Journal of Applied Sciences

ISSN 1812-5654

Journal of Applied Sciences 15 (5): 728-740, 2015
ISSN 1812-5654

ansinet
Asian Network for Scientific Information

RESEARCH ARTICLE OPEN ACCESS

DOI: 10.3923/jas.2015.728.740

Evaluation of a Dynamic 3D S-Box Based on Cylindrical Coordinate System for Blowfish Algorithm

[1]Ashwak Alabaichi and [2]Mohammed S. Mechee
[1]Department of Computer Science, Faculty of Sciences, Kerbala University, Kerbala, Iraq
[2]Department of Mathematics, Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq

ARTICLE INFO
Article History:
Received: December 17, 2014
Accepted: March 20, 2015

Corresponding Author:
Ashwak Alabaichi,
Department of Computer Science,
Faculty of Sciences,
Kerbala University, Kerbala, Iraq

ABSTRACT

In order to measure the degree of security of RAF algorithm, some cryptographic tests must be applied such as randomness test, avalanche criteria, correlation coefficient and criteria of S-Box. In this study, we analyze the security of RAF. The security analysis is divided into two phases. The first phase investigates the output of the entire RAF, including the avalanche text and the correlation coefficient. The second phase investigates the quality of the dynamic 3D S-Box generated by the RAF by using the avalanche criterion (AVAL), the Strict Avalanche Criterion (SAC) and the Bit Independence Criterion (BIC). In addition, RAF algorithm is compared with the Blowfish Algorithm (BA). The avalanche text findings show that both algorithms produced satisfactory results on the second round. The correlation coefficient for RAF showed better non-linearity than BA. The S-Box analyses show that the dynamic 3D S-Box in the RAF is equipped with more security features than dynamic S-boxes in BA. C++ is used in the implementation of both algorithms. MATLAB computing software is used to implement the properties (AVAL, SAC and BIC) as well as the avalanche text and the correlation coefficient.

Key words: S-Box criteria, avalanche text, correlation coefficient

INTRODUCTION

Numerous block ciphers are depending on the traditional Shannon idea of the serial application of confusion and diffusion. Normally, confusion is provided by some forms of substitution "S-Boxes" (Mar and Latt, 2008).

A significant amount of time is taken up on the design or on the analysis that focuses on the substitution boxes (S-Boxes) of the algorithm during the development of a symmetric or private key that comprises the construction of cryptosystems which are constructed as substitution-permutation (S-P) networks (i.e.,"DES-LIKE" system). The S-Boxes bring nonlinearity to the cryptosystems; hence require the strengthening of the cryptographic security. Serious limitations in the S-Boxes can cause the cryptography to break easily (Mar and Latt, 2008; Adams and Tavares, 1990; Hussain *et al*., 2010). Generally, two sets of problems arise in the selection of an S-Box before its cryptographic use can be considered secure. The first challenge lies in the design (or search) of a good S-Box while the second ch1allenge is the verification of a given S-Box as one that satisfies the requirements that entail the types and quantitative values of the desired properties for an S-Box.

The properties of S-Box namely Avalanche (AVAL), Strict Avalanche (SAC) and Bit Independence Criteria (BIC) which guarantee the randomness of the SPN are a measure of its security. Also, these properties are cryptographic desirable in S-Boxes, so they are used as guide in the design of S-Boxes (Adams and Tavares, 1990; Vergili and Yucel, 2000; Alabaichi *et al*., 2013a).

The publications of most of the work on the design of S-Box has attempted the identification of good S-Boxes based on a procedure that involves generating of designs randomly, evaluating them against selected evaluation criterion and rejecting those which fail to meet these criterions (Adams and Tavares, 1990).

This study in the first phase attempts to analyze the avalanche text and correlation coefficient in RAF after which the results are compared with the results of Blowfis's output in (Alabaichi *et al.*, 2013b). While in the seconds phase analyze the properties of AVAL, SAC and BIC that are used for the testing of security of dynamic 3D S-Box in RAF after which the results are compared with the results of Blowfish's S-Boxes in Alabaichi (Alabaichi *et al.*, 2013a).

SECURITY ANALYSIS

Security is the most important factor in evaluating cryptographic algorithms. Security includes features such as the randomness of the algorithm output, the avalanche effect, the correlation coefficient, the resistance of the algorithm to the cryptanalysis and the relative security compared with other candidates (Ariffin, 2012).

The S-Box is the keystone of modern symmetric ciphers, such as block and stream ciphers and is an essential component in the layout of any block system.

Three properties are chosen to test security of the dynamic 3D S-Box, namely, AVAL, SAC and BIC.

In this study, security analysis is divided into two phases. In the first phase, security analysis of the entire algorithm is performed and the results are compared with those of the BA. In the second phase, the component of the RAF, that is, the dynamic 3D S-Box is analyzed.

First phase (security analysis of the RAF): As mentioned in the previous section, the output of entire algorithm (the RAF) is analyzed and compared with the results of the BA in this phase. The analysis includes the avalanche text and the correlation coefficient between plaintext and ciphertext.

The randomness of the RAF output is analyzed in earlier studies titled "A dynamic 3D S-Box based on Cylindrical Coordinate System for Blowfish algorithm" (Alabaichi *et al.*, 2014a) and "A Cylindrical Coordinate System with Dynamic Permutation Table for Blowfish Algorithm" (Alabaichi *et al.*, 2014b).

Avalanche effect: The avalanche effect is a desirable property of any encryption algorithm. If one bit changes in either the plaintext or the key, a significant change occurs in at least half of the bits in the ciphertext, thus making it difficult to analyse ciphertext when an attempt to mount an attack is made. That is performing an analysis on ciphertext while trying to come up with an attack is difficult (Mahmoud *et al.*, 2013). The avalanche text is used to evaluate the avalanche effect of the RAF and the BA in this study. A block cipher satisfies the avalanche text effect when a fixed key and a small change in the plaintext result in a large change in the ciphertext (Dawson *et al.*, 1992).

Mathematically Eq. 1 is defined as:

$$\forall(x,y)|H(x,y) = 1, \text{average } (H(F(x))) = (n/2) \qquad (1)$$

where, F is the avalanche effect when the Hamming distance between the outputs of a random input vector and the output generated by randomly flipping one of its bits should be n/2 or 0.5, on average. That is a minimum message input change is amplified and it produces a maximum message output change, on average (Ariffin, 2012). Numerous researchers have conducted the avalanche effect test including (Ariffin, 2012; (Mahmoud *et al.*, 2013; Dawson *et al.*, 1992; Juremi *et al.*, 2012; Sulaiman *et al.*, 2012; Castro *et al.*, 2005; Doganaksoy *et al.*, 2010; Agrawal and Monisha, 2010; Mohan and Reddy, 2011; Ramanujam and Karuppiah, 2011).

Testing data: All data of the 16-byte blocks of the random plaintext as well as of the 16-byte random key were generated using the BBS pseudo-random bit generator. The 128 sequences of the 128-bit with a 128-bit random key are generated and used in the test for the RAF.

Empirical results and analysis: Table 1 and 2 summarize the values of the avalanche text for the first three rounds and the last round of the RAF algorithm. In each table, the columns "Different bit number (RAF)" indicate that the numbers of bits are different in the ciphertext when one bit is changed in the plaintext. Meanwhile, the columns "Ratio bits (RAF)" indicate the different number of bits divided by the total number of bit sequence.

