DESIGNING MORE EFFICIENT NOVEL S_8 S-BOXES

Tariq Shah[1], Ayesha Qureshi[1], Muhammad Fahad Khan[2]

[1] Department of Mathematics, Quaid-i-Azam University, Islamabad;
[2] Department of Software Engineering, Foundation University, Islamabad;
e-mails: stariqshah@gmail.com, ayesha.qureshi6@gmail.com,
fahad.khan@fui.edu.pk;
Pakistan

Abstract: The contemporary methods for the construction of S_8 S-boxes rely on the application of permutations of symmetric group S_8 on the elements of finite Galois field $GF(2^8)$. The proposed work is intended to diminish the size of S_8 S-boxes by working with a small unit of data. 40,320 S_8 S-boxes of small size are formed by using the action of symmetric group S_8 on the elements of subgroup of $GF(2^8)^*$. In practical applications, all the obtained S-boxes are not functional for retrieving the encrypted information. To deal with this challenge, this study addresses classification algorithm of small S_8 S-boxes into two different categories. Among which the aptness of one category has been confirmed for encryption applications. The results of the experiments based on several widely used statistical analysis validate the practicality of the proposed S-boxes.

Key words: S_8 S-boxes, symmetric group, encryption, decryption.

1. INTRODUCTION

Cryptography is one of the most significant mechanisms used in the field of information security. Encryption algorithms in Cryptography play an important role in ensuring the security of information. With the widely use of digital products and evolution of attacks, research and development of more information security techniques with high efficiency and reliability are demanded.

The encryption process in cryptographic algorithms is supplemented with a nonlinear component capable of creating confusion in the encrypted data. The design of this nonlinear component, called S-box, is of great interest to cryptanalysts because the understanding of its functionality yields insight into the encryption process and its characteristics [1-3].

S-box is an elementary component of symmetric key algorithms which performs substitution. In block ciphers, it is typically used to vague the relationship between the key and the cipher text [4]. In general, an $m \times n$ S-box takes m number of input

bits and transforms them into n number of output bits, where m is not necessarily equal to n. The primary cryptographic properties required by strong S-boxes are balance, nonlinearity, strict avalanche criterion and least linear and differential approximation probabilities. Different cryptographic applications require different acceptable measures of these and other properties.

The advanced encryption standard S-Box was unambiguously designed to be vigorous to linear and differential cryptanalysis by minimizing the correlation between linear transformations of input/output bits [5]. In the development of symmetric cryptosystems, a significant portion of the time spent on design or analysis is centered on the substitution boxes of the algorithm. The study of the design properties and construction methodology of Rijndael S-box played an important role in the analysis of its behavior [6, 7]. In literature, almost all S-boxes are generally synthesized over finite Galois fields by different techniques [8-13]. In [14], the authors presented a very new technique for generating 8×8 S-boxes by using the action of symmetric group S_8 on AES S-box and constructed 40,320 new S-boxes, named as S_8 AES S-boxes. Later, the same idea was used for some other S-boxes and the improved performance parameters and usefulness of S_8 S-boxes was highlighted in practical applications. In [15, 16], the authors shifted the structure of S-box to the subgroup of multiplicative group of Galois field and constructed S-boxes on the elements of subgroup of order 15 adjoining zero. In the continuation of the study of S_8 S-boxes, we will perform the action of symmetric group of permutations on this S-box and get 40,320 small S_8 S-boxes. We have found that all the attained S-boxes are not functional for retrieving the encrypted information. So, we have classified small S_8 S-boxes into two different categories, among which we have specified one of the categories for encryption applications.

Rest of the paper is organized as follows: In section 2, the algebraic expression of S-box on subgroup of Galois field is presented. Section 3 gives the structure of existing S_8 S-boxes in literature. In section 4, we will explain construction mechanism of new S-boxes with their classification technique and suitability in image encryption. Section 5 gives the algebraic analyses of these S-boxes. Conclusion is presented in section 6.

