# A NOVEL APPROACH FOR GENERATING SMALL $8 \times 8$-BIT $S_4$ S-BOXES

Tariq SHAH[1], Ayesha QURESHI[2]

*In this manuscript, we present $8 \times 8$-bit $S_4$ S-boxes of order $16$ by using the action of symmetric group $S_4$ on the LSB's of the S-box generated from subgroup of Galois field. The inspiration is the improved performance parameters and the practical applications of existing $S_8$ S-boxes around Cryptography. The $S_8$ S-boxes use the permutations of symmetric group $S_8$ on the elements of the Galois field $GF(2^8)$. Whereas, in the proposed $S_4$ S-boxes, the symmetric group $S_4$ acts on the LSB's of the elements of the subgroup of Galois field. Consequently, $4!$ new $S_4$ S-boxes have been attained. The fact that the elements of these S-boxes are different from those of the subgroup produces ambiguity about the algebraic complexity of the new S-boxes. The obtained S-boxes have been inspected and equated with the original S-box by balance property, nonlinearity test, linear approximation probability test, differential approximation probability test and strict avalanche criteria. The aptness of the S-boxes to encryption applications has been determined and verified with majority logic criterion.*

**Keywords**: S-box on subgroup of Galois field, symmetric group $S_4$, balance property, nonlinearity test, linear approximation probability test, differential approximation probability test, strict avalanche criteria, majority logic criterion

## 1. Introduction

The 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 the evolution of attacks, the 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 cipher text. The design of this nonlinear component, called substitution box or S-box, is of great interest to cryptanalysts because the understanding of its functionality yields insight into the encryption process and its characteristics.

[1] Prof., Dept. of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan, e-mail: stariqshah@gmail.com

[2] Dept. of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan, e-mail: ayesha.qureshi6@gmail.com

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 [17]. 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 criteria and least linear and differential approximation probabilities etc. 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 [6]. 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 [7, 12]. In literature, almost all S-boxes are generally synthesized over finite Galois fields [1, 5, 6, 8, 9, 10, 18, 19 etc.]. Though, Shah et al. has set up an erection technique of S-boxes through the multiplicative cyclic subgroup $G_s$ of group of units of the Galois rings [16]. In [15], the authors presented a novel construction scheme of S-boxes based on the elements of subgroups of multiplicative groups of units of the commutative finite chain rings of type $\frac{\mathbb{F}_2[u]}{\langle u^k \rangle}$, where $2 \leq k \leq 8$. Later, we shifted the structure to the subgroup of multiplicative group of Galois field and the S-boxes are constructed on the elements subgroup of order15 adjoining zero. In the continuation of this study, we will perform the action of symmetric group of permutations on the S-box and will go to the analysis of its behavior.

Rest of the paper is organized as follows: In section 2, the algebraic expression of S-box on subgroup of Galois field is presented. In section 3, we will explain construction mechanism of new S-boxes. Section 4 gives the analyses of these S-boxes. Conclusions are presented in section 5.

## 2. Algebraic expression of S-box on subgroup of Galois field

In our earlier research, an S-box has been constructed based on the elements of the subgroup of the multiplicative group (say $H$) of finite Galois field. The structure of this S-box can be represented by the following equation:

$$S(x) = p \circ q(x) \tag{1}$$

In this expression, $p$ represents the inversion function and $q$ denotes the affine function of certain kind, defined on the subgroup of Galois field $GF(2^n)$. The construction with this method yields robust algebraic complexity and keeps desirable cryptographic characteristics. The elements of the S-box on subgroup of Galois field $GF(2^8)$, constructed by (1), and the corresponding inverse S-box is given in Table 1 and Table 2 respectively. In the later study, we will name the S-box on subgroup of Galois field as S-box (1) or small $8 \times 8$ S-box.

*Table 1*

**Small $8 \times 8$ S-box**

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

*Table 2*

**Inverse S-box**

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

## 3. Construction of $8 \times 8$-bit $S_4$ S-boxes of Order 16

The application of $S_n$ permutation on the existing elements of an S-box in $GF(2^n)$ creates $n!$ distinct $S_n$ S-boxes in $GF(2^n)$. The mathematical representation of the $S_n$ transformation process is given as,

$$f : S_n \times S-box \to S_n\ S-box \tag{2}$$

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

$$\pi_i\left(S-box(1)\right) = S_8\ S-box_i \tag{3}$$

***Example:*** An example of the small $S_8$ S-box obtained by applying the permutation $(8,7,6,5,4,3,2,1) \in S_8$ on the elements of S-box (1) is given in Table 3. The main characteristic of the S-box in Table 1 due to which the both transformations in (4) are possible is that the elements of the S-box owns distinct LSB's.

