Evaluation of A dynamic 3D S-Box based on Cylindrical Coordinate System for Blowfish Algorithm

Ashwak ALabaichi[1,2]

[1]Department of computer science, Faculty of Sciences, Karbala University, Karbala, Iraq
[2]Information Technology Department, University Utara Malaysia, Kedah, 06010, Sintok, Malaysia
e-mail: ashwakalabaichi2007@yahoo.com

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. We proposed RAF algorithm and analyzed the randomness of the RAF output in earlier papers 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). In this paper, 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 (R2012a, Mathworks) is used to implement the properties (AVAL, SAC, and BIC), as well as the avalanche text and the correlation coefficient.
[Ashwak ALabaichi. **Evaluation of A dynamic 3D S-Box based on Cylindrical Coordinate System for Blowfish Algorithm.** *Life Sci J* 2018;15(10):72-85]. ISSN: 1097-8135 (Print) / ISSN: 2372-613X (Online). http://www.lifesciencesite.com. 9. doi:10.7537/marslsj151018.09.

Keywords: S-Box criteria, avalanche text, correlation coefficient.

1. 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 (Ahmed, n.d.).

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), (Isil, Yücel, 2000), (Isil, Yücel, 2001).

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 paper in the first phase attempts to 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 et al., 2013a). While in the second phase attempts to analyze the avalanche text and correlation coefficient in RAF after which the results are compared with the results of Blowfish's output in (Alabaichi et al., 2013b).

This paper is organized as follows. Section 2 provides a detailed explanation of the security analysis of the RAF and the dynamic 3D S-Box. Section 3 provides a conclusion for the results of this paper. Section 4 discusses future directions for this paper.

2. 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.

2.1 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.

2.1.1 The 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 text avalanche is used to evaluate the avalanche effect of the RAF and the BA in this study. A block cipher satisfies the text avalanche 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

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

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), (Ali et al., 2010), (Himani and Sharma, 2010), (Mohan and Reddy, 2011), (Ramanujam and Karuppiah, 2011).

2.1.1.1 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.

2.1.1.1.1 Empirical Results And Analysis

Tables 1 and table 2, Appendix A, 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 Tables 1 and table 2, Appendix A, 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 Figuress.1 to 4, Appendix A.

2.1.2 The 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 interpreting the correlation coefficient (Mahmoud et al., 2013), (Ariffin, 2012), (Fahmy, 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.

2.1.2.1 Testing Data

The data set tested is the same as the data set tested for the avalanche text in Section 2.1.1.1.

2.1.2.1.1 Empirical Results And Analysis

As presented in Table 3, Appendix A, 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 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 Figure 5, Appendix A.

2.2 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.

2.2.1 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.

2.2.1.1 Avalanche Criteria

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

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

$$\frac{1}{2^n}\sum_{j=1}^{n} W(\alpha_j^{ei}) = \frac{n}{2}, \qquad (2)$$

where

$$W(\alpha_j^{ei}) = \sum_{all\ X \in \{0,1\}^n} \alpha_j^{ei}, \qquad (3)$$

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:

$$A^{ei} = f(\mathbf{X}) \oplus f(\mathbf{X} \oplus e_i) = [\alpha_1^{ei}\ \alpha_2^{ei} \dots \alpha_n^{ei}], \qquad (4)$$

where $\alpha_j^{ei} \in \{0, 1\}$.

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

$$k_{AVAL(i)} = \frac{1}{n2^n}\sum_{j=1}^{n} W(\alpha_j^{ei}) = \frac{1}{2}. \qquad (5)$$

$k_{AVAL}(i)$, 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), (Isil and Yücel, 2000), (Isil and Yücel, 2001), (Webster and Tavares, 1986), (Selçuk and Yücel, 2001).

2.2.1.1.1 Relative Error For Avalanche Criteria

Isil and Yücel (2000) concluded that the S-Box can satisfy Eq. (5) for small values of n, but for $n \geq 6$, 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 $\pm \in_A$ is logical. This range of error is known as the relative error interval for the AVAL. Therefore, the S-Box satisfies the AVAL within $\pm \in_A$, on the condition for all values of i.

$$\frac{1}{2}(1 - \in_A) \leq K_{AVAL(i)} \leq \frac{1}{2}(1 + \in_A) \qquad (6)$$

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

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

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

$$\epsilon_{AVAL} = \max_{\text{overall S-Boxes}} \{\epsilon_A\} . \quad (8)$$

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

$$\frac{1}{2^n} w\left(a_j^{ei}\right) = \frac{1}{2^n} \text{ for all } i, j \quad (9)$$

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

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

for all i, j.