As shown in Table 1 and 2 changing one bit in the input results in a change on approximately half of the output bits in the three rounds, that is, the second, third and last rounds in RAF algorithm. The average change in bits in the RAF algorithm are 0.4912, 0.4926 and 0.4950 in second, third and last rounds, respectively, whereas the average change in bits in the BA are 0.5110, 0.5098 and 0.4972 in second, third and last rounds, respectively (Alabaichi *et al.*, 2013b). In addition, the avalanche text of the RAF approximates the same avalanche text in the BA for these rounds. However, the avalanche text presented by the RAF in the first round is 0.2690 and in the BA in the first round is 0.2555 (Alabaichi *et al.*, 2013b). This result indicates that both algorithms exhibit good avalanche text in the second round.

The results of the avalanche text in both algorithms for the first to third rounds and the last round are presented in Fig. 1(a-d) and Table 1-2.

Correlation coefficient: The correlation coefficient is considered as one of the important aspects of block cipher security that deals with the dependency of the individual output bits on the input bits. This coefficient measures how the two variables affect each other, that is, how much one variable depends on the other. In this section, we use the correlation coefficient to measure the dependency between plaintext and ciphertext. The correlation values can determine the confusion effect of the block cipher. The correlation coefficient which is a number between (-1) and (1), measures the degree of linear relationship between two variables. The correlation is (1) in an increasing linear relationship and (-1) in a decreasing linear relationship. In case of independent variables, the correlation is 0 and the following values are the acceptable range for

Table 1: Values of the avalanche text for RAF algorithm in the first and second rounds

Different bits number (RAF) round 1	Ratio (RAF) round 1	Different bits number (RAF) round 2	Ratio (RAF) round 2	Different bits number (RAF) round 1	Ratio (RAF) round 1	Different bits number (RAF) round 2	Ratio (RAF) round 2
34	0.2656	62	0.4844	39	0.3047	75	0.5859
26	0.2031	57	0.4453	26	0.2031	58	0.4531
40	0.3125	68	0.5313	27	0.2109	61	0.4766
38	0.2969	72	0.5625	41	0.3203	71	0.5547
28	0.2188	58	0.4531	30	0.2344	61	0.4766
21	0.1641	49	0.3828	38	0.2969	65	0.5078
35	0.2734	74	0.5781	29	0.2266	63	0.4922
36	0.2813	74	0.5781	32	0.2500	65	0.5078
38	0.2969	71	0.5547	28	0.2188	51	0.3984
37	0.2891	70	0.5469	34	0.2656	62	0.4844
37	0.2891	66	0.5156	31	0.2422	63	0.4922
31	0.2422	60	0.4688	37	0.2891	72	0.5625
39	0.3047	68	0.5313	38	0.2969	62	0.4844
34	0.2656	68	0.5313	38	0.2969	64	0.5000
37	0.2891	62	0.4844	27	0.2109	57	0.4453
32	0.2500	55	0.4297	32	0.2500	63	0.4922
35	0.2734	65	0.5078	38	0.2969	65	0.5078
34	0.2656	64	0.5000	35	0.2734	64	0.5000
32	0.2500	54	0.4219	30	0.2344	62	0.4844
22	0.1719	57	0.4453	38	0.2969	59	0.4609
27	0.2109	57	0.4453	37	0.2891	63	0.4922
33	0.2578	67	0.5234	32	0.2500	70	0.5469
38	0.2969	65	0.5078	31	0.2422	66	0.5156
29	0.2266	64	0.5000	31	0.2422	59	0.4609
31	0.2422	64	0.5000	30	0.2344	59	0.4609
33	0.2578	60	0.4688	32	0.2500	62	0.4844
33	0.2578	65	0.5078	25	0.1953	53	0.4141
35	0.2734	65	0.5078	33	0.2578	61	0.4766
32	0.2500	69	0.5391	32	0.2500	70	0.5469
37	0.2891	63	0.4922	26	0.2031	48	0.3750
38	0.2969	67	0.5234	34	0.2656	57	0.4453
26	0.2031	58	0.4531	40	0.3125	74	0.5781
29	0.2266	71	0.5547	32	0.2500	64	0.5000
30	0.2344	62	0.4844	35	0.2734	62	0.4844
29	0.2266	59	0.4609	28	0.2188	54	0.4219
34	0.2656	60	0.4688	38	0.2969	69	0.5391
28	0.2188	60	0.4688	25	0.1953	52	0.4063
34	0.2656	62	0.4844	27	0.2109	53	0.4141
33	0.2578	66	0.5156	33	0.2578	65	0.5078
27	0.2109	60	0.4688	29	0.2266	59	0.4609
27	0.2109	56	0.4375	35	0.2734	64	0.5000
32	0.2500	61	0.4766	31	0.2422	53	0.4141
34	0.2656	64	0.5000	33	0.2578	66	0.5156
29	0.2266	65	0.5078	29	0.2266	59	0.4609
30	0.2344	66	0.5156	36	0.2813	68	0.5313
33	0.2578	63	0.4922	31	0.2422	66	0.5156
36	0.2813	60	0.4688	31	0.2422	66	0.5156
32	0.2500	58	0.4531	31	0.2422	67	0.5234
31	0.2422	66	0.5156	34	0.2656	66	0.5156
26	0.2031	54	0.4219	27	0.2109	60	0.4688
34	0.2656	64	0.5000	34	0.2656	59	0.4609
38	0.2969	72	0.5625	34	0.2656	63	0.4922
39	0.3047	68	0.5313	38	0.2969	62	0.4844
37	0.2891	66	0.5156	38	0.2969	70	0.5469
31	0.2422	59	0.4609	39	0.3047	67	0.5234
35	0.2734	56	0.4375	31	0.2422	64	0.5000
34	0.2656	63	0.4922	28	0.2188	60	0.4688
29	0.2266	58	0.4531	36	0.2813	71	0.5547
36	0.2813	67	0.5234	33	0.2578	66	0.5156
36	0.2813	66	0.5156	31	0.2422	61	0.4766
29	0.2266	65	0.5078	31	0.2422	60	0.4688
37	0.2891	70	0.5469	41	0.3203	69	0.5391
28	0.2188	54	0.4219	33	0.2578	58	0.4531
34	0.2656	61	0.4766	34	0.2656	60	0.4688
Average					0.2555		0.4912

Table 2: Values of the avalanche text for RA algorithm in the third and last rounds