2. ALGEBRAIC EXPRESSION OF S-BOX ON SUBGROUP OF GALOIS FIELD

The erection of an S-box based on linear fractional transformation applied on the subgroup of multiplicative part of Galois field $GF(2^8)$ is presented in [15]. The S-box is constructed on the elements of the subgroup of order 15 (say H_{15}) adjoining zero, of $GF(2^8)^*$, with the following irreducible polynomial for multiplication: $f(x) = x^8 + x^4 + x^3 + x^2 + 1$. The structure of this S-box can be represented by the following expression:

$$S(z) = \begin{cases} \dfrac{az \oplus b}{cz \oplus d}, & z \neq d^2 \\ y \in H_{15} \cup \{0\} \backslash S(z), & z = d^2 \end{cases}, \quad (1)$$

where $a, b, c, d \in H_{15}$ such that $b = a^{-1}$ and $d = c^{-1}$ with $ad - bc \neq 0$. Table 1 gives the conventional representation of the S-box for the values of a, b, c, and d chosen to be 152, 11, 78 and 69 respectively. The construction with this method possesses desirable algebraic complexity and cryptographic characteristics.

Table 1. S-box on $H_{15} \cup \{0\}$

LSB's	**0**	**1**	**2**	**3**
0	152	79	147	220
1	69	0	10	11
2	214	221	78	68
3	146	1	153	215

3. STRUCTURE OF EXISTING S_8 S-BOXES IN LITERATURE

Advanced encryption standard (AES) is a renowned algorithm used in symmetric key cryptography. The study of structural properties of AES shows that S-box transformation is the only nonlinear constituent that can provide confusion in the algorithm. That is why, many different types of S-boxes for AES have been proposed by various authors in literature. The most used 8×8 S-boxes includes APA, Gray, Skipjack, Liu J, Xyi and residue prime S-box. All mentioned S-boxes are constructed on the elements of finite Galois field of order 256.

In [14], the authors presented a new technique for generating 8×8 S-boxes by using the action of symmetric group S_8 on AES S-box and constructed 40,320 new S-boxes, named as S_8 AES S-boxes. They also proved that algebraic complexity of S_8 AES S-boxes remains the same as AES S-box. The computation algorithm of S_8 AES S-boxes is presented in Fig. 1. Later, the same idea was used for some other S-boxes and the improved performance parameters and usefulness of S_8 S-boxes was highlighted in practical applications [17-20]

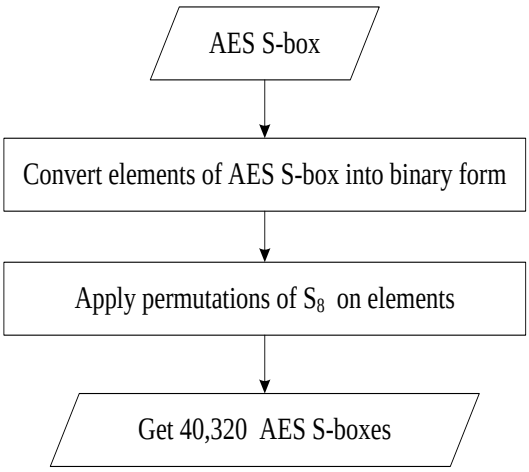


Fig. 1. Algorithm for S_8 AES S-boxes

4. CONSTRUCTION OF SMALL S_8 S-BOXES

Theorem: *The application of S_n permutations on the existing elements of an S-box in $GF(2^n)$ creates $n!$ distinct S_n S-boxes in $GF(2^n)$. This action does not affect the algebraic complexity of S-box. The mathematical representation of the S_n transformation process is given as,*

$$f: S_n \times S - box \rightarrow S_n\ S - box. \quad (2)$$

If $S_8 = \{\pi_i | i = 1,2,3, \ldots, 8!\}$, then according to equation (2), 8! new S_8 S-boxes can be obtained from S-box Table 1 with the following procedure,

$$\pi_i(S - box\ on\ H_{15} \cup \{0\}) = S_8\ S - box_i. \quad (3)$$

Example 1: *An example of the small S_8 S-box obtained by using the permutation* $(8\ 7\ 6\ 5\ 4\ 3\ 2\ 1) \in S_8$ *, is given in Table 2.*

Table 2. Example of small S_8 S-box

	0	**1**	**2**	**3**
0	25	242	201	59
1	162	0	80	208
2	107	187	114	34
3	73	128	153	235

4.1. Classification of small S_8 S-boxes

In section 4, we have obtained 40,320 small S_8 S-boxes by the action of symmetric group S_8 on the S-box on subgroup of Galois field. The elements of the S-box on subgroup of Galois field owns distinct least significant bits (LSB's) due to which the both transformations of encryption and decryption are possible. But this characteristic of the S-box is not inherited in all S_8 S-boxes. Thus, all S-boxes are not functional in retrieving the encrypted information. So, we have divided these S-boxes into two groups. First group contains the S-boxes with elements having distinct LSB's, while the other contains the remaining ones. Among 40,320 S-boxes, we found 5,760 S-boxes in first group that can be used in image encryption applications. The S-box in Example 1 lies in second group as its elements does not own distinct LSB's. Table 3 gives the example of S-box lying in first group. We will use this S-box for experimental work and analysis purpose.