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 $\{-\epsilon_S, +\epsilon_S\}$ 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), (Isil and Yücel, 2000), (Isil and Yücel (2001), (Selçuk and Yücel, 2001).

2.2.1.2.1 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 $\pm\epsilon_A$ for all values of i and j. The following equation is then satisfied:

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

Using Eq. (11) for a given S-box, the relative error ϵS for the SAC is:

$$\epsilon_S = \max_{1 \le i, j \le n} |2k_{SAC}(i, j) - 1| . \quad (12)$$

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

$$\epsilon_{SAC} = \max_{\text{Overall S-Boxes}} \{\epsilon_S\} . \quad (13)$$

2.2.1.2 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 $i, j, k \in \{1, 2,\ldots, n\}$, 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

$$BIC^{e_i}(a_j, a_k) = |corr(a_j^{ei}, a_k^{e_i})| . \quad (14)$$

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

$$BIC(f) = \max_{\substack{1 \le i \le n, \\ 1 \le j, k \le n, \\ j \ne k}} BIC^{e_i}(a_j, a_k), \quad (15)$$

BIC (f) assumes the values of [0, 1] (Isil and Yücel, 2000), (Isil and Yücel, 2001), (Selçuk and Yücel, 2001), (Manikandan et al., 2012).

2.2.1.3.1 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 (Isil and Yücel, 2000), (Isil and Yücel, 2001), (Horst, 1973):

ϵ_{BIC} = BIC (*f*). (16)

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

$\epsilon_{BIC=\max}$ [e]. (17)

Overall S-Boxes

2.2.2 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.

2.2.3 Empirical Results And Analysis

12 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.

2.2.3.1 Empirical Results Of The Avalanch Criteria

Table 4, Appendix B, 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 paper for a brief. In Table 4, Appendix B, the second column indicates the random encryption keys in hexadecimal; the third column indicates the changed *i*th input bit; the last column indicates the average change in the output bits when the *i*th 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.

Tables 5 to 7, Appendix B, summarize the values of ϵA, 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 Tables 5 to 7 show that the dynamic 3D S-Box in RAF satisfy AVAL with maximum error values (ϵ_{AVAL}) of 0.0566. Whereas BA satisfies the AVAL maximum error values (ϵ_{AVAL}) of 0.0518 (Alabaichi et al., 2013a) In addition, the entropy of E_{ks} is not affected on the AVAL results.

2.2.3.2 Empirical Results Of The SAC

Table 8, Appendix B, summarize the values of k_{SAC} *(i, j)* which satisfy Equation (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 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, Appendix B, 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.

Tables 9 to 11, Appendix B summarize the values of ϵ_{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 (ϵSAC) of 0.2813 as shows in Tables 9 to 11, Appendix B. In addition, the entropy of E_{ks} bears no effect on the SAC results. Whereas BA satisfies the SAC with a maximum error values (ϵ_{SAC}) of 0.3594 [9]. In addition, the entropy of E_{ks} is not affected by the SAC.

2.2.3.3 Empirical Results Of The BIC

Table 12, Appendix B, 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 Tables 12 to 14, Appendix B, it can be inferred that the dynamic 3D S-Box in RAF

satisfy BIC with a maximum error value (ϵBIC) 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 (ϵ_{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 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 Appendix B, summarizes ϵ_{AVAL}, ϵ_{SAC}, and ϵ_{BIC} for the S-Boxes in the RAF and the BA.

3. 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.

4. Future work

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.

