JJEE
Volume 3, Number 2, 2017
Pages 150-158
Jordan Journal of Electrical Engineering
ISSN (Print): 2409-9600, ISSN (Online): 2409-9619

Lifting Based S-Box for Scalable Block Cipher Design Based on Filter Banks

Saleh S. Saraireh

Department of Communication and Electronics Engineering, Philadelphia University, Amman, Jordan
e-mail: ssaraireh@philadelphia.edu.jo

Received: January 30, 2017 *Accepted: April 27, 2017*

Abstract— The security of data exchange is considered a significant problem. It requires the use of various cryptographic algorithms, such as stream cipher and block cipher. The implementation of a secure cryptographic block cipher algorithm requires the generation of strong substitution and permutation layers. These layers should satisfy the principles of security (diffusion and confusion). The proposed lifting scheme substitution box (s-box), which can be used to implement the substitution layer in a filter bank block cipher structure to support the scalability and security of the cipher. The cryptographic properties of the proposed s-box are studied, evaluated and compared with Rijndael s-box for the avalanche criteria, strict avalanche criterion (SAC), bit independent criterion (BIC), XOR table distribution, and linear approximation table (LAT). The results obtained confirm the security and scalability of the proposed s-box.

Keywords— Avalanche, Block cipher, Cryptography, Filter bank, Lifting, S-Box, Scalability.

I. INTRODUCTION

A Novel scalable block cipher structure based on filter banks over a finite field was proposed by the authors in [1]. The substitution layer combines the analysis filter bank and novel lifting scheme s-box to address the scalability limitations in existing block ciphers [2] without increasing complexity. This is achieved by exploiting the scalability and high diffusion properties of the filter bank structures; the scalable confusion via a judicious lifting scheme [1] enables the security versus complexity versus performance trade-off to be made for a particular application. Such trade-off is becoming increasingly important in emerging communications systems.

The lifting scheme being reversible by structure reduces the boundary existence; also, prediction and update lifting steps can be either linear or nonlinear based on the application. Hence, it allows nonlinearity to be introduced in a regular, extendable and simple form. These advantages of the lifting scheme make it suitable to implement a strong scalable s-box.

To examine the strength of the s-box, it is necessary to study its cryptographic properties. In [3], parity check bits were embedded in the output of the s-box of the modified DES cipher; the embedded process was applied to increase the resistant of the cipher against linear cryptanalysis. The obtained results showed that the embedded process did not enhance the security of the modified DES cipher. The security of the modified DES cipher s-box was examined in [4]; each s-box of the modified DES was precoded separately into even weight codes of length 4. The results were compared with the original DES using the same number of rounds.

In [5], the security of the s-boxes for RIJNDAEL, Exponentiation K Safer-64 and Logarithm K Safer-64 were evaluated. The evaluation process used different criteria, such as avalanche, strict avalanche and bit independence. The results showed the dominance of the Rijndael over the others. The s-boxes of AES, MARS, Skipjack, Serpent and Twofish ciphers were analyzed based on two layers, namely, white box layer and black box layer [6]. The outcome

Corresponding author's e-mail: ssaraireh@philadelphia.edu.jo

of the analysis showed that AES s-box is the most secure among all s-boxes followed by MARS s-box and Skipjack s-box, respectively.

In this paper, the diffusion and confusion properties of the proposed s-box are analyzed in terms of the avalanche, strict avalanche, and bit independent criteria for the diffusion aspects. Confusion aspects are analyzed in terms of the XOR table distribution and linear approximation table. It is shown that the proposed s-box satisfies the cryptographic security properties above.

The lifting scheme s-box is shown in Fig. 1. Note that the symbol *S* in Fig. 1 is denoting the inverse function with affine transform over GF(28), which is a nonlinear function. The lifting scheme over GF(28) as shown in Fig. 1 can be represented mathematically by the following equations:

$$a_1 = x_2 \oplus S(x_1) \tag{1}$$

$$a_2 = (x_1 \oplus S(a_1)) \tag{2}$$

$$y_2 = (a_1 \oplus S(a_2)) \tag{3}$$

$$y_1 = a_2 \oplus S(y_2) \tag{4}$$

where $\oplus$ is an exclusive or (XOR) operation.