Different bits number (RAF) round 3	Ratio (RAF) round 3	Different bits number (RAF) last round	Ratio (RAF) last round	Different bits number (RAF) round 3	Ratio (RAF) round 3	Different bits number (RAF) last round	Ratio (RAF) last round
59	0.4609	60	0.4688	68	0.5313	73	0.5703
61	0.4766	54	0.4219	71	0.5547	65	0.5078
63	0.4922	68	0.5313	60	0.4688	67	0.5234
62	0.4844	59	0.4609	66	0.5156	67	0.5234
65	0.5078	64	0.5000	66	0.5156	58	0.4531
59	0.4609	64	0.5000	65	0.5078	69	0.5391
70	0.5469	68	0.5313	67	0.5234	59	0.4609
71	0.5547	64	0.5000	72	0.5625	56	0.4375
62	0.4844	57	0.4453	62	0.4844	64	0.5000
64	0.5000	59	0.4609	56	0.4375	56	0.4375
66	0.5156	66	0.5156	63	0.4922	58	0.4531
63	0.4922	55	0.4297	63	0.4922	62	0.4844
66	0.5156	64	0.5000	57	0.4453	78	0.6094
70	0.5469	59	0.4609	55	0.4297	66	0.5156
56	0.4375	62	0.4844	61	0.4766	67	0.5234
57	0.4453	70	0.5469	61	0.4766	68	0.5313
62	0.4844	67	0.5234	64	0.5000	64	0.5000
57	0.4453	55	0.4297	65	0.5078	68	0.5313
54	0.4219	63	0.4922	64	0.5000	66	0.5156
63	0.4922	67	0.5234	53	0.4141	55	0.4297
62	0.4844	67	0.5234	54	0.4219	54	0.4219
68	0.5313	69	0.5391	76	0.5938	56	0.4375
60	0.4688	61	0.4766	70	0.5469	61	0.4766
67	0.5234	67	0.5234	69	0.5391	65	0.5078
63	0.4922	66	0.5156	64	0.5000	60	0.4688
59	0.4609	62	0.4844	71	0.5547	65	0.5078
59	0.4609	65	0.5078	60	0.4688	71	0.5547
62	0.4844	64	0.5000	60	0.4688	67	0.5234
70	0.5469	68	0.5313	71	0.5547	63	0.4922
58	0.4531	63	0.4922	53	0.4141	70	0.5469
58	0.4531	61	0.4766	59	0.4609	61	0.4766
67	0.5234	71	0.5547	62	0.4844	63	0.4922
71	0.5547	61	0.4766	65	0.5078	54	0.4219
63	0.4922	57	0.4453	62	0.4844	60	0.4688
64	0.5000	69	0.5391	60	0.4688	64	0.5000
61	0.4766	72	0.5625	61	0.4766	67	0.5234
66	0.5156	60	0.4688	58	0.4531	53	0.4141
52	0.4063	67	0.5234	55	0.4297	66	0.5156
67	0.5234	66	0.5156	58	0.4531	73	0.5703
63	0.4922	67	0.5234	60	0.4688	63	0.4922
65	0.5078	70	0.5469	67	0.5234	64	0.5000
68	0.5313	75	0.5859	50	0.3906	63	0.4922
60	0.4688	64	0.5000	64	0.5000	62	0.4844
71	0.5547	60	0.4688	68	0.5313	70	0.5469
72	0.5625	63	0.4922	64	0.5000	71	0.5547
72	0.5625	61	0.4766	63	0.4922	65	0.5078
58	0.4531	64	0.5000	69	0.5391	55	0.4297
62	0.4844	65	0.5078	68	0.5313	49	0.3828
72	0.5625	54	0.4219	60	0.4688	63	0.4922
58	0.4531	64	0.5000	67	0.5234	61	0.4766
67	0.5234	60	0.4688	58	0.4531	57	0.4453
70	0.5469	66	0.5156	61	0.4766	58	0.4531
63	0.4922	55	0.4297	60	0.4688	61	0.4766
59	0.4609	62	0.4844	62	0.4844	56	0.4375
60	0.4688	63	0.4922	65	0.5078	60	0.4688
53	0.4141	62	0.4844	61	0.4766	63	0.4922
64	0.5000	62	0.4844	64	0.5000	65	0.5078
67	0.5234	69	0.5391	67	0.5234	59	0.4609
59	0.4609	63	0.4922	69	0.5391	66	0.5156
62	0.4844	65	0.5078	59	0.4609	65	0.5078
70	0.5469	74	0.5781	66	0.5156	62	0.4844
73	0.5703	62	0.4844	62	0.4844	61	0.4766
62	0.4844	67	0.5234	56	0.4375	63	0.4922
60	0.4688	60	0.4688	56	0.4375	71	0.5547
Average					0.4926		0.4950

interpreting the correlation coefficient (Mahmoud *et al*., 2013; Ariffin *et al*., 2012; Fahmy *et al*., 2005; Mohammad *et al*., 2009):

- 0 indicates a non-linear relationship
- +1 indicates a perfect positive linear relationship
- -1 indicates a perfect negative linear relationship
- The values between 0 and 0.3 (0 and -0.3) indicate a weak positive (negative) linear relationship
- The values between 0.3 and 0.7 (-0.3 and -0.7) indicate a moderate positive (negative) linear relationship
- The values between 0.7 and 1.0 (-0.7 and -1.0) indicate a strong positive (negative) linear relationship