Example 2: *An example of the small S_8 S-box lying in first group obtained by using the permutation* $(7\ 6\ 4\ 3\ 8\ 5\ 2\ 1) \in S_8$ *and the corresponding inverse S-box is given in Table 3 and Table 4 respectively.*

Table 3. Example of proposed small S_8 S-box

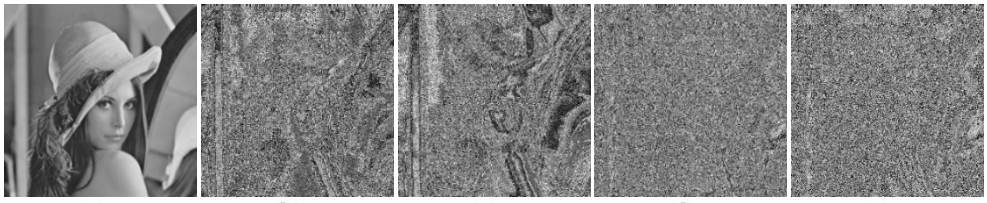
	0	**1**	**2**	**3**
0	37	206	169	103
1	74	0	132	140
2	227	111	198	66
3	161	8	45	235

Table 4. The inverse small S_8 S-box

	0	**1**	**2**	**3**
0	69	220	11	152
1	214	0	10	147
2	221	146	68	79
3	215	78	1	153

4.2. Majority logic criterion for small S_8 S-boxes

In this section, we will examine the results of correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis and decide by using majority logic criterion [21], the best S-box candidate among AES S-box, S_8 AES S-box, S-box on $H_{15} \cup \{0\}$, and the proposed small S_8 S-box.

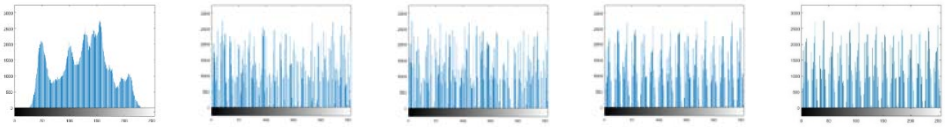


(a) (b) (c) (d) (e)

Fig. 2. (a) Plain image. (b) substituted image with AES S-box. (c) substituted image with S_8 AES S-box. (d) substituted image with S-box on $H_{15} \cup \{0\}$, (e) substituted image with proposed small S_8 S-box.

Fig. 2(a-e) depicts the standard grayscale image of Lena in png format, of size 512×512 pixels and the substituted images using AES S-box, S_8 AES S-box, S-box on $H_{15} \cup \{0\}$, and the proposed small S_8 S-box respectively. The visual analysis is revealing that the proposed small S_8 S-box is very competent in hiding the image contents. The numerical results of statistical analyses used by the majority logic criterion are listed in Table 5. It is clear from the results of statistical analyses that the proposed small S_8 S-box yields desirable results for MLC.

In Fig. 3, the encryption quality has been shown by means of histograms of plain image and the corresponding substituted images respectively.



(a) *(b)* *(c)* *(d)* *(e)*

Fig. 3: Histograms (a) Plain image. (b) substituted image with AES S-box. (c) substituted image with S_8 AES S-box. (d) substituted image with S-box on $H_{15} \cup \{0\}$. (e) substituted image with the proposed small S_8 S-box.

Table 5. Results of statistical analyses used by majority logic criterion

Attribute	Plain image	AES S-box	S_8 AES S-box	S-box on $H_{15} \cup \{0\}$	Small S_8 S-box
Entropy	5.9032	6.4196	6.4309	7.4451	6.4437
Contrast	0.2288	10.5914	9.2531	10.3525	10.2486
Correlation	0.9503	0.0666	0.1216	0.0175	0.0206
Energy	0.1318	0.0172	0.0174	0.0160	0.0157
Homogeneity	0.9058	0.4352	0.4452	0.4054	0.4024
MAD	19.8828	33.9488	32.0243	31.9990	31.8747

5. ALGEBRAIC COMPLEXITY OF SMALL S_8 S-BOXES

This segment has been devoted for calculating and equating the algebraic complexity of the new S-boxes by computing the results for balance property, nonlinearity, linear approximation probability, differential approximation probability and strict avalanche criterion.