The lifting scheme is used in the encryption side. Thus, it is necessary to satisfy perfect reconstruction in the decryption side. This can be carried out by a perfect reconstruction lifting scheme, which needs a small process arrangement as shown in Fig. 2. The reconstruction shown in Fig. 2 can be represented mathematically as follows:

$$b_1 = y_1 \oplus S(y_2) \tag{5}$$

$$b_2 = y_2 \oplus S(b_1) \tag{6}$$

$$x_1 = b_1 \oplus S(b_2) \tag{7}$$

$$x_2 = b_2 \oplus S(x_1) \tag{8}$$

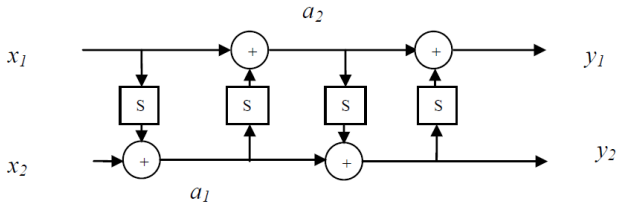

Fig. 1. Lifting scheme

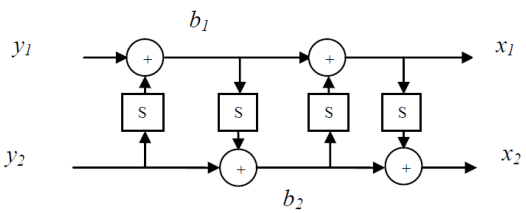

Fig. 2. Perfect reconstruction lifting scheme

II. BACKGROUND

A. Avalanche Criteria

Avalanche criterion was defined by Feistel [7]. It is considered one of the most important cryptographic properties of s-box. It is necessary to certify that a small change between two plaintexts gives a random difference (avalanche change) between two corresponding cipher texts. In order to satisfy avalanche criteria, flipping a single bit of the input value will result in half of the output bit values change.

For a cryptographic function $f(x): Z_2^n \to Z_2^n$, there are 2^n different inputs. Suppose that plaintexts P and P_i be different only in bit i $(P_i = P \oplus e_i)$, where e_i is a vector with *n*-bits and a 1 in position *i* [8], then the outputs of P and P_i are $f(P)$ and $f(P_i)$; the difference vector D^{e_i} is called the avalanche vector which can be computed as in (9). Its elements are called the avalanche variables [5]:

$$D^{e_i} = f(p) \oplus f(p_i) = [d_1^{e_i}, d_2^{e_i}, d_3^{e_i}, \ldots\ldots\ldots, d_n^{e_i}], \qquad d_j^{e_i} \in Z_2 \tag{9}$$

The overall change of the j^{th} avalanche variable over the whole input size 2^n can be done by taking into account all input pairs P and Pi which differ in the i^{th} bit [5]:

$$W(d_j^{e_i}) = \sum_{P \in Z_2^n} d_j^{e_i} \tag{10}$$

The cryptographic function is said to satisfy the avalanche criterion if for all $i = 1,2,\ldots,n$ [5]:

$$k_{AVAL}(i) = \frac{1}{n2^n} \sum_{j=1}^{n} W(a_j^{e_i}) = \frac{1}{2} \tag{11}$$

Normally, the $k_{AVAL}(i)$ takes values in the range [0, 1]. According to (11), $k_{AVAL}(i)$ is the calculation of the probability of change of the overall output bits when only the i^{th} bit in the input is altered. If $k_{AVAL}(i)$ is very close to one half, the cryptographic function satisfies the avalanche criterion; otherwise it does not.

B. Strict Avalanche Criterion (SAC)

Completeness and avalanche were joined into a strict avalanche criterion (SAC) by Webster and Tavares [9]. A cryptographic function $f(x): Z_2^n \to Z_2^n$ satisfies SAC if for all $i \in \{1,2,\ldots,n\}$ and $j \in \{1,2,\ldots,n\}$; input bit *i* changes output bit *j* with a probability of exactly 0.5. In such a case, it is necessary to separately satisfy each term of the summation of (11). This means that for each *i* and *j* to satisfy, SAC should satisfy the following equation [5]:

$$\frac{1}{2^n} W(a_j^{e_i}) = \frac{1}{2} \tag{12}$$

The SAC parameter ($k_{SAC}(i, j)$) can be defined as follows [5]:

$$k_{SAC}(i,j) = \frac{1}{2^n} W(a_j^{e_i}) = \frac{1}{2} \tag{13}$$

It should be noted that $k_{SAC}(i)$ takes the values in the range [0, 1]; and is considered as the calculation of the probability of change of the j^{th} output bit once the i^{th} bit in the input is altered. The cryptographic function satisfies the strict avalanche criterion, if $k_{SAC}(i)$ is very close to 0.5; otherwise it does not.