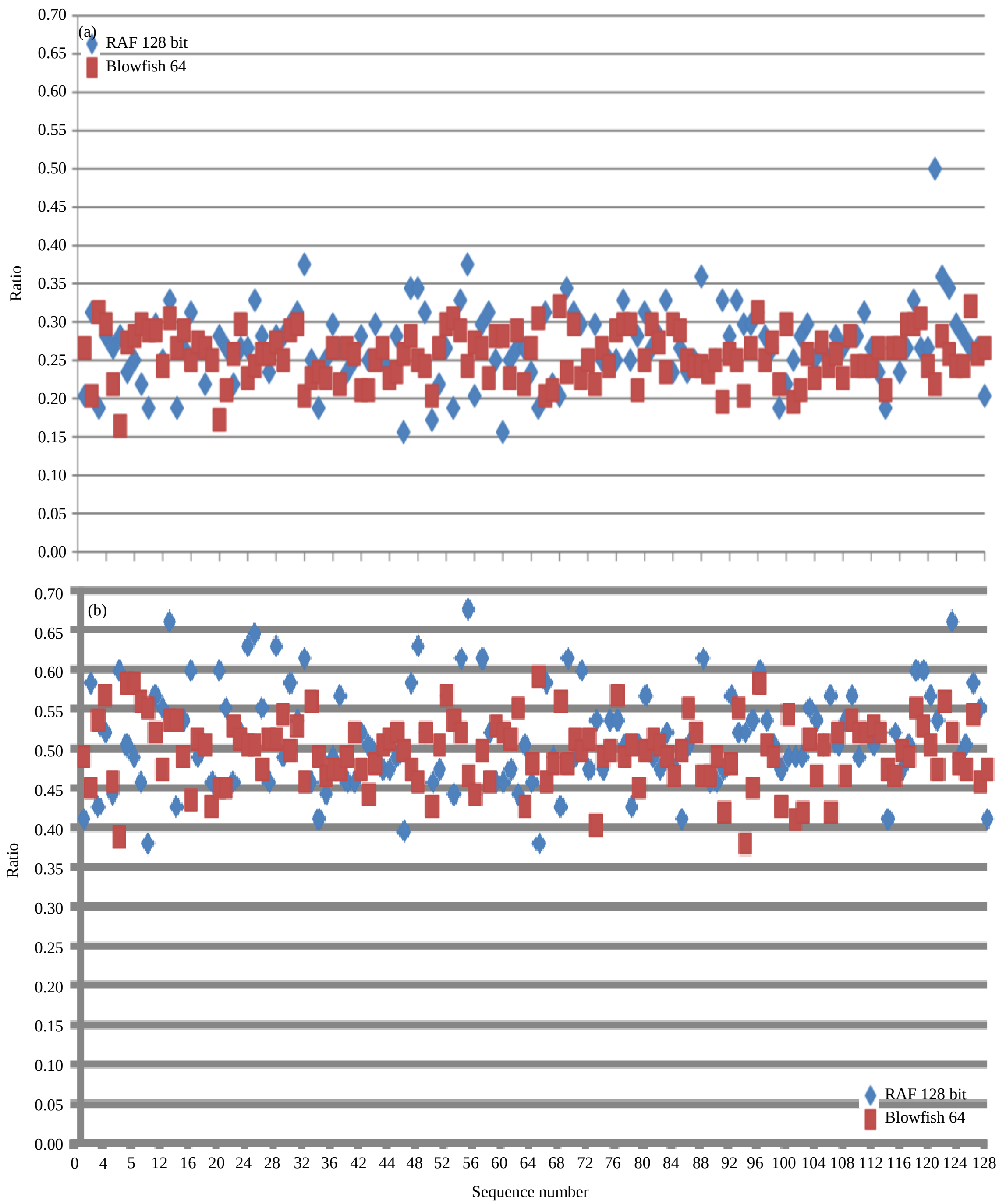

Fig. 1(a-d): Continue

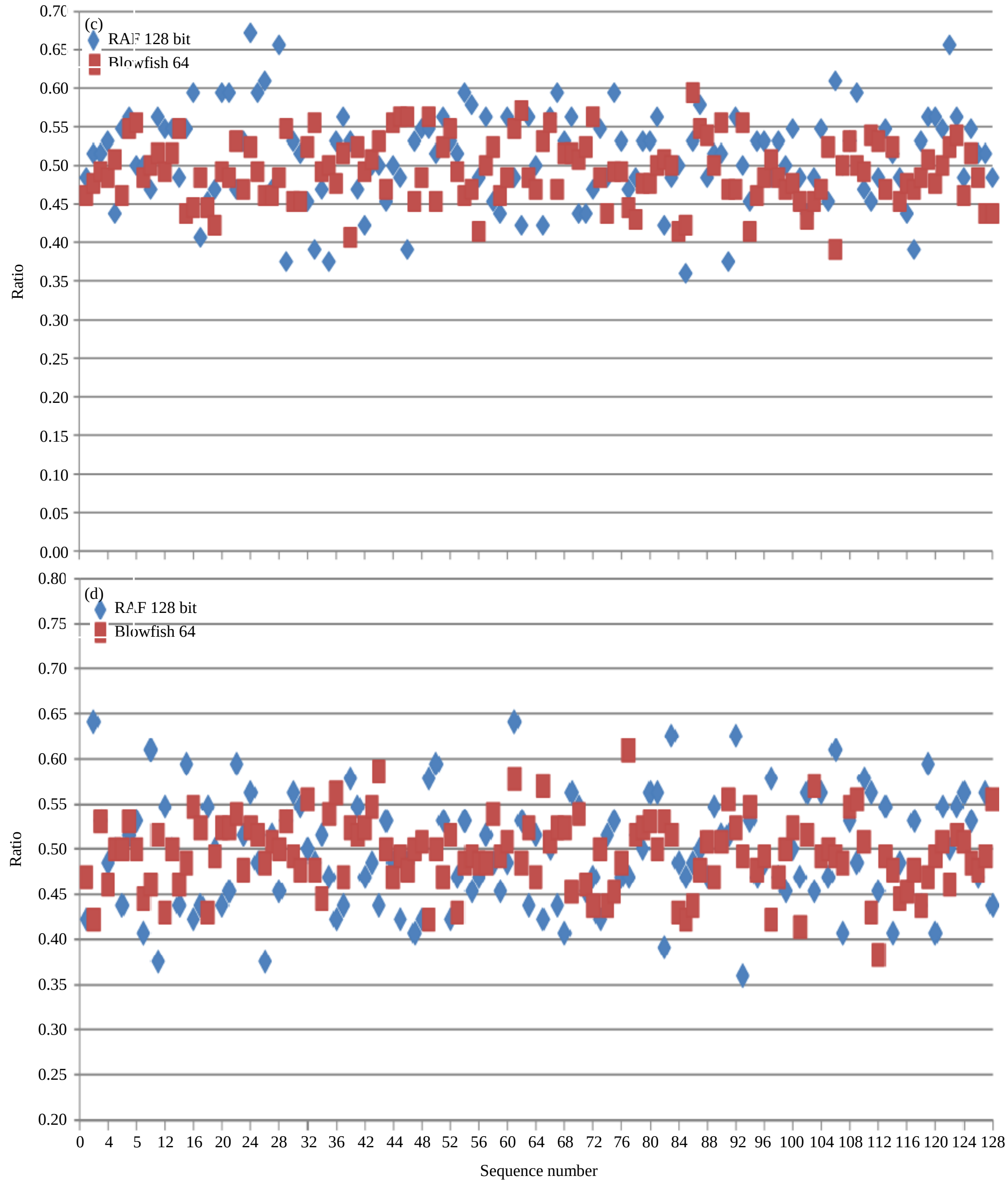

Fig. 1(a-d): Avalanche text of both algorithms for (a) First round, (b) Second round, (c) Third round and (d) last round

Testing data: The data set tested is the same as the data set tested for the avalanche text.

Empirical results and analysis: As presented in Table 3 and 87 correlation coefficient values in the RAF are near zero, thus indicating perfect non-linear relation between plaintext and ciphertext. However, 41 values are greater than 0.1 and less than 0.3 or greater than -0.1 and less than -0.3, thus indicating weak linear positive or negative relation. Meanwhile, 80 values in the BA are near zero, thus indicating non-linear relation between inputs and outputs. One value is -0.3974, thus indicating moderate negative linear relation. However, 47 values are greater than 0.1 and less than 0.3 or greater than -0.1 and less than -0.3, thus indicating weak

Table 3: Values of the correlation coefficient between plaintext and Ciphertext for RAF algorithm

Sequence No.	RAF	Sequence No.	RAF
1	-0.0290	65	-0.0834
2	0.1998	66	0.0373
3	-0.0781	67	-0.0366
4	-0.0297	68	-0.0129
5	-0.0201	69	0.0157
6	0.0315	70	-0.00098
7	-0.0928	71	-0.1805
8	0.0854	72	0.0314
9	-0.0020	73	-0.0628
10	-0.0972	74	-0.0417
11	0.0618	75	0.0821
12	-0.0350	76	0.0507
13	0.1222	77	-0.1266
14	-0.0201	78	0.1513
15	0.1776	79	-0.0612
16	-0.1851	80	-0.0753
17	0.0729	81	0.1034
18	0.0652	82	0.0499
19	-0.0893	83	0.0476
20	0.0573	84	-0.0089
21	0.0639	85	-0.0470
22	0.0166	86	0.1256
23	0.1251	87	-0.1670
24	0.0609	88	-0.1287
25	0.1171	89	0.0315
26	-0.1122	90	-0.0797
27	-0.0262	91	0.1196
28	-0.0171	92	-0.0518
29	-0.0918	93	-0.0127
30	-0.0739	94	-0.0156
31	0.0646	95	-0.0628
32	0.2020	96	-0.0752
33	-0.0800	97	-0.1985
34	-0.0320	98	-0.0320
35	-0.0807	99	-0.0127
36	0.0012	100	0.1780
37	-0.0388	101	-0.2189
38	0.0142	102	-0.0161
39	-0.0929	103	0.0253
40	-0.0313	104	0.1083
41	-0.0306	105	0.1216
42	0.1106	106	0.1408
43	0.0277	107	-0.1034
44	0.0614	108	0.1110
45	0.0809	109	-0.0787
46	0.0688	110	-0.1248
47	0.1381	111	0.0606
48	-0.0029	112	-0.1692
49	0.0156	113	0.0455
50	0.0495	114	-0.0511
51	-0.1491	115	0.1423
52	-0.0320	116	0.000244
53	0.1869	117	0.0807
54	-0.1216	118	-0.1050
55	-0.1216	119	-0.0249
56	0.0285	120	-0.0422
57	0.0573	121	0.0821
58	0.0181	122	-0.0648
59	-0.1083	123	0.0578
60	0.0591	124	0.0825
61	-0.0237	125	0.0784
62	-0.1209	126	0.1002
63	0.1738	127	0.1398
64	0.1588	128	0.1086

positive (negative) linear relationship (Alabaichi *et al*., 2013b). Although both algorithms have good non-linear relations, all results show that the RAF exhibits non-linear relations with better impact than BA. The results of the correlation of both algorithms are illustrated in Fig. 2 and Table 3.