5.1. Balance property

S-boxes are Boolean mappings from $\{0,1\}^p \to \{0,1\}^q$ and there are p component functions each being a map from $\{0,1\}^p \to \{0,1\}$. A Boolean map of m bits is said to be balanced if its output yields the value 1 with probability $1/2$ over its input set [22]. Balanced Boolean mappings are mostly practiced in cryptography. If a map is not balanced, it will have a statistical bias, making it subject to cryptanalysis such as the correlation attack. The S-box arranged in Table 3 is a set of 8 Boolean vectors of size 16. The truth tables of these vectors, say $f_0, f_1, f_2, \dots, f_7 : H_{15} \cup \{0\} \to \{0,1\}$, are given in Table 6. Except f_5 all the vectors are balanced. The balancedness of some of the Boolean vectors of S-boxes diverts to

imbalance when they are constructed on algebraic substructures. But more are the number of balanced Boolean vectors, the more robust will be the S-box. Note that, the S-box on $H_{15} \cup \{0\}$ also holds seven balanced and one non-balanced Boolean function.

Table 6. Truth table of Boolean vectors

x	$f_7(x)$	$f_6(x)$	$f_5(x)$	$f_4(x)$	$f_3(x)$	$f_2(x)$	$f_1(x)$	$f_0(x)$
0	0	0	1	0	0	1	0	1
152	1	1	1	0	0	0	1	1
78	0	0	1	0	1	1	0	1
10	1	1	0	0	0	1	1	0
153	0	1	1	0	1	1	1	1
214	1	0	0	0	0	1	0	0
68	0	1	0	0	1	0	1	0
147	0	1	1	0	0	1	1	1
79	1	1	1	0	1	0	1	1
146	1	0	1	0	1	0	0	1
215	1	0	0	0	1	1	0	0
220	1	0	1	0	0	0	0	1
221	0	0	0	0	1	0	0	0
69	0	0	0	0	0	0	0	0
11	0	1	0	0	0	0	1	0
1	1	1	0	0	1	1	1	0

5.2. Nonlinearity test

The security of cryptographic transformations depends on the nonlinearity of substitutions. The non-linearity of

$$f \in \{B_n | B_n \; is \; a \; Boolean \; function \; with \; n \; variables\}$$

is the minimum distance between f and the set of all affine functions A_n [23]. i.e.

$$NL(f) = \min_{h \in A_n} d(f, h). \quad (4)$$

Or equivalently, it is half the number of bits in the Boolean function, less the largest absolute value of the unexpected distance. The unexpected distance is computed with the Fast Walsh Transform (FWT) [24]. It can be perceived from Table 7 that the action of symmetric group S_8 on S-box on subgroup $GF(2^8)^*$ does not affects the average value of nonlinearity.

Table 7. Results of nonlinearity

Boolean mappings	f_7	f_6	f_5	f_4	f_3	f_2	f_1	f_0	**Average**
S-box on $H_{15} \cup \{0\}$	4	4	0	4	2	4	4	4	3.25
Small S_8 S-box	4	4	4	0	4	2	4	4	3.25

5.3. Linear approximation probability test

The maximum imbalance of an event between input and output bits is quantified by the linear approximation probability test. The linear approximation probability (or the probability of bias) of an S-box $S: GF(2^m) \rightarrow GF(2^n)$ is denoted and defined as:

$$LP_S = \max_{\Gamma x, \Gamma y \neq 0} \left| \frac{\#\{x \in GF(m): x \cdot \Gamma x = f(x) \cdot \Gamma y\}}{2^m} - \frac{1}{2} \right|, \quad (5)$$

where Γx and Γy are the bit-masks to the parity of the input and output bits respectively and '.' denotes the 'bitwise and' operation [25]. The S-box on $H_{15} \cup \{0\}$ exhibits LP with a value of 0.125, which is the maximum linear probability of the 8-bit S-box. Whereas, for small S_8 S-box the value of LP is zero.