Appendix A

Table 1. Summarize the values of the avalanche text for RAF algorithm in the first and second rounds

No. of Seq.	Different bits number (RAF) Round 1	Ratio (RAF) Round 1	Different bits number (RAF) Round 2	Ratio (RAF) Round 2	No. of Seq.	Different bits number (RAF) Round 1	Ratio (RAF) Round 1	Different bits number (RAF) Round 2
1	34	0.2656	62	0.4844	65	39	0.3047	75
2	26	0.2031	57	0.4453	66	26	0.2031	58
3	40	0.3125	68	0.5313	67	27	0.2109	61
4	38	0.2969	72	0.5625	68	41	0.3203	71
5	28	0.2188	58	0.4531	69	30	0.2344	61
6	21	0.1641	49	0.3828	70	38	0.2969	65
7	35	0.2734	74	0.5781	71	29	0.2266	63
8	36	0.2813	74	0.5781	72	32	0.2500	65
9	38	0.2969	71	0.5547	73	28	0.2188	51
10	37	0.2891	70	0.5469	74	34	0.2656	62
11	37	0.2891	66	0.5156	75	31	0.2422	63

12	31	0.2422	60	0.4688	76	37	0.2891	72
13	39	0.3047	68	0.5313	77	38	0.2969	62
14	34	0.2656	68	0.5313	78	38	0.2969	64
15	37	0.2891	62	0.4844	79	27	0.2109	57
16	32	0.2500	55	0.4297	80	32	0.2500	63
17	35	0.2734	65	0.5078	81	38	0.2969	65
18	34	0.2656	64	0.5000	82	35	0.2734	64
19	32	0.2500	54	0.4219	83	30	0.2344	62
20	22	0.1719	57	0.4453	84	38	0.2969	59
21	27	0.2109	57	0.4453	85	37	0.2891	63
22	33	0.2578	67	0.5234	86	32	0.2500	70
23	38	0.2969	65	0.5078	87	31	0.2422	66
24	29	0.2266	64	0.5000	88	31	0.2422	59
25	31	0.2422	64	0.5000	89	30	0.2344	59
26	33	0.2578	60	0.4688	90	32	0.2500	62
27	33	0.2578	65	0.5078	91	25	0.1953	53
28	35	0.2734	65	0.5078	92	33	0.2578	61
29	32	0.2500	69	0.5391	93	32	0.2500	70
30	37	0.2891	63	0.4922	94	26	0.2031	48
31	38	0.2969	67	0.5234	95	34	0.2656	57
32	26	0.2031	58	0.4531	96	40	0.3125	74
33	29	0.2266	71	0.5547	97	32	0.2500	64
34	30	0.2344	62	0.4844	98	35	0.2734	62
35	29	0.2266	59	0.4609	99	28	0.2188	54
36	34	0.2656	60	0.4688	100	38	0.2969	69
37	28	0.2188	60	0.4688	101	25	0.1953	52
38	34	0.2656	62	0.4844	102	27	0.2109	53
39	33	0.2578	66	0.5156	103	33	0.2578	65
40	27	0.2109	60	0.4688	104	29	0.2266	59
41	27	0.2109	56	0.4375	105	35	0.2734	64
42	32	0.2500	61	0.4766	106	31	0.2422	53
43	34	0.2656	64	0.5000	107	33	0.2578	66
44	29	0.2266	65	0.5078	108	29	0.2266	59
45	30	0.2344	66	0.5156	109	36	0.2813	68
46	33	0.2578	63	0.4922	110	31	0.2422	66
47	36	0.2813	60	0.4688	111	31	0.2422	66
48	32	0.2500	58	0.4531	112	31	0.2422	67
49	31	0.2422	66	0.5156	113	34	0.2656	66
50	26	0.2031	54	0.4219	114	27	0.2109	60
51	34	0.2656	64	0.5000	115	34	0.2656	59
52	38	0.2969	72	0.5625	116	34	0.2656	63
53	39	0.3047	68	0.5313	117	38	0.2969	62
54	37	0.2891	66	0.5156	118	38	0.2969	70
55	31	0.2422	59	0.4609	119	39	0.3047	67
56	35	0.2734	56	0.4375	120	31	0.2422	64
57	34	0.2656	63	0.4922	121	28	0.2188	60
58	29	0.2266	58	0.4531	122	36	0.2813	71
59	36	0.2813	67	0.5234	123	33	0.2578	66
60	36	0.2813	66	0.5156	124	31	0.2422	61
61	29	0.2266	65	0.5078	125	31	0.2422	60
62	37	0.2891	70	0.5469	126	41	0.3203	69
63	28	0.2188	54	0.4219	127	33	0.2578	58
64	34	0.2656	61	0.4766	128	34	0.2656	60
Average							0.2555	

Table 2. Summarize the values of the avalanche text for RA algorithm in the third and last rounds