*Table 3*

**An example of small $S_8$ S-box**

| LSB's | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 162 | 187 | 59 |
| 1 | 235 | 73 | 242 | 201 |
| 2 | 34 | 107 | 153 | 80 |
| 3 | 114 | 25 | 128 | 208 |

But in Table 3, the action of permutation of $S_8$ on S-box (1) abolishes this property. Thus, second part of the transformation cannot be completed. The comprehensive procedure will be enlightened in the succeeding section.

$$x \in GF\left(2^8\right) \xrightarrow{S-box} y \in GF\left(2^8\right) \xrightarrow{S-box} x \in GF\left(2^8\right) \quad (4)$$

This matter has been fixed by the application of $S_4$ permutation on the LSB's of the elements of the S-box on subgroup of Galois field and $4!$ new distinct $8 \times 8$-bit $S_4$ S-boxes have been obtained. The mathematical representation of the $S_4$ transformation process is given as,

$$g: S_4 \times LSBs\,of\ S-box \rightarrow S_4\,S-box \quad (5)$$

If $S_4 = \{\sigma_j : j = 1, 2, 3, ..., 4!\}$, then according to the transformation (5) , $4!$ New $8 \times 8$ $S_4$ S-boxes are obtained from S-box (1) with the following procedure,

$$\sigma_j\left(LSBs\,of\ S-box(1)\right) = 8 \times 8 - bit\ S_4\ S-box_j \quad (6)$$

***Example:*** An example of the $8 \times 8$ $S_4$ S-box obtained by the action of permutation $(4,3,2,1) \in S_4$ on the LSB's of the elements of S-box (1) is given in Table 4 and the corresponding inverse S-box is specified in Table 5.

*Table 4*

**An example of $8 \times 8$ $S_4$ S-box**

| LSB's | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| **0** | 145 | 79 | 153 | 148 |
| **1** | 13 | 0 | 156 | 214 |
| **2** | 71 | 5 | 66 | 219 |
| **3** | 222 | 74 | 8 | 211 |

*Table 5*

**Inverse $8 \times 8$ $S_4$ S-box**

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

## 4. Analysis of new S-boxes

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

### 4.1 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 [2]. 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 4 is a set of $8$ Boolean vectors of size $16$. The truth tables of these vectors, say $f_0, f_1, f_2, \dots, f_7 : H \cup \{0\} \to \{0,1\}$, 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 subgroup of Galois field 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 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 152 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |
| 78 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 10 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 153 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| 214 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 68 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 147 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 79 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 146 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 215 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| 220 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 221 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 69 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |

### 4.2 Nonlinearity Test

The security of cryptographic transformations depends on the nonlinearity of substitutions. The nonlinearity of:

$f \in \{B_n | B_n \text{ is a Boolean function with } n \text{ variables}\}$ is the minimum distance between $f$ and the set of all affine functions $A_n$ [4]. i,e,.

$$NL(f) = \min_{h \in A_n} d(f, h) \tag{7}$$

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) [13]. It can be perceived from Table 7 that the action of symmetric group $S_4$ on S-box (1) 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 |
|---|---|---|---|---|---|---|---|---|---|
| Small $8 \times 8$ S-box | 4 | 4 | 0 | 4 | 2 | 4 | 4 | 4 | 3.25 |
| $8 \times 8$ $S_4$ S-box | 4 | 4 | 0 | 4 | 4 | 4 | 4 | 2 | 3.25 |

### 4.3 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 $S: GF\left(2^m\right) \to GF\left(2^n\right)$ is denoted and defined as:

$$LP_S = \max_{\Gamma x, \Gamma y \neq 0} \left| \frac{\#\left\{x \in GF\left(2^m\right) : x \cdot \Gamma x = f\left(x\right) \cdot \Gamma y\right\}}{2^m} - \frac{1}{2} \right|, \tag{8}$$

where $\Gamma x$ and $\Gamma y$ are the bit-masks to the parity of the input and output bits respectively and '.' denotes the 'bitwise and' operation [11]. The proposed small $8 \times 8$ S-box exhibits *LP* with a value of 0.125, which is the maximum linear probability of the 8-bit S-box. Whereas, for $8 \times 8$ $S_4$ S-box the value of *LP* is zero.

### 4.4 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 $S: GF(2^m) \to GF(2^n)$ is denoted and defined as :

$$DP_S = \max_{\Delta x \neq 0, \Delta y} \left( \frac{\#\left\{x \in GF\left(2^m\right) \middle| S\left(x\right) \oplus S\left(x \oplus \Delta x\right) = \Delta y\right\}}{2^m} \right) \tag{9}$$

where, $\Delta x \in GF(2^m)$ and $\Delta y \in GF(2^n)$ are differentials at the input and output respectively [3]. 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 $8 \times 8$ $S_4$ S-box by applying the input and output differentials are given in Table 8. The maximum of the matrix is $0.25$, showing that $DP(8 \times 8\ S_4\ S-box = 0.25)$, which coincides the optimal differential bound of $4 \times 4$ S-boxes and of small $8 \times 8$ S-box.

