Appendix 2: One of the Published Paper

IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

A Novel Technique for SAC Analysis of S-Boxes for Boomerang-Style Attacks

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

DOI: https://doi.org/10.26438/ijcse/v7i5.713 | Available online at: www.ijcseonline.org

Accepted: 10/May/2019, Published: 31/May/2019

***Abstract*—** In recent times, there exist several approaches for differential-style attacks like truncated differential attack, high-level differential attack, boomerang attack etc. This paper involves the study of boomerang-style attack on S-boxes and a new SAC analysis approach to test the strength of S-boxes against such attacks. The proposed analysis is tested on each input elements of 8 S-boxes of DES and 8 input elements on the S-box of AES. The vulnerability factor $^{n}/_{2}$ has been measured by calculating all $\mathbf{1's}$ of every column from the generated SAC matrix. Finally a comparison of standard deviation, coefficient of variance and other factors show the way towards the conclusion.

***Keywords*—**Block Cipher, S-box, Differential Cryptanalysis, Boomerang attack, Truncated Differential

I. INTRODUCTION

Differential cryptanalysis is one of the most important cryptanalytic techniques in cryptology. Published cipher may be broken by using differential cryptanalysis. So, one of the most important responsibilities of the block cipher designer is to ensure protection and security against such cryptanalysis.

The upper bound probability of any differential characteristics is tentatively p and the designer of the algorithm presumes, following the "folk theorem", that differential attack requires at least $^{1}/_{p}$ texts to break the cipher. [1] But unfortunately the "folk theorem" is not always right, as there is a type of differential attack, called Boomerang attack that can allow an adversary to beat the $^{1}/_{p}$ bound in some cases.

In this paper, the possibility of boomerang type attack on S-boxes of cryptographic algorithms has been measured. To represent the approach, the boomerang approach has been implemented to generate a SAC matrix for all possible inputs of all S-boxes of DES and all possible input of the S-box of AES. The generated SAC matrix is leads towards the statistical analysis of vulnerability of attack.

The Section I contains the introduction of the work, section II contains related works of the proposed technique, section III contains discussion on differential cryptanalysis and boomerang attack, section IV defines the design of S-boxes, section V is about proposed method, section VI contains brief experimental results, and finally, sections VII and VIII include the discussion and conclusion respectively.

II. RELATED WORK

D. Wagner, in his research [1] introduced an attack called Boomerang attack. This attack leads to prove that the so called folk theorem is not always right according to which, differential attack requires at least $^{1}/_{p}$ text to break a cipher where, p is the upper bound probability of any differential characteristics. According to his research, if the best characteristic for half of the rounds of the cipher has probability q, then the boomerang attack can be used successfully on $O(q^{-4})$ chosen text. In some cases, it may be possible that $q^{-4} \ll p^{-1}$, wherein boomerang attack allows one to beat the folk theorem bound. Sometimes, Boomerang attack also uses some extensive structures that are available in conventional differential attack.

Boomerang connectivity table is a good cryptanalysis tool [2]. In this research paper, it is revisited with the issue of dependency of two characteristics in a block cipher E_m and proposed a new tool called Boomerang Connectivity Tool (BCT), which evaluates r in a systematic and easy-to-understand way when E_m is composed of a single S-box layer. BCT shows that the probability around the boundary may be even higher than p or q.

A variant of differential cryptanalysis against the block cipher, Impossible Boomerang Attack (IBA) was introduced by Choi et. al. [3]. This research approach is the combination of differential cryptanalysis and boomerang attack.

Amplified Boomerang attack has been introduced in a research [4] dedicated on SHACAL, which is a 4-round block cipher [6]. SHACAL was designed by using hash standard SHA-1in encryption mode for the first time. Kim et. al. proposed a 10-step differential characteristic with probability 2^{-12} in rounds 2 and 4. Using this characteristic, they described a 36-step boomerang distinguisher. With this distinguisher they devised amplified boomerang attacks on reduced round SHACAL with different size keys.

A key recovery attack on the full round of SQUARE using a related key boomerang distinguisher was proposed in [5]. They constructed a 7-round related key boomerang distinguisher with probability 2^{-119} by finding local collision[7], and calculated its probability using ladder switch and local amplification techniques.