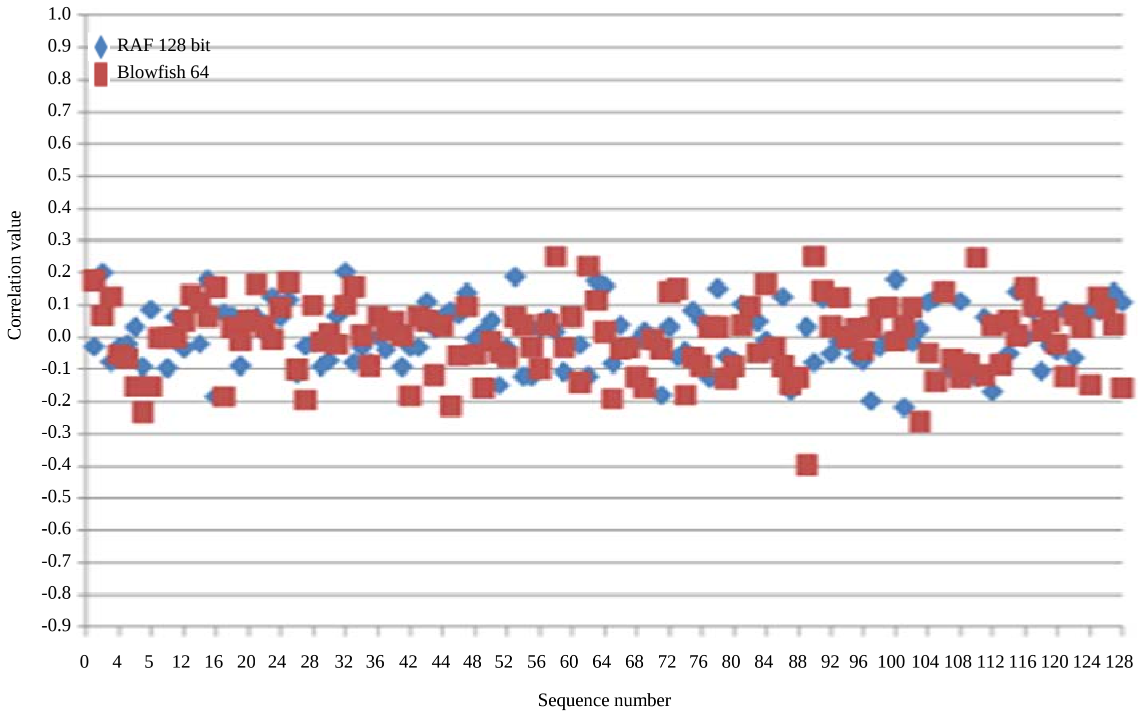

Fig. 2: Results of correlation coefficient of both algorithms

Second phase (security analysis of the dynamic 3D S-BOX): In this phase, we analyze the security of the dynamic 3D S-Box, including its properties such as AVAL, SAC and BIC.

Criteria of the S-Box: AVAL, SAC and are BIC used to guide S-Boxes design, therefore, these criteria are used to evaluate the dynamic 3D S-Box of the RAF.

Avalanche criteria: According to Feistel (1973), AVAL is an important cryptographic property of block ciphers, S-Boxes and SPNs.

In formulating this, an n×n S-Box satisfies AVAL under the condition that for all i = 1, 2,..., n:

$$\frac{1}{2^n}\sum_{j=1}^{n} W\left(a_j^{ei}\right) = \frac{n}{2} \quad (2)$$

Where:

$$w\left(a_j^{ei}\right) = \sum_{\text{all } x\varepsilon\{0,1\}^n} a_j^{ei} \quad (3)$$

where, ei is the unit vector with bit i = 1 and all other bits are equal to 0.

A^{ei} XOR sums are referred to as avalanche vectors. Each vector has n bits or avalanche variables. This condition only occurs when a change in the ith bit in the input string is implemented.

A^{ei} is defined as:

$$A^{ei} = f(X) \oplus f(X \oplus e_i) = [a_1^{ei}\ a_2^{ei} \ldots a_n^{ei}] \quad (4)$$

where, $a_j^{ei} = \{0, 1\}$.

The total change in the jth avalanche variable, a_j^{ei} is computed over the entire input alphabet with size 2^n (note that $0<W(a_j^{ei})<2^n$). Equation 2 is manipulated to define an AVAL parameter, $k_{AVAL}(i)$ as:

$$k_{AVAL(i)} = \frac{1}{n2^n}\sum_{j=1}^{n} W\left(a_j^{ei}\right) = \frac{1}{2} \quad (5)$$

$k_{AVAL}(i)$ which has the values of [0,1] should be interpreted as the probability of change in the overall output bits when only the ith bit in the input string is changed. If $k_{AVAL}(i)$ differs from 1/2 for any i, then it is assumed that the S-Box does not satisfy AVAL. If $k_{AVAL}(i)$ is approximately 1/2 for all is, then the S-Box satisfies AVAL within a small range of error. If approximately 1/2 of the resulting avalanche variables are equal to 1 for all values of i, such that $1<i<m$, then the function has a good avalanche effect (Mar and Latt, 2008; Hussain *et al.*, 2010; Webster and Tavares, 1986; Selcuk and Melek, 2001).

Relative error for avalanche criteria: Vergili and Yucel (2000) concluded that the S-Box can satisfy Eq. 5 for small values of n but for n≥6, satisfying the AVAL criterion is difficult for the S-Box. Therefore, expecting that the criterion given by Eq. 5 will be satisfied within an error range of $\pm e_A$ is logical. This range of error is known as the relative error interval for the AVAL. Therefore, the S-Box satisfies the AVAL within $\pm e_A$, on the condition for all values of i:

$$\frac{1}{2}(1-e_A) \le K_{AVAL(i)} \le \frac{1}{2}(1+e_A) \quad (6)$$

is true. Given an S-Box, the corresponding relative error e_A can be found in Eq. 6 as:

$$e_A = \max_{1 \le i \le n} \left|2k_{AVAL}(i) - 1\right| \quad (7)$$

For a set of S-Boxes with the same size, the maximum relative error is:

$$e_{AVAL} = \max_{\text{Overall S-Boxes}} \{e_A\} \quad (8)$$

Strict avalanche criteria: Webster and Tavares (1986) combined completeness and avalanche properties into the SAC. An S-Box satisfies the SAC if the probability of change in any output bit approximates 1/2 whenever an input bit changes. SAC can be described mathematically as follows:

- The F-function: $\{0, 1\}^n \rightarrow \{0, 1\}^n$ satisfies the SAC for all i, j, ε (1, 2, ..., n). The flipping input bit i changes the output bit j with a probability of exactly 1/2. Thus, an S-Box fulfills the requirements of the SAC if:

$$\frac{1}{2_n} W(a_j^{ei}) = \frac{1}{2_n} \text{ for all i, j} \quad (9)$$

can be modified to define a SAC parameter, $K_{SAC}(i, j)$ as:

$$K_{SAC}(i, j) = \frac{1}{2^n} W(a_j^{ei}) = \frac{1}{2} \text{ for all i, j} \quad (10)$$

K_{SAC} (i, j) can assume the values [0,1] and should be interpreted as the probability of change in the jth output bit when the ith bit in the input string is changed. If $k_{SAC}(i, j)$ is not 1/2 for any (i, j) pair, then the S-Box does not satisfy the SAC. Satisfying Eq. 10 for all values of i and j is unrealistic, therefore, interpreting Eq. 10 within an error interval of $\{-e_S, + e_S\}$ is meaningful. That is, if $k_{SAC}(i, j)$ approximates 1/2 for all (i, j) pairs, then the S-Box satisfies the SAC within a small range of error (Mar and Latt, 2008; Hussain *et al*., 2010; Selcuk and Melek, 2001).