5.4. Differential approximation probability test

Differential cryptanalysis is based on the use of imbalances in the input/output XOR distribution. Differential approximation probability measures the differential uniformity demonstrated by an S-box. The S-box is immune to the differential attack if each output XOR occurs with an equal probability for each input XOR. The differential approximation probability of an S-box $S: GF(2^m) \rightarrow GF(2^n)$ is denoted and defined as :

$$DP_f = \max_{\Delta x \neq 0, \Delta y} \left(\frac{\#\{x \in GF(2^m): S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^m} \right), \quad (6)$$

where $\Delta x \in GF(2^m)$ and $\Delta y \in GF(2^n)$ are differentials at the input and output respectively [26]. The smaller the differential uniformity, the stronger is the S-box. The outcomes of the differential approximation probability of the most probable output XOR for small S_8 S-box by applying the input and output differentials are given in Table 8. The maximum of the matrix is 0.25, showing that $DP(\text{small } S_8 \text{ S} - \text{box } = 0.25)$, which coincides the optimal differential bound of 4×4 S-boxes and of S-box on $H_{15} \cup \{0\}$.

Table 8. DP of the most probable output XOR for small S_8 S-box

0	**1**	**2**	**3**
0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25
0.25	0.25	0.25	---

5.5. Strict Avalanche Criterion

The strict avalanche criterion, introduced by Webster and Tavares in [27], is a generalization of the avalanche effect and it was built on the concepts of completeness and avalanche. The effect of a single input bit change on the output bits is examined by this criterion. A Boolean function $f_n: GF(2^n) \to \{0,1\}$ is said to fulfill this criteria if, whenever a single input bit is complemented, each of the output bits changes with a 50% probability. Mathematically,

$$\sum_{i=0}^{2^n-1} f_n(v_i) \oplus f_n(v_i \oplus \alpha) = 2^{n-1}, \tag{7}$$

where $\alpha \in GF(2^n)$ such that $HW(\alpha) = 1$. Table 9 shows that the value of average strict avalanche criterion remains analogous after the action. The average value is 0.4688, which is much closed to the ideal value 0.5.

Table 9. Results of Strict avalanche criterion

Boolean mappings	f_7	f_6	f_5	f_4	f_3	f_2	f_1	f_0	**Average**
S-box on $H_{15} \cup \{0\}$	0.5	0.5	0	0.5	0.5	0.5	0.5	0.75	0.4688
Small S_8 S-box	0.75	0.5	0.5	0	0.5	0.5	0.5	0.5	0.4688

6. CONCLUSION

In literature, the idea of generation of new S-boxes by the action of symmetric group of permutations S_8 on the elements of 8×8 S-boxes has been practiced by the researchers. But when this idea is applied to the constructions over algebraic substructure, we came across with some issues and found that some of the attained S-boxes are not functional in encryption applications. In this work, we have resolved this problem by classifying the small S_8 S-boxes into two groups, among which the suitability of one group to various encryption applications has been demonstrated.

REFERENCES

[1] Javeed, A. et al. Design of an S-box using Rabinovich-Fabrikant system of differential equations perceiving third order nonlinearity. *Multimedia Tools and Applications*, 9 (vol. 79), 2020, pp. 6649-6660.

[2] Shah, T., Shah, D. Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over $\mathbb{Z}_2$. *Multimedia Tools and Applications*, 2 (vol. 78), 2019, pp.1219-1234.

[3] Jamal, S.S. et al. Construction of new substitution boxes using linear fractional transformation and enhanced chaos. *Chinese Journal of Physics*, vol. 60, 2019, pp.564-572.

[4] Shannon, C. E. Communication theory of secrecy systems. *The Bell System Technical Journal*, 4 (vol. 28), 1949, pp. 656-715.

[5] Daemen, J., Rijmen, V. *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer-Verlag, Berlin Heidelberg, 2002.

[6] Ferguson, N., et al. A simple algebraic representation of Rijndael. In: Vaudenay S., Youssef A.M. (eds) *Selected Areas in Cryptography. SAC 2001*. Lecture Notes in Computer Science, vol 2259. Springer, Berlin, Heidelberg, 2001, pp. 103-111.

[7] Murphy, S., Robshaw, M.J. Essential algebraic structure within the AES. In: Yung M. (eds) *Advances in Cryptology - CRYPTO 2002*, Lecture Notes in Computer Science, vol 2442, Springer, Berlin, Heidelberg, 2002, pp. 1-16.

[8] Cui, L. et al. A new S-box structure named Affine-Power-Affine. International Journal of Innovative Computing, Information and Control, 3 (vol. 3), 2007, pp. 45-53.

[9] Yi, X. et al. A method for obtaining cryptographically strong 8×8 S-boxes. *GLOBECOM 97. IEEE Global Telecommunications Conference. Conference Record*, Phoenix, AZ, USA, November 1997, pp. 689-693.