Analysis of vulnerability factor for truncated differential using SAC has been proposed in [8]. This research approach describes and analyzes the truncated differential on S-boxes of DES and AES.

III. Differential Cryptanalysis and Boomerang Attack

A. Differential Cryptanalysis

The method which analyzes the effect of particular differences in plaintext pairs on the differences of the ciphertext pairs is call differential cryptanalysis [9]. Differential cryptanalysis is a chosen-plaintext attack on secret-key block ciphers that are based on iterating a cryptographically weak function r times. The success of attacks on r round cipher depends on the existence of $(r-1)$ -round differentials with higher probability [10]. The "difference" ΔX between two plaintexts (or ciphertexts) X and X^* can be defined as $\Delta X = X \oplus X^{*-1}$, where $\oplus$ denotes a specified group of operation on the set of plaintexts.

Differential cryptanalysis exploits the fact that the round function f in an iterated cipher is usually cryptographically weak [10]. In a differential cryptanalysis, all the sub-keys are fixed and only the plaintext can be chosen randomly. In differential cryptanalysis attack, differential probability helps us to determine which differential to use in the attack.

B. Boomerang Attack

Boomerang attack was introduced by David Wagner in [1] where he proved the 'folk theorem' of differential cryptanalysis as wrong. Boomerang attack uses the technique of truncated differential. So, if a cipher is safe from boomerang attack, then it also proves good against truncated differentials. The boomerang attack is a differential attack that attempts to generate a quartet structure at an intermediate value halfway through the cipher.

The attack considers four plaintexts A, A', B, B' along with their cipher-texts C, C', D, D'. If $E(\cdot)$ is the encryption operation and divide the cipher into $E = E_1 \circ E_0$ where E_0 is the first half of the cipher and E_1 is the last half then differential characteristics are $\Delta \rightarrow \Delta^*$ for E_0 and $\nabla \rightarrow \nabla^*$ for E_1^{-1}. The boomerang attack is given in *fig. 1*.

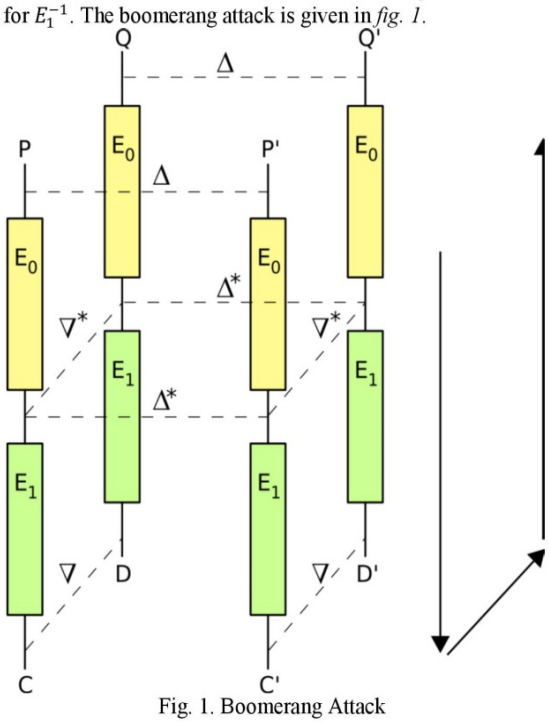

Fig. 1. Boomerang Attack

IV. Design Aspect of S-box

Substitution boxes (S-boxes) are the only non-linear part of a SP network in a cryptosystem. S-boxes are composed with highly non-linear Boolean functions. SP network is a private key cryptosystem. There are two components of SP network as π_s and π_p. Each permutation π_s is called S-box [11]. It replaces a set of input bits with a different set of bits as its output. The following criteria must be there in Boolean function that are responsible for a cryptographically good S-box [12] [13]:

- Bijection requires a 1-to-1 and onto mapping from input vectors to output vectors in the S-box of size $n \times n$ bits.

- Strict Avalanche Criterion (SAC) occurs if a change in one input bit i causes each output bit to change with probability of one half.
- Bit independence criterion or correlation-immunity.
- Non-linearity of S-box from input to output.
- Balance of Boolean vectors that are responsible for S-boxes that have the same number of $0's$ and $1's$.