Relative error for the strict avalanche criteria: The SAC is a more specialized form of the AVAL, thus the number of S-Boxes that satisfies the SAC is smaller than the number of S-Boxes that satisfies the AVAL. Moreover, this criterion for a large S-Box size (n≥6) is satisfied with a small error range. Therefore, by modifying Eq. 10, an S-Box satisfies the SAC within $\pm e_A$ for all values of i and j. The following equation is then satisfied:

$$\frac{1}{2}(1-e_S) \le K_{SAC}(i, j) \le \frac{1}{2}(1+e_S) \quad (11)$$

Using Eq. 11 for a given S-Box, the relative error e_S for the SAC is:

$$e_s = \max_{1 \le i,\, j \le n} \left|2K_{SAC}(i, j)\right| - 1 \quad (12)$$

For a set of S-Boxes with the same size, the maximum relative error is:

$$e_{SAC} = \max_{\text{Overall S-Boxes}} \{es\} \quad (13)$$

Bit independence criteria: Webster and Tavares (1986) introduced another property for the S-Box which they named as the BIC. This property is most appropriate for cryptographic transformation in which all the avalanche variables become independent pairs when a given set of avalanche vectors is generated by complementing a single plaintext bit. To measure the degree of independence between a pair of avalanche variables, calculating the correlation coefficient is necessary. The independence of the output bits ensures that any two output bits i and j act "Independently" of each other. Therefore, bits i and j are neither equal to each other significantly more, nor significantly less, than half the time (over all possible input vectors).

The BIC is defined mathematically as follows. A function $f:\{0, 1\}^n \rightarrow \{0, 1\}^n$ satisfies the BIC on the condition for all values of i, j, k, ε {1, 2, ..., n}, with j ≠ k. Inverting input bit i causes output bits j and k to change independently. The correlation coefficient computed between the jth and kth components of the output difference string is known as the avalanche vector A^{ei}. A parameter of bit independence that corresponds to the effect of the ith input bit that change on the jth and kth bits of A^{ei} is defined as:

$$BIC^{ei}(a_j, a_k) = \left|\text{corr}\,(a_j^{ei}, a_k^{ei})\right| \quad (14)$$

Overall, the BIC parameter for the S-Box of the F-function is:

$$BIC(f) = \max,\ BIC^{ei}(a_j, a_k)$$

$$1 \leq i \leq n$$
$$1 \leq j, k \leq n \quad (15)$$
$$j \neq k$$

BIC (f) assumes the values of [0, 1] (Hussain *et al*., 2010; Selcuk and Melek, 2001; Manikandan *et al*., 2012).

Relative error for the bit independence criteria: The relative error for the BIC is slightly different from those of the AVAL and the SAC. This error is presented as follows (Hussain *et al*., 2010; Feistel, 1973):

$$e_{BIC} = BIC\ (f) \quad (16)$$

For a set of S-Boxes with the same size, the maximum relative error is:

$$e_{BIC} = \max \{e\}$$
$$\text{Overall S-Boxes} \quad (17)$$

Testing data: All random 128-bit and 256-bit encryption keys (E_{ks}) as well as the random 128-bit plaintext were generated by BBS.

Empirical results and analysis: Twelve experiments have been conducted on the Dynamic 3D S-Box in the RAF by using three types of E_{ks}: Random, low entropy ones and low entropy zeroes with three properties AVAL, SAC, BIC, thus comprising 12 128-bit E_{ks} in all experiments to examine the effect of entropy of the E_{ks} on the security of the dynamic 3D S-Box in the RAF. The first 10 experiments are conducted with 10 random 128-bit E_{ks}. The remaining two experiments are carried out with a non-random E_k. One experiment is conducted with low entropy ones encryption key and the last experiment is performed with low entropy zeroes encryption key. In summary, the total number of S-Boxes tested in these experiments is 12 dynamic 3D S-Boxes in the RAF.

Empirical results of the avalanch criteria: Table 4, summarizes the values of $k_{AVAL}(i)$ that satisfies Eq. 5. Moreover, the values of k_{AVAL} that correspond to the changed input bits e_i, (i = 1… 8) where e_1 represents the first changed input bit, whereas e_2 represents the second changed input bit. Subsequently, the other parameters follow the same pattern, whereby e_i (i = 3… 8). The results of the first experiment are discussed in this study for a brief. In Table 4, the second column indicates the random encryption keys in hexadecimal, the third column indicates the changed ith input bit, the last column indicates the average change in the output bits when the ith input bit is changed.

The results in Table 4 indicate that the values of $k_{AVAL}(i)$ approximates to half. This means that the dynamic 3D S-Box in RAF does not satisfy the exact AVAL criterion, i.e., these S-Boxes satisfy AVAL only within a range of error. Other experiments have similar results.

Table 5-7, summarize the values of eA, the maximum (Max) and the minimum (Min) values of the k_{AVAL} which correspond to the changed input bits ei where i = 1...8 with ten random 128-bit Eks, non random128-bit Eks (low entropy zeroes and low entropy ones) and random plaintext (a24a52153c3ede6735e0865e8d99bfbc), respectively. Results in Table 5-7 showed that the dynamic 3D S-Box in RAF satisfy AVAL with maximum error values (e_{AVAL}) of 0.0566. Whereas BA satisfies the AVAL maximum error values (e_{AVAL}) of 0.0518 (Alabaichi *et al*., 2013a). In addition, the entropy of E_{ks} is not affected on the AVAL results.

Empirical results of the SAC: Table 8 and summarize the values of k_{SAC} (i, j) which satisfy Eq. 10 in RAF. The values of k_{SAC} (i, j) correspond to the changed input bits e_i, (i = 1… 8) where e_1 represents the first changed input bit, e_2 represents the second changed input bit and subsequently the other parameters e_i (i = 3 … 8).

The results of the first dynamic 3D S-Box from the first experiment are discussed as follows. This experiment includes SAC values with 8-bit input (i) and 8-bit output (j) with the

Table 4: Values of ith avalanche k_{AVAL}(i) for the dynamic 3D S-box in RAF with the first random 128 –bit E_{ks}

No of experiments	Random 128-bit E_k in Hexadecimal	ith Avalanche	Value of ith Avalanche (k_{AVAL}(i))
1	5a22cf8f5c8b190447fe784467b2e538	$k_{AVAL\,(1)}$	0.5068
		$k_{AVAL\,(2)}$	0.5010
		$k_{AVAL\,(3)}$	0.5088
		$k_{AVAL\,(4)}$	0.5088
		$k_{AVAL\,(5)}$	0.5205
		$k_{AVAL\,(6)}$	0.4971
		$k_{AVAL\,(7)}$	0.4834
		$k_{AVAL\,(8)}$	0.5186

Table 5: Values of the e_A, maximum and minimum of K_{AVAL} for the dynamic 3D S-Box with ten random 128- bit E_{ks} in RAF

No. of experiment	Random 128-bit E_{ks} in hexadecimal	e_A	Maximum value of K_{AVAL}	Minimum value of K_{AVAL}
1	5a22cf8f5c8b190447fe784467b2e538	0.0410	0.5205	0.4795
2	6ba36e2fe0a4c7840de1537e13c20ec	0.0488	0.5244	0.4756
3	ab4c050208e34cccbae675df094ae619	0.0321	0.51605	0.48395
4	d48e31d6dec336ff5f34c98bf8ff088d	0.0356	0.5178	0.4822
5	92323d1aafe9e47ee94ba07dc68bdbd	0.0391	0.5195	0.4805
6	7458aa85d6c3c9ef77d07170bba24fbb	0.0566	0.5283	0.4717
7	05605ab55f5cf2eca8781dac2e1bed6b	0.0352	0.5176	0.4824
8	7223 49c1b517cc13292c0b56108c46	0.0261	0.5131	0.4869
9	c49df5e51f2b99736adba9132533896b	0.0366	0.5183	0.4817
10	cc38bd5bacd5eff2f32cfa505193c2bf	0.0488	0.5244	0.4756