[10] Tran, M.T. et al. Gray S-Box for advanced encryption standard. *2008 International Conference on Computational Intelligence and Security*, Suzhou, China, December 2008, pp. 253-258.

[11] Abuelyman, E.S. et al. An optimized implementation of the S-Box using residue of prime numbers. *International Journal of Computer Science and Network Security*, 4 (vol. 8), 2008, pp. 304-309.

[12] Liu, J. et al. An AES S-box to increase complexity and cryptographic analysis. *19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers)*, Taipei, Taiwan, March 2005, pp. 724-728.

[13] Kim, J. et al. Advanced differential-style cryptanalysis of the NSA's Skipjack block cipher. *Cryptologia*, 3 (vol. 33), 2009, pp. 246-270.

[14] Hussain, I. et al. A new algorithm to construct secure keys for AES. *International Journal of Contemporary Mathematical Sciences*, 26 (vol. 5), 2010, pp. 1263-1270.

[15] Qureshi, A., Shah, T. S-box on subgroup of Galois field based on linear fractional transformation. *Electronics Letters*, 9 (vol. 53), 2017, pp. 604-606.

[16] Shah, T., Qureshi, A. S-box on subgroup of Galois field. *Cryptography*, 2 (vol. 3), 2019, pp. 1-9.

[17] Hussain, I. et al. An efficient image encryption algorithm based on S_8 S-box transformation and NCA map. *Optics Communications*, 24 (vol. 285), 2012, pp. 4887-4890.

[18] Hussain, I. et al. Construction of S_8 Liu J S-boxes and their applications. *Computers & Mathematics with Applications*, 8 (vol. 64), 2012, pp. 2450-2458.

[19] Hussain, I. et al. S_8 affine-power-affine S-boxes and their applications. *Neural Computing and Applications*, 1 (vol. 21), 2012, pp. 377-383.

[20] Shah, T., Qureshi, A. Encrypting grayscale images using S_8 S-boxes chosen by logistic map. *International Journal of Computer Science and Information Security*, 4 (vol. 14), 2016, pp. 440-444.

[21] Shah, T. et al. Statistical analysis of S-box in image encryption applications based on majority logic criterion. *International Journal of the Physical Sciences*, 16 (vol. 6), 2011, pp. 4110-4127.

[22] Benjamini, J. et al. Balanced Boolean functions that can be evaluated so that every input bit is unlikely to be read, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, Baltimore, MD, USA, May 2005, pp. 244-250.

[23] Carlet, C. Nonlinearity of Boolean functions. In: van Tilborg H.C.A., Jajodia S. (eds) *Encyclopedia of Cryptography and Security*, Springer, Boston, MA, 2011.

[24] Ritter, T. "Measuring Boolean function nonlinearity by Walsh transform", http://www.ciphersbyritter.com/ARTS/MEASNONL.HTM, 1998.

[25] Matsui, M. Linear cryptanalysis method for DES cipher. In: Helleseth T. (eds) *Advances in Cryptology - EUROCRYPT '93. EUROCRYPT 1993*, Lecture Notes in Computer Science, vol 765. Springer, Berlin, Heidelberg, 1994, pp. 386-397.

[26] Biham, E., Shamir, A. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 3 (vol. 4), 1991, pp. 3-72.

[27] Webster, A.F., Tavares, S.E. On the design of S-boxes. In: Williams H.C. (eds) *Advances in Cryptology - CRYPTO '85 Proceedings. CRYPTO 1985*, Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg, 1986, pp. 523-534.

Information about the authors:

DR. TARIQ SHAH is working as a Professor and head of mathematical cryptography group at Quaid-i-Azam University Islamabad, Pakistan. He has introduced number of courses at postgraduate and graduate level in different institutions. He is founder of mathematical cryptography and designs different structures for the construction of nonlinear component of block ciphers and cryptosystems.

DR. AYESHA QURESHI has completed her PhD degree from Quaid-i-Azam University, Islamabad, Pakistan. Her areas of scientific research are Information security/ Cryptography and other related fields.

MUHAMMAD FAHAD KHAN is currently an Assistant Professor with Foundation University and a Ph.D. Scholar with the Department of Computer Science, Quaid-i-Azam University, Islamabad. He has authored more than 30 research papers. His research interests include steganography, cryptography, and multimedia communication.

Manuscript received on 04 March 2020