Table 1. Partial Truth Table of S-Box 1in DES system

x_1	x_2	x_3	x_4	x_5	x_6	y_1	y_2	y_3	y_4
0	0	0	0	0	0	1	1	1	0
0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	1	0	0
0	0	0	0	1	1	1	1	1	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
1	1	1	1	0	0	0	1	0	1
1	1	1	1	0	1	0	1	1	0
1	1	1	1	1	0	0	0	0	0
1	1	1	1	1	1	1	1	0	1

For the construction of S-box, the function $f: \{0,1\}^n \rightarrow \{0,1\}^m$, with a high non-linearity, there are 2^n rows with m columns

V. PROPOSED METHOD

This research work was started with the confusion analysis of S-boxes. There are several previous research works in [8], [14], [15] where confusion of S-boxes has been analyzed with differential cryptanalysis. In this research, most importantly, confusion of S-boxes has been analyzed against the boomerang type attack.

In [8], 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.

In [14], 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 input. In 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 the original ciphertext and ciphertexts obtained from every two alternative bit alteration of original input. The method has been used for all 8 S-boxes of DES and the S-box of AES.

In this work, the boomerang-style attack has been implemented on S-boxes of DES and AES and SAC matrices have been generated, which are then subjected to the proposed statistical analysis.

The proposed analysis in this paper involves the following:

1) Analysis of frequency of every bit column-wise and its various avalanche effects from the generated SAC.
2) Coefficient variance analysis of generated SAC.
3) Analysis of frequency of various differential values from the generated SAC.

Using the V-vector (Vulnerability Vector) [16,17], the proposed algorithm is as below:

A. Proposed Algorithm: Confusion Analysis of S-boxes using Boomerang-style Attack

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

Step 1: Choose any 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.

$P_i s$ may be generated as follows:

- Generate all possible pairs of input bits by using:
$$\frac{n(n-1)}{2}$$
- Make the number of pairs multiple of the input bit size by padding $0's$ on the MSB side.
- Change every even bit of every pair.
- Combine the pairs to generate P_i.

Step 3: Construct the SAC matrix by including $S_i = C_i \oplus C$ 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, within the ranging value, each S-box of DES generates 4 bits of output.

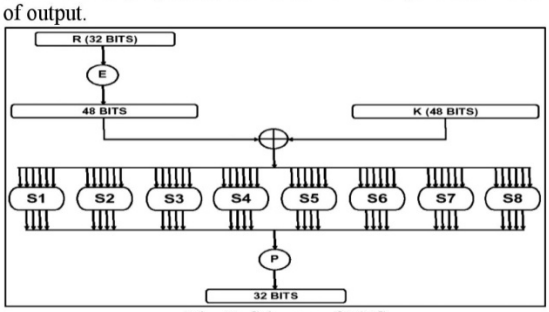

Fig. 2: S-boxes of DES

$S = matrix\ 4 \times 16, values\ from\ 0\ to\ 15$
$B\ (6\ bit\ input) = \boldsymbol{b_1}b_2b_3b_4b_5\boldsymbol{b_6}$
$\boldsymbol{b_1b_6} \rightarrow r = row\ of\ the\ matrix\ (2\ bits: 00,01,10,11)$
$b_2b_3b_4b_5 \rightarrow c$
$= column\ of\ matrix\ (0,1,\ldots,15)$
$C\ (output) = Binary\ representation\ S(r,c)$

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

$S = matrix\ 16 \times 16, in\ octal\ value\ 0\ to\ F$
$B\ (8\ bit\ input) = b_1b_2b_3b_4\boldsymbol{b_5b_6b_7b_8}$
$b_1b_2b_3b_4 \rightarrow r = row\ of\ the\ matrix\ for\ output$
$\boldsymbol{b_5b_6b_7b_8} \rightarrow c = column\ of\ the\ matrix\ for\ output$
$C\ (8\ bit\ output) = octal\ value\ S(r,c)$

VI. EXPERIMENTAL RESULTS

A. Coefficient Variance (CV) Analysis of Generated SAC of S-boxes of DES using Boomerang-style Attack Method

By following the proposed algorithm, using boomerang-style plaintext, a SAC matrix has been generated for every possible input for every S-box of DES. The $1's$ of every column output of S-boxes have been counted for all 64 possible inputs and corresponding outputs of the 8 S-boxes and identified as V-vector (**V**ulnerability Vector). 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 truncated [8] and 2-bit [15] alteration methods. The line graph of frequencies of V-vector for all 8 S-boxes of DES is showed in Fig. 4.

