Boomerang Attack.

REFERENCES

[1] Knudsen, Lars R. "*Truncated and higher order differentials*." International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 1994.

[2] X. Lal. "*Higher order derivatives and differential cryptanalysis*". In Proc. "Symposium on Communication, Coding and Cryptography", in honour of James L. Massey on the occasion of his 60'th birthday, Feb. 10-13, 1994, Monte-Verita, Ascona, Switzerland, 1994.

[3] E. Biham and A. Shamir. "*Differential cryptanalysis of DES-like cryptosystems*". Journal of Cryptology, 4(1):3-72, 1991.

[4] K. Nyberg. "*Differentially uniform mappings for cryptography*". In T. Helleseth, editor, Advances in Cryptology- Proc. Eurocrypt'93, LNCS 765, pages 55-64. Springer Verlag, 1993.

[5] K. Nyberg and L.R. Knudsen. "*Provable security against differential cryptanalysis*." In E.F. Brickell, editor, Advances in Cryptology - Proc. Crypto'92, LNCS 740, pages 566-574. Springer Verlag, 1993.

[6] Nyberg, Kaisa. "*Perfect nonlinear S-boxes*." Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1991.

[7] Moriai S., Sugita M., Aoki K., Kanda M. (2000) "*Security of E2 against Truncated Differential Cryptanalysis*." In: Heys H., Adams C. (eds) Selected Areas in Cryptography. SAC 1999. Lecture Notes in Computer Science, vol 1758. Springer, Berlin, Heidelberg.

[8] Rasoolzadeh, Shahram, et al. "*An improved truncated differential cryptanalysis of KLEIN*." Tatra Mountains Mathematical Publications 67.1 (2016): 135-147.

[9] Lee, Seonhee, et al. "*Truncated differential cryptanalysis of Camellia*." International Conference on Information Security and Cryptology. Springer, Berlin, Heidelberg, 2001.

[10]https://www.cosic.esat.kuleuven.be/ecrypt/courses/albena11/slides/LRK-truncated_differentials.pdf

[11] Webster, A. F., and Stafford E. Tavares. "*On the design of S-boxes*." Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1985 (pp. 523-534).

[12] Shannon, C.E. "*A mathematical theory of communication*." Bell System Technical Journal 27, 1948. p. 379–423, 623–656.

[13] Ramamoorthy, V., et al., "*The Design of Cryptographic S-boxes Using CPSs*." J. Lee (Ed.): CP 2011, LNCS 6876, Springer-Verlag Berlin Heidelberg, 2013. p. 54-68.

[14] A.Datta, D.Bhowmick, S. Sinha, "*A Novel Technique for Analysing Confusion in S-boxes*." International Journal of Innovative Research in Computer and Communication Engineering, 2016. 4(6): p. 11608-11615.

[15] A.Datta, D.Bhowmick, S. Sinha, "*Implementation of SAC Test for Analyzing Confusion in an S-box Using a Novel Technique*." International Journal of Scientific Research in Computer Science Applications and Management Studies, Vol. 7, Issue 3, No. 182

[16] Webster, A.F., Tavares, S.E. "*On the Design of S-boxes*". Advance in Cryptology. Proc. CRYPTO '85, Springer-Verlag, Berlin, 1986. pp. 523-534.

[17] Forrié R. (1990) "*The Strict Avalanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition*." In: Goldwasser S. (eds) Advances in Cryptology — CRYPTO' 88. CRYPTO 1988. Lecture Notes in Computer Science, vol 403. Springer, New York, NY

[18] D.Bhowmick, A.Datta, S. Sinha. "*A Bit-Level Block Cipher Diffusion Analysis Test*." Springer International Publishing Switzerland 2015: S.C.Satpathy et. al. (eds), Proc of 3rd Int. Conf. on Front. of Intell. Comput. (FICTA) 2014-Col. I, Advances in Intelligent Systems and Computing 327. pp: 667-674.

[19] Coppersmith, D. "*The Data Encryption Standard and its Strength against Attacks*." IBM Journal of Research and Development. 38(3) 243, 1994.

[20] P. Sharma, D. Mishra, V.K. Sarthi, P. Bhatpahri, R. Shrivastava, "*Visual Encryption Using Bit Shift Technique*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.3, pp.57-61, 2017

[21] M. Arora, S. Sharma, "*Synthesis of Cryptography and Security Attacks*", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.5, pp.1-5, 2017

Authors Profile

Avijit Datta is a Research Scholar in the Department of Computer Science and Application, University of North Bengal and Assistant Professor of Siliguri Institute of Technology, Siliguri. He received Master of Computer Application (MCA) degree in 2005 from UPTU, UP, India. His research interest is Cryptology.

Dipanjan Bhowmik is an UGC-SRF in the Department of Computer Science and Application, University of North Bengal. He received Master of Computer Application (MCA) degree in 2011 from University of North Bengal, WB, India. His research interest is Cryptology.

Sharad Sinha is an Assistant Professor of University of North Bengal. He received Ph.D. degree in 2008 and Master of Computer Application (MCA) degree in 1992 from University of North Bengal, WB, India. His research interest is Cryptology, NLP.