If a cryptographic function satisfies the SAC, then it also satisfies the completeness and avalanche criterion. However, if the cryptographic function satisfies the completeness and the avalanche criterion, it does not mean it should satisfy the SAC.

C. Bit Independent Criterion (BIC)

Bit independent criterion was defined by Webster and Tavares [9]. A cryptographic function $f(x): Z_2^n \to Z_2^n$ satisfies bit independent criterion if for all $i, j, k \in \{1,2,...,n\}$ with $j \neq k$; changing the input bit *i* makes the output bits *j* and *k* change independently [7].

In order to determine the bit independent criterion of a cryptographic function, it needs to calculate the correlation coefficient between the j^{th} and k^{th} components of the avalanche vector. The bit independence parameter is related to the result of changing the input bit *i* to the output bits *j* and *k* of the avalanche vector. It can be calculated mathematically by [7]:

$$BIC^{ei}(d_j, d_k) = \max_{1 \le i \le n} \left| corr(d_j, d_k) \right| \tag{14}$$

Then the BIC can be calculated as follows [7]:

$$BIC(f) = \max_{1 \le i \le n, 1 \le j,k \le n, j \neq k} BIC(d_j, d_k) \tag{15}$$

The BIC takes a value in the range [0, 1]; the best value of BIC is equal to 0. While avalanche variables are independent, BIC is 1 in the worst case. The avalanche variables are correlated.

D. XOR Table Distribution

In order to investigate the security of the block cipher against differential cryptanalysis, which exploits the high values of the XOR table of s-boxes used by a block cipher, it is essential to determine the XOR table distribution (difference distribution table) of the s-box. The values in the XOR table should be as small as possible to avoid differential cryptanalysis.

The dimension of the XOR table of an $n \times n$ s-box is a $2^n \times 2^n$ matrix [10], with rows and columns indices $0, 1, 2, ..., 2^{n-1}$. In order to implement the XOR table distribution, assume that the input vector is P and changed by ΔP; then the output difference is ΔC and given by:

$$\Delta C = f(P) \oplus f(P \oplus \Delta P) \tag{16}$$

where $\Delta P \in Z_2^n$ and $\Delta C \in Z_2^m$.

Now the XOR table distribution is given by [5]:

$$XOR_f(\Delta P, \Delta C) = \#\{P \mid f(P) \oplus f(P \oplus \Delta P) = \Delta C\} \tag{17}$$

The entries of the XOR table always take an even value; the sum of all values in the row equals 2^n. In order to design a secure and strong block cipher, it is necessary to have a secure s-box that satisfies the confusion property, and has small entries in its XOR table distribution.

E. Linear Approximation Table (LAT)

In order to evaluate the security of the block cipher against linear cryptanalysis, it is necessary to determine the linear approximation table which gives information about the security of the s-box against linear cryptanalysis. Therefore, it is considered as a measure of resistance for the s-boxes against linear cryptanalysis. To avoid linear cryptanalysis, the values of the linear approximation table should be as small as possible [4].
The dimensions of the linear approximation table are the same as the XOR table distribution. It is $2^n \times 2^n$ matrix for an $n \times n$ s-box; and its rows and columns indices are $0,1,2,..., 2^{n-1}$.
To implement the linear approximation table, it is assumed that X is an input of an s-box (S); Y is the output of the s-box $Y = S(X)$; and the linear approximation table has its entry sitting at the X'^{th} row and the Y'^{th} column, defined as [4]:

$$LAT\,(X',Y') = \#\{X \mid Y' \bullet S(X) = X' \bullet X\} - 2^{n-1} \tag{18}$$

where ($\bullet$) indicates the scalar or products of the vectors X and X'.
Basically, linear cryptanalysis exploits weak elements of the linear approximation table, whereas differential cryptanalysis exploits the weak components of the XOR distribution table. For both tables, the weak element is the highest magnitude element in the corresponding table.