Table 6: Values e_A, maximum and minimum of K_{AVAL} for the dynamic 3D S-Box with low entropy ones encryption key in RAF algorithm

No. of experiment	Low entropy 128-bit encryption key in hexadecimals	e_A	Maximum value of K_{AVAL}	Minimum value of K_{AVAL}
11	11111111111111111111111111111111	0. 0264	0.5132	0.4868

Table 7: Values e_A, maximum and minimum of K_{AVAL} for the dynamic 3D S-Box with low entropy zeroes encryption key in RAF algorithm

No. of experiment	low entropy 128-bit encryption key in hexadecimals	e_A	Maximum value of K_{AVAL}	Minimum value of K_{AVAL}
12	00000000000000000000000000000000	0.0229	0.5115	0.4885

Table 8: Values of Strict Avalanche Criterion (SAC) of dynamic 3D S-box in RAF with 8 bits input (i) and 8 bits output (j)

$K_{SAC(1,j=1..8)}$	0.5078	0.5547	0.4375	0.5156	0.5625	0.4922	0.5	0.4844
$K_{SAC(2,j=1..8)}$	0.6016	0.4297	0.5	0.5313	0.5156	0.4922	0.4688	0.4688
$K_{SAC(3,j=1..8)}$	0.5703	0.4609	0.4844	0.5313	0.5	0.4922	0.4844	0.5469
$K_{SAC(4,j=1..8)}$	0.5078	0.5391	0.4375	0.5313	0.5781	0.5234	0.4688	0.4844
$K_{SAC(5,j=1..8)}$	0.4922	0.4766	0.5781	0.5	0.5	0.5391	0.5625	0.5156
$K_{SAC(6,j=1..8)}$	0.5547	0.4766	0.5625	0.4844	0.3906	0.4766	0.4688	0.5625
$K_{SAC(7,j=1..8)}$	0.4766	0.4453	0.5	0.5313	0.4375	0.4922	0.4688	0.5156
$K_{SAC(8,j=1..8)}$	0.5078	0.5078	0.4063	0.6406	0.5313	0.5078	0.5625	0.4844

Table 9: Values of e_S, maximum and minimum of K_{SAC} for the dynamic 3D S-Box with ten random 128-bit E_{ks} in RAF

No. of experiment	e_S	Maximum value of K_{SAC}	Minimum value of K_{SAC}
1	0.2813	0.6406	0.3594
2	0.2344	0.6172	0.3828
3	0.2031	0.6016	0.3984
4	0.2656	0.6328	0.3672
5	0.2344	0.6172	0.3828
6	0.2656	0.6328	0.3672
7	0.2031	0.6016	0.3984
8	0.1875	0.5938	0.4063
9	0.2656	0.6328	0.3672
10	0.2344	0.6172	0.3828

Table 10: Values of the e_S, maximum and minimum of K_{SAC} for dynamic 3D S-Box with low entropy ones encryption key in RAF algorithm

No. of experiment	e_S	Maximum value of K_{SAC}	Minimum value of K_{SAC}
11	0.1875	0.5938	0.4063

Table 11: Values of the e_S, maximum & minimum of K_{SAC} for the dynamic 3D S-Boxes with low entropy zeroes encryption key in RAF

No of experiment	e_S	Maximum value of K_{SAC}	Minimum value of K_{SAC}
12	0.2031	0.6016	0.3984

first random encryption key. The first row indicates the average change in every output bit when the first input bit is changed, the second row shows the average change in every output bit when the second input bit is changed and so on until the eighth row.

Table 8 and show that the values of K_{SAC} (i, j) random E_{ks} are approximate to one half. This means that the dynamic 3D S-Box in RAF does not exactly satisfy SAC, i.e., the dynamic 3D S-Box in RAF algorithm satisfy SAC within an error range.

Table 9-11 and summarize the values of e_{SAC}, the maximum (Max) and the minimum (Min) values of the K_{SAC} which correspond to the changed input bits e_i where i = 1...8 with ten random 128-bit E_{ks}, non random128-bit E_{ks} (low entropy zeroes and low entropy ones) and random plaintext (a24a52153c3ede6735e0865e8d99bfbc), respectively.

The dynamic 3D S-Box in RAF satisfies SAC with a maximum error value (eSAC) of 0.2813 as shows in Table 9-11. In addition, the entropy of E_{ks} bears no effect on the SAC results. Whereas BA satisfies the SAC with a maximum error values (e_{SAC}) of 0.3594 (Alabaichi *et al.*, 2013a). In addition, the entropy of E_{ks} is not affected by the SAC.

Empirical results of the BIC: Table 12 summarizes the values of BIC (i) which satisfy Equations 14 and 15 . The values of BIC (i) which correspond to the changed input bits e_i (i = 1 ... 8) with ten random 128-bit E_{ks}, non random128-bit E_{ks} (low entropy zeroes and low entropy ones) and random plaintext (a24a52153c3ede6735e0865e8d99bfbc), respectively. The second column indicates to BIC when ith input bit is changed.

From the results in Table 12-14 and it can be inferred that the dynamic 3D S-Box in RAF satisfy BIC with a maximum error value (eBIC) of 0.2698. In addition, the entropy of E_{ks} did not affect the BIC results. Whereas BA satisfies the BIC with maximum error value (e_{BIC}) of 0.4725 (Alabaichi *et al.*, 2013a). In addition, the entropy of E_{ks} was not affected by the BIC results.

Finally, based on all the aforementioned results, a conclusion can be drawn that the dynamic 3D S-Box in RAF satisfy the AVAL, the SAC and the BIC with maximum error values of 0.0566, 0.2813 and 0.2698, respectively. Meanwhile, the S-Boxes in the BA satisfy the AVAL, the SAC and the BIC with maximum error values of 0.0518, 0.3594 and 0.4725, respectively. The dynamic 3D S-Box in the RAF and the S-Boxes in the BA satisfy the AVAL approximate the same. Meanwhile, the SAC and the BIC are more effectively

Table 12: Values of the BIC for dynamic 3D S-Boxes in RAF with ten random 128-bit E_{ks}

No. of experiment	BIC
1	0.2698
2	0.2690
3	0.2197
4	0.2646
5	0.2672
6	0.2401
7	0.2694
8	0.2437
9	0.2809
10	0.2437

Table 13: Values of BIC for dynamic 3D S-Box with low entropy ones encryption key in RAF algorithm

No. of experiment	BIC
11	0.2595

Table 14: Values of BIC for dynamic 3D S-Box with low entropy encryption key in RAF algorithm

No. of experiment	BIC
12	0.2649

Table 15: Values of e_{AVAL}, e_{SAC} and e_{BIC} for S-Boxes in RAF and BA algorithms

S-box and Algorithm	e_{AVAL}	e_{SAC}	e_{BIC}
Dynamic 3D S-BOX in RAF	0.0566	0.2813	0.2698
S-boxes in BA	0.0518	0.3594	0.4725

satisfied by the dynamic 3D S-Box in RAF than the S-Boxes in BA. This means RAF is more secure than BA. In addition, the entropy of the keys has no effect on the security of the S-Boxes in both algorithms.

Table 15 summarizes e_{AVAL}, e_{SAC} and e_{BIC} for the S-Boxes in the RAF and the BA.