No. of Seq.	Different bits number (RAF) Round 3	Ratio (RAF) Round 3	Different bits number (RAF) Last Round	Ratio (RAF) Last Round	No. of Seq.	Different bits number (RAF) Round 3	Ratio (RAF) Round 3	Different bits number (RAF) Last Round
1	59	0.4609	60	0.4688	65	68	0.5313	73
2	61	0.4766	54	0.4219	66	71	0.5547	65
3	63	0.4922	68	0.5313	67	60	0.4688	67
4	62	0.4844	59	0.4609	68	66	0.5156	67
5	65	0.5078	64	0.5000	69	66	0.5156	58
6	59	0.4609	64	0.5000	70	65	0.5078	69
7	70	0.5469	68	0.5313	71	67	0.5234	59
8	71	0.5547	64	0.5000	72	72	0.5625	56
9	62	0.4844	57	0.4453	73	62	0.4844	64
10	64	0.5000	59	0.4609	74	56	0.4375	56
11	66	0.5156	66	0.5156	75	63	0.4922	58
12	63	0.4922	55	0.4297	76	63	0.4922	62
13	66	0.5156	64	0.5000	77	57	0.4453	78
14	70	0.5469	59	0.4609	78	55	0.4297	66
15	56	0.4375	62	0.4844	79	61	0.4766	67
16	57	0.4453	70	0.5469	80	61	0.4766	68
17	62	0.4844	67	0.5234	81	64	0.5000	64
18	57	0.4453	55	0.4297	82	65	0.5078	68
19	54	0.4219	63	0.4922	83	64	0.5000	66
20	63	0.4922	67	0.5234	84	53	0.4141	55
21	62	0.4844	67	0.5234	85	54	0.4219	54
22	68	0.5313	69	0.5391	86	76	0.5938	56
23	60	0.4688	61	0.4766	87	70	0.5469	61
24	67	0.5234	67	0.5234	88	69	0.5391	65
25	63	0.4922	66	0.5156	89	64	0.5000	60
26	59	0.4609	62	0.4844	90	71	0.5547	65
27	59	0.4609	65	0.5078	91	60	0.4688	71
28	62	0.4844	64	0.5000	92	60	0.4688	67
29	70	0.5469	68	0.5313	93	71	0.5547	63
30	58	0.4531	63	0.4922	94	53	0.4141	70
31	58	0.4531	61	0.4766	95	59	0.4609	61
32	67	0.5234	71	0.5547	96	62	0.4844	63
33	71	0.5547	61	0.4766	97	65	0.5078	54
34	63	0.4922	57	0.4453	98	62	0.4844	60
35	64	0.5000	69	0.5391	99	60	0.4688	64
36	61	0.4766	72	0.5625	100	61	0.4766	67
37	66	0.5156	60	0.4688	101	58	0.4531	53
38	52	0.4063	67	0.5234	102	55	0.4297	66
39	67	0.5234	66	0.5156	103	58	0.4531	73
40	63	0.4922	67	0.5234	104	60	0.4688	63
41	65	0.5078	70	0.5469	105	67	0.5234	64
42	68	0.5313	75	0.5859	106	50	0.3906	63
43	60	0.4688	64	0.5000	107	64	0.5000	62
44	71	0.5547	60	0.4688	108	68	0.5313	70
45	72	0.5625	63	0.4922	109	64	0.5000	71
46	72	0.5625	61	0.4766	110	63	0.4922	65
47	58	0.4531	64	0.5000	111	69	0.5391	55
48	62	0.4844	65	0.5078	112	68	0.5313	49

49	72	0.5625	54	0.4219	113	60	0.4688	63
50	58	0.4531	64	0.5000	114	67	0.5234	61
51	67	0.5234	60	0.4688	115	58	0.4531	57
52	70	0.5469	66	0.5156	116	61	0.4766	58
53	63	0.4922	55	0.4297	117	60	0.4688	61
54	59	0.4609	62	0.4844	118	62	0.4844	56
55	60	0.4688	63	0.4922	119	65	0.5078	60
56	53	0.4141	62	0.4844	120	61	0.4766	63
57	64	0.5000	62	0.4844	121	64	0.5000	65
58	67	0.5234	69	0.5391	122	67	0.5234	59
59	59	0.4609	63	0.4922	123	69	0.5391	66
60	62	0.4844	65	0.5078	124	59	0.4609	65
61	70	0.5469	74	0.5781	125	66	0.5156	62
62	73	0.5703	62	0.4844	126	62	0.4844	61
63	62	0.4844	67	0.5234	127	56	0.4375	63
64	60	0.4688	60	0.4688	128	56	0.4375	71
Average							0.4926	