III. SIMULATION RESULTS AND DISCUSSION

A. Avalanche Criterion

Generally, if s-box (11) is not matched exactly, there will be some marginal error, which is called a relative error interval $\pm \in$. This error should be very small and the value of $k_{AVAL}(i)$ should be very close to 0.5; otherwise, the s-box does not satisfy the avalanche criteria. Consequently, the diffusion property is not satisfied.
The avalanche criterion within an error range $\pm \in$ for all i is defined as follows [5]:

$$\frac{1}{2}(1-\in) \le k_{AVAL}\ (i) \le \frac{1}{2}(1+\in) \tag{19}$$

The overall relative absolute error $(\in_{AVAL})$ of s-box is calculated by [5]:

$$\in_{AVAL} = \max_{1 \le i \le n} \left| 2\ k_{AVAL}(i) - 1 \right| \tag{20}$$

For the proposed lifting s-box, the avalanche criterion in (11) is evaluated and found; and the maximum relative absolute error is obtained using (20), where its value is 0.0083 compared with 0.0352 for the s-box of Rijndael [5]. Fig. 3 depicts the relative absolute error corresponding to the bit position of the avalanche vector for lifting scheme s-box.

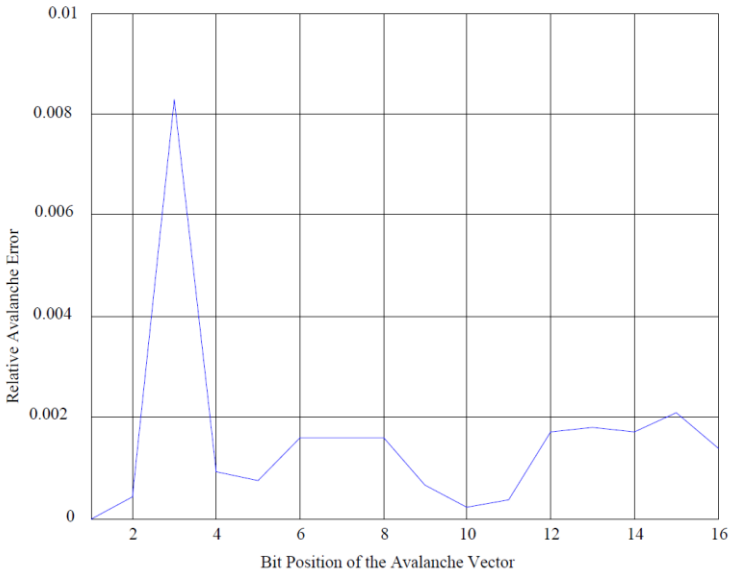

Fig. 3. Relative absolute error versus bit position of the avalanche lifting scheme s-box

B. Strict Avalanche Criterion (SAC)

As mentioned earlier, the satisfaction of completeness and avalanche criterion does not mean there will be satisfaction of strict avalanche criterion, but the reverse is true. Therefore, it is necessary to run the strict avalanche criterion test to investigate the diffusion of the proposed lifting scheme s-boxes. The strict avalanche criterion is considered a special case of the avalanche criterion, as represented in (12). Thus, the error margin for the strict avalanche criterion is more than the error margin for the avalanche criterion.

Normally, the strict avalanche criterion does not satisfy (13) with exactly one half, but there is some error margin. However, this error margin should be very small. The relative absolute error of the strict avalanche criterion ($\in_{SAC}$) is defined as follows [5]:

$$\in_{SAC} = \max_{1\le i,\, j\le n} \left| 2k_{SAC}(i,\, j) - 1 \right| \tag{21}$$

By applying (13) and (21), the maximum relative absolute error of SAC for the lifting scheme s-box is found to be 0.0139, while it is 0.1250 for Rijndael [5]. The result denotes that the lifting scheme s-box satisfies both the SAC with a very small error margin and the diffusion property. Fig. 4 shows 16 curves corresponding to input differences e1, e2, e3…, e16.

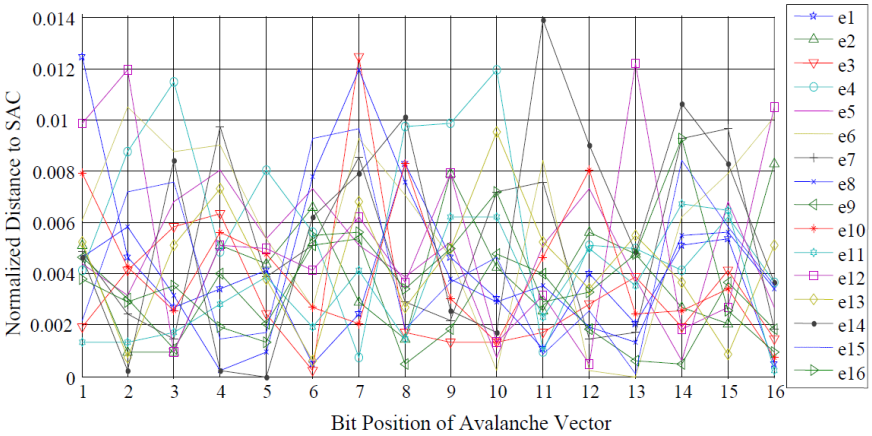

Fig. 4. Relative absolute error for SAC versus bit position of the avalanche vector for lifting scheme s-box