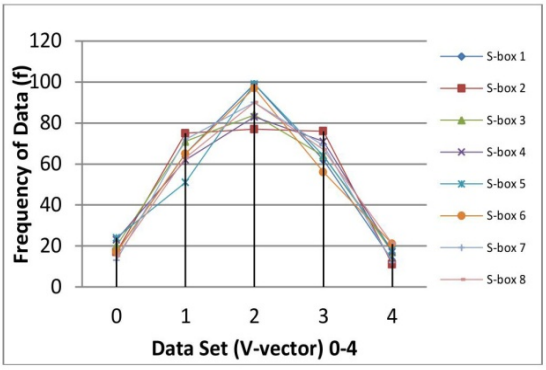

Fig. 4: Line Graph of Frequencies of V-vector for S-boxes of DES

TABLE 1.0 – SAC MATRIX OF INPUT '0' TO 'S-BOX 0' USING BOOMERANG-STYLE APPROACH

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

TABLE 1.1 – 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 1.2 – 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 2.0 – SAC MATRIX OF INPUT '0' TO 'S-BOX 1' USING BOOMERANG-STYLE APPROACH

SAC Matrix of Input - 0			
1	0	1	1
1	1	1	0
1	1	1	0
0	1	0	0

V-vector of Input - 0			
3	3	3	1

TABLE 2.1 – 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 2.2 – 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

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	1.957031	0.962997	0.981324	0.501435
2	1.957031	1.025497	1.012668	0.517451
3	1.949219	1.10289	1.050186	0.538773
4	1.988281	1.144394	1.069736	0.538034
5	2.003906	1.105453	1.051405	0.524678
6	1.996094	1.066391	1.032662	0.517341
7	1.980469	0.941025	0.970064	0.489816
8	2.0625	1.066406	1.032669	0.500688

C. *Coefficient Variance (CV) Analysis of Generated SAC of S-box of AES using Boomerang-Style Attack Method*

By following the proposed algorithm, using boomerang-style plaintext, a SAC matrix has been generated for S-box of AES. 1*s* of every column output of S-box has been counted and the sum of 1*s* of every column is being identified as the V-vector (**V**ulnerability Vector). The V-vectors have been calculated for some example inputs and corresponding outputs of the S-box. Some of the generated SAC matrices are given 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 truncated [8] and 2-bit [15] 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 BOOMERANG-STYLE APPROACH

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

TABLE 4.1– 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 4.2 – 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 5.0 – SAC MATRIX OF INPUT 10101010 TO AES S-BOX USING BOOMERANG-STYLE APPROACH

Input : 10101010							
Original Output : 10101100							
0	0	0	1	0	1	0	1
1	0	1	0	1	0	0	1
0	1	1	1	1	1	0	1
1	1	0	0	1	1	1	0
1	0	0	1	0	1	1	0
0	1	0	0	1	1	0	0
1	0	1	1	0	0	0	0

V-vector of input 10101010							
4	3	3	4	4	5	2	3

TABLE 5.1 – SAC MATRIX OF INPUT 10101010 TO 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 5.2 – 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

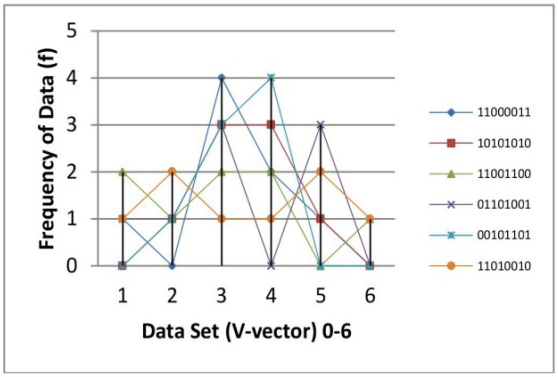

Fig. 5: Line Graph of Frequencies of V-vector for inputs using S-box of AES

D. Experimental Results for AES S-Box

The experimental results of the 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
$(195)_{10}$	3.25	1.1875	1.089725	0.3353
$(170)_{10}$	3.5	0.75	0.866025	0.247436
$(204)_{10}$	3	0.25	1.581139	0.527046
$(105)_{10}$	3.375	1.984375	1.408678	0.417386
$(45)_{10}$	3.375	0.484375	0.695971	0.206213
$(210)_{10}$	3.5	2.75	1.658312	0.473804

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 $1's$ in every column of each SAC matrix and by using the data set ranging from 0 to 4 and it's frequency of appearance, the line graph has been plotted as shown 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 0.48 to 0.53, where CV < 1 and average coefficient of variance of S-boxes of DES is 51%.
The V-vector for the single S-box of AES 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 as shown 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 0.52 where CV < 1 and average coefficient of variance of S-box of AES is 36%.