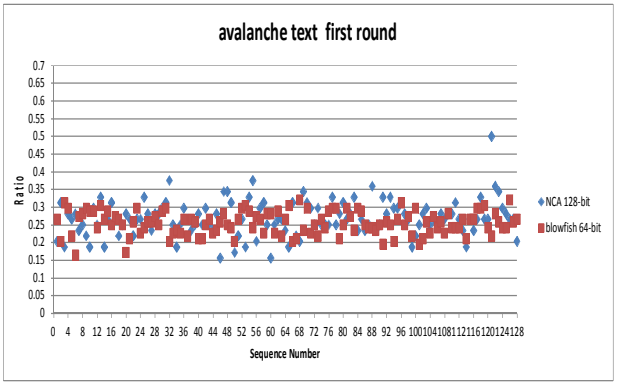

Figure1. Results of avalanche text of both algorithms algorithms for the first round

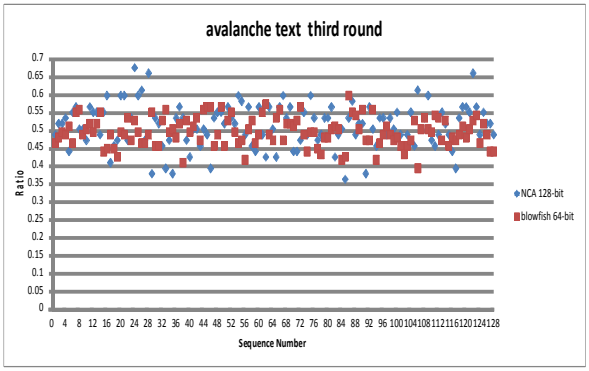

Figure 3. Results of avalanche text of both algorithms algorithms for the third round

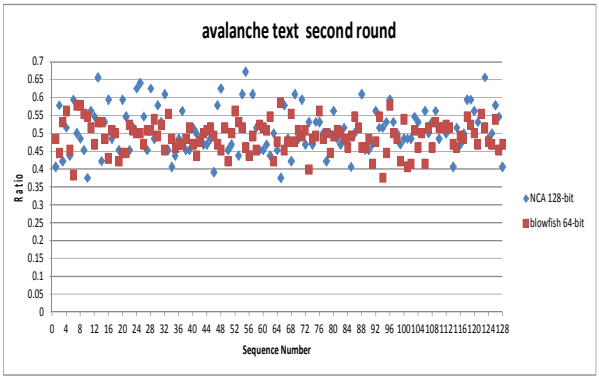

Figure 2. Results of the avalanche text of the both for the second round

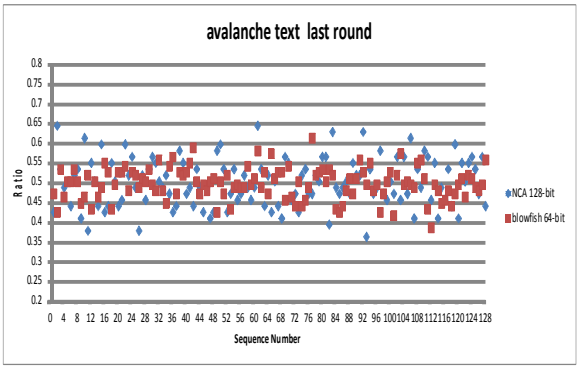

Figure 4. Results of the avalanche text of the both for the last round.

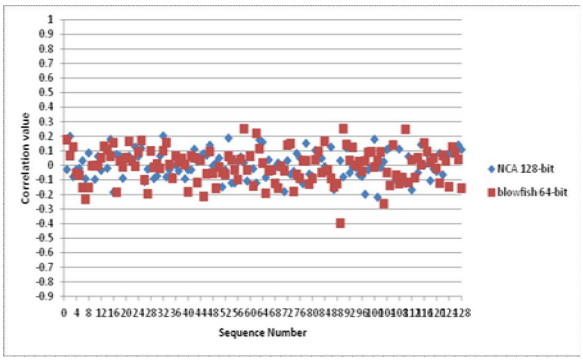

Figure 5. Illustrated results of correlation coefficient of both algorithms.