C. Bit Independent Criterion (BIC)

The calculation of BIC is different from the calculations of the avalanche criterion and SAC. The calculation of BIC is based on calculation of (14) to find $BIC(f)$ for the s-box, which is considered the maximum correlation value between any two avalanche values. Therefore, the relative absolute error ($\in_{BIC}$) is defined as follows [5]:

$$\in_{BIC} = BIC(f) \tag{22}$$

It is found to be 0.0204 compared with 0.1341 for the s-box of Rijndael [5]. Fig. 5 corresponds to the maximum relative absolute error for BIC of the lifting scheme s-box according to the avalanche bit position.

Table 1 summarizes the maximum relative errors for the lifting s-box and Rijndael s-box. The relative error values obtained for the lifting s-box are very small; reflecting the high diffusion rate that the proposed s-box exhibits. Also, the relative error values for the proposed s-box are very small compared with the relative error values for the s-box of Rijndael. This means that the proposed s-box has a higher diffusion rate; as a result, more security can be exhibited.

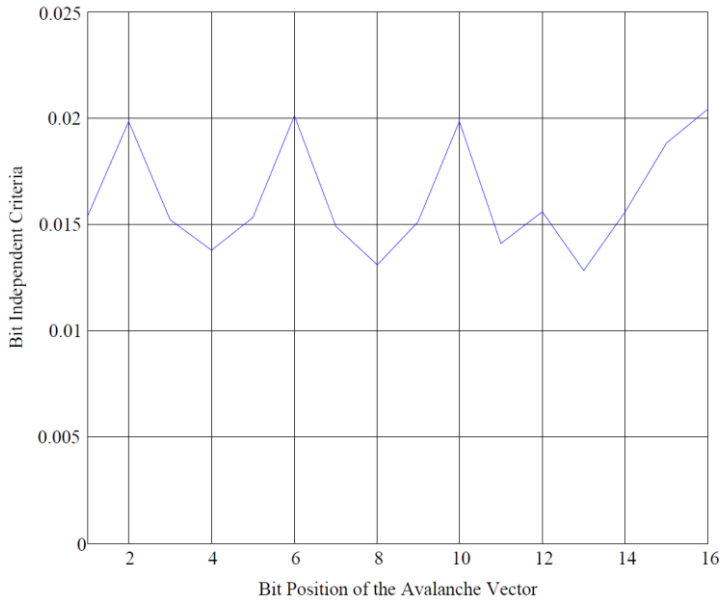

Fig. 5. Relative absolute error for BIC versus bit position of the avalanche vector for the lifting scheme s-box

TABLE 1
MAXIMUM RELATIVE ERROR FOR THE LIFTING SCHEME S-BOX AND RIJNDAEL S-BOX

$\in_{AVAL}$		$\in_{SAC}$		$\in_{BIC}$	
Lifting	Rijndael [5]	Lifting	Rijndael [5]	Lifting	Rijndael [5]
0.0083	0.0352	0.0139	0.1250	0.0204	0.1341

D. XOR Table Distribution

To investigate the confusion of the proposed lifting scheme s-box, determination of the XOR table distribution is required since the s-box is the only nonlinear component of a block cipher. The XOR table distribution evaluates the security of the block cipher against differential cryptanalysis; and is considered the first step towards examining the strength of the block

cipher against differential cryptanalysis. From the XOR table distribution, designers can decide if the intended s-box is suitable for their block ciphers or not.

The dimension of the XOR distribution table of the s-box depends on its input; its entries are calculated using (17). It should be noted that for the lifting scheme s-boxes, the dimension of the XOR distribution table depends on the number of input bits for each branch. It is $2^{16} \times 2^{16}$ in the case of a 16×16 lifting scheme s-box.

All the entries of the XOR distribution table should be as small as possible because differential attacks exploit large values in the XOR distribution table in order to break the cipher.