VIII.CONLUSION

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 work, a boomerang-style attack approach to test the confusion characteristic has been proposed and was used to analyze statistically the occurrence of $1's$ of every column of SAC matrices of DES and AES S-boxes.

For the both cases of AES and DES, the coefficient of variance (CV) was found to range from 0.48-0.53 and 0.2-0.52, respectively, which are in the lower end of the spectrum indicating that performances of S-boxes of DES and AES are pretty good with respect to the proposed test using boomerang-style approach. The average CV of DES and AES is 51% and 36%, respectively, which helps us to

draw the conclusion that the performance of S-box of AES is better than that of S-boxes of DES.

The proposed boomerang-style attack approach for testing confusion characteristics of S-boxes will lead us to formulate more testing algorithm on different cryptographic algorithms.

REFERENCES

[1] Wagner D. (1999) The Boomerang Attack. In: Knudsen L. (eds) Fast Software Encryption. FSE 1999. Lecture Notes in Computer Science, vol 1636. Springer, Berlin, Heidelberg

[2] Cid C., Huang T., Peyrin T., Sasaki Y., Song L. (2018) Boomerang Connectivity Table: A New Cryptanalysis Tool. In: Nielsen J., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2018. EUROCRYPT 2018. Lecture Notes in Computer Science, vol 10821. Springer, Cham

[3] Choy J., Yap H. (2009) Impossible Boomerang Attack for Block Cipher Structures. In: Takagi T., Mambo M. (eds) Advances in Information and Computer Security. IWSEC 2009. Lecture Notes in Computer Science, vol 5824. Springer, Berlin, Heidelberg

[4] Kim, Jongsung & Moon, Dukjae & Lee, Wonil & Hong, Seokhie & Lee, Sangjin & Jung, Seokwon. (2002). Amplified boomerang attack against reduced-round SHACAL. SIACRYPT 2002, LNCS 2501, pp. 243–253, 2002.c©Springer-Verlag Berlin Heidelberg 2002.doi: 10.1007/3-540-36178-2_15.

[5] Koo, Bonwook & Yeom, Yongjin & Song, Junghwan. (2010). Related-Key Boomerang Attack on Block Cipher SQUARE. IACR Cryptology ePrint Archive. 2010. 73. 10.1587/transfun.E94.A.3.

[6] H. Handschuh, D. Naccache, SHACAL, NESSIE project, October 2001.

[7] Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1-18.Springer, Heidelberg (2009)

[8] Avijit Datta, Dipanjan Bhowmik, Sharad Sinha, "A New Approach towards Confusion Analysis of S-boxes using Truncated Differential Cryptanalysis", International Journal of Computer Sciences and Engineering, Vol.7, Issue.1, pp.249-256, 2019.

[9] Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4(1), 3–72. doi:10.1007/bf00630563

[10] Lai X., Massey J.L., Murphy S. (1991) Markov Ciphers and Differential Cryptanalysis. In: Davies D.W. (eds) Advances in Cryptology — EUROCRYPT '91. EUROCRYPT 1991. Lecture Notes in Computer Science, vol 547. Springer, Berlin, Heidelberg

[11] Cheung, Jennifer Miuling. "The design of S-boxes." PhD diss., Sciences, 2010.

[12] C. Adams and S. Tavares. The structured design of cryptographically good s-boxes.Journal of Cryptology, 3(1):27–41, 1990.

[13] J. Cobas and J. Brugos. Complexity-theoretical approaches to the design and analysis of cryptographical boolean functions. InComputer Aided Systems Theory–EUROCAST2005, Lecture Notes in Computer Science. Springer-Verlag, Berlin, Germany, 2005.

[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] 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.

[17] 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

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.