Table 3. Summarize the values of the correlation coefficient between plaintext and Ciphertext for RAF algorithm

1	-0.029	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	-0.002	73	-0.0628
10	-0.0972	74	-0.0417
11	0.0618	75	0.0821
12	-0.035	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	-0.047
22	0.0166	86	0.1256
23	0.1251	87	-0.167
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	0.202	96	-0.0752
33	-0.08	97	-0.1985
34	-0.032	98	-0.032
35	-0.0807	99	-0.0127
36	0.0012	100	0.178
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	0.111
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	-0.032	116	0.000244
53	0.1869	117	0.0807
54	-0.1216	118	-0.105
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

Appendix B

Table 4. Summarize the values of i*th* 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. Summarize the values of the ϵ_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	ϵ_A	Maximum value of $K_{AVA}L$	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	**92323**d1aafe9e47ee94ba07dc68bdbd	0.0391	0.5195	0.4805
6	**7458**aa85d6c3c9ef77d07170bba24fbb	0.0566	0.5283	0.4717
7	**05605**ab55f5cf2eca8781dac2e1bed6b	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. Summarize the values ϵ_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	ϵ_A	Maximum value of K_{AVAL}	Minimum value of K_{AVAL}
11	**11111111111111111111111111111111**	0.0264	0.5132	0.4868

Table 7. Summarize the values ϵ_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.	ϵ_A	Maximum value of K_{AVAL}	Minimum value of K_{AVAL}
12	**00000000000000000000000000000000**	0.0229	0.5115	0.4885

Table 8. Summarize the 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	0.5000	0.4844
$K_{SAC\ (2,j=1..8)}$	0.6016	0.4297	0.5000	0.5313	0.5156	0.4922	0.4688	0.4688
$K_{SAC\ (3,j=1..8)}$	0.5703	0.4609	0.4844	0.5313	0.5000	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	0.5000	0.5000	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	0.5000	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. Summarize the values of ϵ_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	ϵ_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. Summarize the values of the ϵ_S, maximum and minimum of K_{SAC} for dynamic 3D S- box with low entropy ones encryption key in RAF algorithm

No of experiment	ϵ_S	Maximum value of k_{SAC}	Minimum value of k_{SAC}
11	0.1875	0.5938	0.4063

Table 11. Summarize the values of the ϵ_S, maximum & minimum of K_{SAC} for the dynamic 3D S-boxes with low entropy zeroes encryption key in RAF

No of experiment	ϵ_S	Maximum value of k_{SAC}	Minimum value of k_{SAC}
12	0.2031	0.6016	0.3984

Table 12. Summarize the 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. Summarize the 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. Summarize the 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. Summarize the values of ϵ_{AVAL}, ϵ_{SAC} and ϵ_{BIC} for S-boxes in RAF and BA algorithms

Algorithm & S-box	ϵ_{AVAL}	ϵ_{SAC}	ϵ_{BIC}
dynamic 3D S –BOX in RAF	0.0566	0.2813	0.2698
S-boxes in BA	**0.0518**	**0.3594**	**0.4725**

Corresponding Author:
Dr. Ashwak Alabaichi
Department of computer science
Faculty of Science
Karbala University, Karbala, Iraq
E-mail: ashwakalabaichi2007@yahoo.com