It should be noted that when the input XOR equals zero, the output XOR will be zero for all pairs. Because it is impossible to have any nonzero value, the entry of the XOR table will be 2^{16} in the case of 16×16 s-box. Also, all the values in the table are even values; and the sum of each line equals 2^{16} when the dimension of the XOR distribution table is $2^{16} \times 2^{16}$. This means that the summation of each line in the XOR table distribution depends on the size of its s-box.

For the proposed lifting scheme s-box, the maximum value in its XOR distribution table is 22 by applying (17). This value is very low indeed compared to the s-box size (16x16), resulting in a very small maximum differential probability.

E. Linear Approximation Table (LAT)

The other table to be produced to examine the confusion property of the proposed s-box is the linear approximation table. The linear approximation table evaluates the security of a block cipher against linear cryptanalysis.

As mentioned earlier, designers can use the XOR table distribution to decide on use of suitable s-boxes to counter differential cryptanalysis. The linear approximation table can, however, be used by cryptographers to decide on use of suitable s-boxes to counter linear cryptanalysis.

The dimensions of the linear approximation table depend on the size of the s-box and it is $2^{16} \times 2^{16}$ for 16×16 lifting scheme s-box. The entries of the linear approximation table are calculated by using (18), the entries should be as small as possible to avoid linear cryptanalysis. If the input subset is X'=0; and the output subset is $Y' = 0$, the entry to LAT contains 32768 for a 16×16 lifting scheme s-box. Entries are zeros for all other output subsets. The maximum value obtained in the linear approximation table ($LAT_{\max}$) is 902. This value is very low compared to the s-box size (16x16), resulting in a very small maximum linear probability.

Maximum values in the XOR table distribution and the linear approximation table are very small compared to the s-box size; therefore, the proposed lifting scheme satisfies the confusion property. Consequently, it is immune to linear and differential cryptanalysis.

IV. CONCLUSIONS

The cryptographic properties of the lifting scheme s-box were evaluated and compared with Rijndael s-box. The results showed that the lifting s-box is dominant over Rijndael s-box. It is considered as a strong s-box as it obeys the avalanche criterion, SAC and BIC with very small marginal error. The maximum values in the XOR table distribution and the linear approximation table are also very small values compared with the s-box size. Therefore, the lifting scheme s-box supports the security and scalability of the scalable filter bank block cipher.

REFERENCES

[1] S. Saraireh and M. Benaissa, "A scalable block cipher design using filter banks and lifting over finite fields," *Proceedings of IEEE International Conference on Communications*, pp. 1-5, 2009.

[2] J. Daemen and V. Rijmen, "AES proposal: Rijndael, AES algorithm submission," *Produced by NIST Computer Security Resource Center*, pp. 1-45, 1999, http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf

[3] Y. Borissov, P. Boyvalenkov, and R. Tsenkov, "Linear cryptanalysis and modified DES with embedded parity check in the s-boxes," *Cryptography and Information Security, Lecture Notes in Computer Science*, vol. 116, no. 9540, pp. 60-78, 2016.

[4] Y. Borissov, P. Boyvalenkov, and R. Tsenkov, "On a linear cryptanalysis of a family of modified DES ciphers with even weight s-boxes," *Cybernetics and Information Technologies*, vol. 16, no 4, pp. 3-11, 2016.

[5] S. Kavut and M. Yücel, "On some cryptographic properties of Rijndael," *Lecture Notes in Computer Science: Information Assurance in Computer Networks, Methods, Models and Architectures for Network Security*, vol. 101, no. 2052, pp. 300-311, 2001.

[6] A. Ahmad and M. Farooq, "S-box scope: a meta s-box strength evaluation framework for heterogeneous confusion boxes," *Proceedings of Hawaii International Conference on System Sciences*, pp 5545-5553, 2016.

[7] I. Vergili and D. Melek, "Avalanche and bit independence properties for the ensembles of randomly chosen nxn s-boxes," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 9, no. 2, pp. 137-145, 2001.

[8] K. Kim, T. Matsumoto, and H. Imai, "A recursive construction method of s-boxes satisfying strict avalanche criterion," *Advances in Cryptology, Lecture Notes in Computer Science*, vol. 90, no. 537, pp. 545-553, 1990.

[9] A. Webster and S. Tavares, "On the design of s-boxes," *Advances in Cryptology*, vol. 85, no. 218, pp. 523-534, 1986.

[10] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal. of Cryptology*, vol. 4, no. 1, pp. 3-72, 1991.