CONCLUSION

Several conclusions are drawn from this research and the most significant ones are discussed as follows.

Based on the results of the avalanche text test, the avalanche texts of the RAF are 0.4912, 0.4926 and 0.4950 in the second, third and last rounds, respectively, whereas the avalanche texts of the BA are 0.5110, 0.5098, 0.4972 in the second, third and last rounds, respectively. In addition, the avalanche text of the RAF approximates the same avalanche text in the BA in these rounds. However, the avalanche texts of the first round of the RAF and the BA are 0.2690 and 0.2555, respectively. The two algorithms provide good avalanche texts from the second round and their results of the correlation coefficient exhibit good non-linear relations. Based on the evaluation of the S-Boxes in the RAF and the BA, the 3D S-Box in the RAF is more secure than the S-Boxes in the BA because the 3D S-Box in RAF satisfies the AVAL, the SAC and the BIC with maximum error values of 0.0566, 0.2813 and 0.2698, respectively. By contrast, the S-Boxes in BA satisfy the AVAL, the SAC and the BIC with maximum error values of 0.0518, 0.3594 and 0.4725, respectively. The dynamic 3D S-Box in the RAF and the S-Boxes in the BA exhibit approximately the same result in satisfying the AVAL. Meanwhile, the dynamic 3D S-Box in the RAF satisfies the SAC and the BIC more effectively than the S-Boxes in the BA. By contrast, the entropy of the keys does not affect the security of the S-Boxes in both algorithms.

Thus, the dynamic permutation box and the dynamic 3D S-Box when combined serve as an effective approach that strengthens the RAF algorithm.

Following the present study, future work can be conducted on the following topics:

- Analyzing the performance of the RAF based on following factors: speed, throughput and power consumption. Afterward, the performance of the RAF can be compared with other algorithms of various platforms
- Implementing and evaluating the characteristic criteria of the RAF, including flexibility, hardware, software suitability and algorithm simplicity

REFERENCES

Adams, C. and S. Tavares, 1990. The structured design of cryptographically good S-boxes. J. Cryptol., 3: 27-41.

Agrawal, H. and M. Sharma, 2010. Implementation and analysis of various symmetric cryptosystems. Indian J. Sci. Technol., 3: 1173-1176.

Alabaichi, A., R. Mahmod and F. Ahmad, 2013a. Analysis of some security criteria for S-boxes in blowfish algorithm. Int. J. Digital Content Technol. Applic., 7: 8-20.

Alabaichi, A., R. Mahmod and F. Ahmad, 2013b. Security analysis of blowfish algorithm. Proceding of the 2nd International Conference on Informatics and Applications, September 23-25, 2013, Lodz, Poland, pp: 12-18.

Alabaichi, A., R. Mahmod and F. Ahmad, 2014a. A cylindrical coordinate system with dynamic permutation table for blowfish algorithm. Int. J. Soft Comput., 9: 318-332.

Alabaichi, A., R. Mahmod and F. Ahmad, 2014b. A dynamic 3D S-box based on cylindrical coordinate system for blowfish algorithm. Proceedings of the 3rd International Conference on Computer Science and Computational Mathematics, May 8-9, 2014, Langkawi, Malaysia, pp: 273-288.

Ariffin, S., 2012. A human immune system inspired byte permutation of block cipher. Ph.D. Thesis, Universiti Putara Malaysia, Malaysia.

Ariffin, S., R. Mahmod, A. Jaafar, M. Rezal and K. Ariffin, 2012. An Immune System-Inspired Byte Permutation Function to Improve Confusion Performance of Round Transformation in Symmetric Encryption Scheme. In: Computer Science and its Applications: CSA 2012, Yeo, S.S., Y. Pan, Y.S. Lee and H.B. Chang (Eds.). Springer Science and Business Media, Dordrecht, Netherland, ISBN: 9789400756991, pp: 339-351.

Castro, J.C.H., J.M. Sierra, A. Seznec, A. Izquierdo and A. Ribagorda, 2005. The strict avalanche criterion randomness test. Math. Comput. Simul., 68: 1-7.

Dawson, E., H. Gustafson and A.N. Pettitt, 1992. Strict key avalanche criterion. Aust. J. Combinator., 6: 147-153.

Doganaksoy, A., B. Ege, O. Kocak and F. Sulak, 2010. Cryptographic randomness testing of block Ciphers and Hash functions. Cryptology ePrint Archive: Report 2010/564, pp: 1-12. https://eprint.iacr.org/2010/564.pdf.

Fahmy, A., M. Shaarawy, K. El-Hadad, G. Salama and K. Hassanain, 2005. A proposal for a key-dependent AES. Proceedings of the 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, March 27-31, 2005, Tunisia, pp: 1-7.

Feistel, H., 1973. Cryptography and computer privacy. Sci. Am., 228: 15-23.

Hussain, I., T. Shah, M. Afzal and H. Mahmood, 2010. Comparative analysis of S-boxes based on graphical SAC. Int. J. Comput. Applic., 2: 5-8.

Juremi, J., R. Mahmod and S. Sulaiman, 2012. A proposal for improving AES S-box with rotation and key-dependent. Proceedings of the International Conference on Cyber Security, Cyber Warfare and Digital Forensic, June 26-28, 2012, Kuala Lumpur, Malaysia, pp: 38-42.

Mahmoud, E.M., A.A. El Hafez, T.A. Elgarf and A. Zekry, 2013. Dynamic AES-128 with key-dependent S-box. Int. J. Eng. Res. Applic., 3: 1662-1670.

Manikandan, G., N. Sairam and M. Kamarasan, 2012. A new approach for improving data security using iterative blowfish algorithm. Res. J. Applied Sci., 4: 603-607.

Mar, P.P. and K.M. Latt, 2008. New analysis methods on strict avalanche criterion of S-boxes. World Acad. Sci. Eng. Technol., 2: 111-115.

Mohammad, F.Y., A.E. Rohiem and A.D. Elbayoumy, 2009. A novel S-box of AES algorithm using variable mapping technique. Proceedings of the 13th International Conference on Aerospace Sciences and Aviation Technology, May 26-28, 2009, Kobry Elkobbah, Cairo, Egypt, pp: 1-10.

Mohan, H.S. and A.R. Reddy, 2011. Performance analysis of AES and MARS encryption algorithms. Int. J. Comput. Sci. Issues, 8: 363-368.

Ramanujam, S. and M. Karuppiah, 2011. Designing an algorithm with high avalanche effect. Int. J. Comput. Sci. Network Secur., 11: 106-111.

Selcuk, K. and Y. Melek, 2001. On Some Cryptographic Properties of Rijndael. In: Information Assurance in Computer Networks: Methods, Models and Architectures for Network Security, Gorodetski, V.I., V.A. Skormin and L.J. Popyack (Eds.). Springer-Verlag, Berlin, Germany, ISBN: 9783540451167, pp: 300-311.

Sulaiman, S., Z. Muda and J. Juremi, 2012. The new approach of Rijndael key schedule. Proceedings of the International Conference on Cyber Security, Cyber Warfare and Digital Forensic, June 26-28, 2012, Kuala Lumpur, Malaysia, pp: 23-27.

Vergili, I. and M. Yucel, 2000. On satisfaction of some security criteria for randomly chosen S-boxes. Proceedings of the 20th Biennial Symposium on Communications, May 28-31, 2000, Kingston, Ontario, Canada, pp: 64-68.

Webster, A. and S. Tavares, 1986. On the Design of S-Boxes. In: Advances in Cryptology-CRYPTO'85 Proceedings, Williams, H.C. (Ed.). Springer-Verlag, Berlin, Germany, ISBN: 9780387164632, pp: 523-534.