References

1 ALabaichi A, Mahmod R, and Ahmad F. A dynamic 3D S–Box based on Cylindrical Coordinate System for Blowfish Algorithm. ICCSCM 2014a: Langkawi, Malaysia, ISBN: 978-967-11414-6-5: 277-92.
2 ALabaichi A, Mahmod R, Ahmad F. A Cylindrical Coordinate System with Dynamic Permutation Table for Blowfish Algorithm. International Journal of Soft Computing 2014b: 5(9):1-17.
3 Mar P, Latt K. New analysis methods on strict avalanche criterion of S-boxes, World Academy of Science, Engineering and Technology 2008: 48:150-4.
4 Adams C, Tavares S. The structured design of cryptographically good S-boxes, journal of Cryptology 1990: 3(1): 27-41.
5 Hussain I, Shah T, Mahmood H, Afzal M. Comparative analysis of S-boxes based on graphical SAC. 2010. International Journal of Computer Applications: 2(5):1-7.
6 Ahmed N. Testing an S-Box for Cryptographic Use, International Journal of Computer and Electrical Engineering, 1-5. http://www2.imm.dtu.dk/~naah/f/Testing%20an%20SBox%20for%20Cryptographic%20Use.pdf.
7 Isil V, Yücel M. On Satisfaction of Some Security Criteria for Randomly Chosen S-Boxes. 2000: In Proc. 20th Biennial Symp. On Communications, Kingston (May 2000).64-68.
8 Isil V, Yücel M. Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen n ×n S-Boxes. Turk J Elec Engin 2001: 9 (2):137-45.
9 ALabaichi A, Mahmod R, and Ahmad F. Analysis of Some Security Criteria for S-Boxes in Blowfish Algorithm. JDCTA 2013a: 7(12): 8–20.
10 ALabaichi A, Mahmod R, Ahmad F. Security Analysis of Blowfish Algorithm. Proceding of SDIWC: ICIA on IEEE, lodz university of tehnolgoy 2013b: ISBN: 978-1-4673-5256:12–8.
11 Ariffin S. A human immune system inspired byte permutation of block cipher, Ph. D. Thesis, Malaysia, UPM, 2012.

12 Mahmoud E, El Hafez A, Elgarf T, Zekry A. Dynamic AES-128 with Key-Dependent S- box. IJERA 2013: ISSN: 2248-9622: 3(1):1662-70.
13 Dawson E, Gustafson H, Pettitt AN. Strict Key Avalanche Criterion, Australasian Journal of Combinatorics. 1992: 6:147-53.
14 Juremi J, Mahmod M, Sulaiman S. A proposal for improving AES S-Box with rotation and key-dependent, in Cyber Security, Cyber Warfare and Digital Forensic (CyberSec): IEEE: 2012: 38-42.
15 Sulaiman S, Muda Z, Juremi J. The new approach of Rijndael key schedule, in Cyber Security, Cyber Warfare and Digital Forensic (CyberSec): 2012: IEEE, 23-27.
16 Castro J, Sierra J, Seznec A, Izquierdo A, Ribagorda A. The strict avalanche criterion randomness test. Mathematics and Computers in Simulation: Elsevier 2005: 68(1): 1-7.
17 Ali D, Ege B, Koçak O, Sulak F. Cryptographic Randomness Testing of Block Ciphers and Hash Functions, ACR Cryptology ePrint Archive 2010: 564, 1-12.
18 Himani A, Sharma M. Implementation and analysis of various symmetric cryptosystems 2010: 3 (12): 1173-76.
19 Mohan H, Reddy A. Performance Analysis of AES and MARS Encryption Algorithms. IJCSI 2011: 8(1):363-8.
20 Ramanujam S, Karuppiah M. Designing an algorithm with high Avalanche Effect, IJCSNS 2011:11(1):1-6.
21 Ariffin A, Mahmod R, Jaafar A, Rezal M, Ariffin K. An Immune System-Inspired Byte Permutation Function to Improve Confusion Performance of Round Transformation in Symmetric Encryption Scheme, in Computer Science and its Applications: Springer. 2012:339- 51.
22 Fahmy A, Shaarawy M, El-Hadad K, Salama G, Hassanain K. A proposal for A key- dependent AES. 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications 2005: Tunisia: SETIT, 1-7.
23 Mohammad F, Rohiem A, Elbayoumy A. A Novel S-Box of AES Algorithm Using Variable Mapping Technique. 13th International Conference on AEROSPACE SCIENCES & AVIATION TECHNOLOGY2009: 1-10.
24 Horst F. Cryptography and computer privacy. Scientific American. 1973:228(5):15- 23.
25 Webster A.F., Tavares S. E. On the design of S-Boxes. in Advances in Cryptology'85 Proceedings: Springer: 1986:1-10.
26 Selçuk K, Yücel M. On some cryptographic properties of Rijndael. Information Assurance in Computer Networks: Springer 2001:300-11.
27 Manikandan G, airam N, Kamarasan M. A New Approach for Improving Data Security using Iterative Blowfish Algorithm, Research Journal of Applied Sciences 2012: 4(6): 603-7.

10/25/2018