*Table 8*

**$DP$ of the most probable output XOR for $8 \times 8\ S_4$ 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 | --- |

### 4.5 Strict avalanche criterion

The strict avalanche criterion, introduced by Webster and Tavares in [20], 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 $f_n: GF(2^n) \rightarrow \{0,1\}$ is said to fulfill this criterion if, whenever a single input bit is complemented, each of the output bits changes with a $50\%$ probability. Mathematically,

$$\sum_{i=0}^{2^n-1} f_n(v_i) \oplus f_n(v_i \oplus \alpha) = 2^{n-1} \tag{10}$$

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 |
|---|---|---|---|---|---|---|---|---|---|
| Small $8 \times 8$ S-box | 0.5 | 0.5 | 0 | 0.5 | 0.5 | 0.5 | 0.5 | 0.75 | 0.4688 |
| $8 \times 8\ S_4$ S-box | 0.5 | 0.5 | 0 | 0.5 | 0.75 | 0.5 | 0.5 | 0.5 | 0.4688 |

### 4.6 Majority logic criterion

The objective of this section is to examine the results of correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis and mean of absolute deviation (MAD) analysis and decide by using majority logic criterion, the best S-box candidate. Majority logic criterion is stated as: Let there are $n$ S-boxes and $I_1, I_2, \dots, I_n$ be the encrypted images using S-boxes $S_1, S_2, \dots, S_n$ respectively, then S-box $S_j$ is considered better than $S_k$ for $j = \{1,2,\dots,n\}$ and $k \in \{1,2,\dots,n\} \setminus \{j\}$ if

- Amount of correlation, homogeneity and energy for $I_j$ is smaller than that of $I_k$.
- Amount of entropy, contrast and MAD for $I_j$ is greater than that of $I_k$. [14]

The process of encryption includes byte sub step. The leftmost two LSB's of the input pixel of the plain image are used as row index whereas the rightmost two LSB's are used as column index to select an 8-bit S-box value. LSB's of the S-box value are taken as MSB's of the output pixel and MSB's of the input pixel are taken as LSB's of the output pixel. In this way, all the pixels are substituted to encrypt the whole image. In the decryption operation, the leftmost two MSB's of the input pixel of the encrypted image are used as row index and the rightmost two MSB's are used as column index to select an 8-bit value from the corresponding inverse S-box. LSB's of the S-box value are taken as LSB's of the output pixel and LSB's of the input pixel are taken as MSB's of the output pixel.

Figure 1(a) depicts the standard grayscale image of Lena(.png), of size 512×512 pixels, (b) - (e) are the encrypted images using AES S-box, $S_8$ AES, small $8 \times 8$ S-box and $8 \times 8$ $S_4$ S-box respectively. The visual analysis is revealing that the $8 \times 8$ $S_4$ 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 10. It is observed from the results of statistical analyses that the $8 \times 8$ $S_4$ S-box improves the results for MLC. In figure 2, the encryption quality has been shown by means of histograms of plain image and the encrypted images.

Observations from Table 10:

Correlation of: AES S-box $<$ **$8 \times 8$ $S_4$ S-box** $<$ Small $8 \times 8$ S-box $<$ $S_8$ AES S-box

Homogeneity of: Small $8 \times 8$ S-box $<$ **$8 \times 8$ $S_4$ S-box** $<$ AES S-box $<$ $S_8$ AES S-box

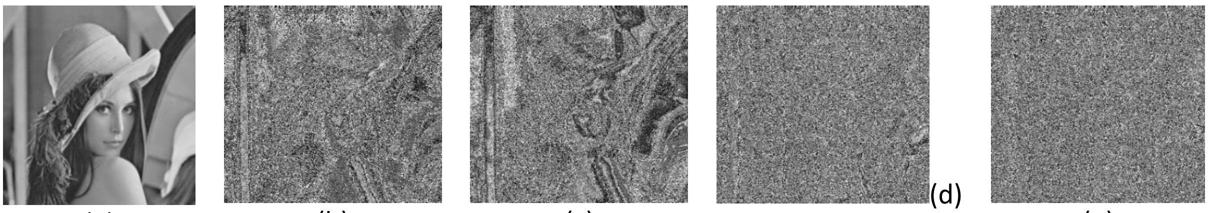
Energy of: Small $8 \times 8$ S-box $<$ **$8 \times 8$ $S_4$ S-box** $<$ AES S-box $<$ $S_8$ AES S-box

And,

Entropy of: AES S-box $=$ **$8 \times 8$ $S_4$ S-box** $=$ Small $8 \times 8$ S-box $=$ $S_8$ AES S-box

Contrast of: AES S-box $>$ **$8 \times 8$ $S_4$ S-box** $>$ Small $8 \times 8$ S-box $>$ $S_8$ AES S-box

MAD of: AES S-box $>$ **$8 \times 8$ $S_4$ S-box** $>$ $S_8$ AES S-box $>$ Small $8 \times 8$ S-box



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

Fig. 1. (a) Plain image, (b) Encrypted image using AES S-box, (c) Encrypted image using $S_8$ AES S-box, (d) Encrypted image using small $8 \times 8$ S-box, (e) Encrypted image using $8 \times 8$ $S_4$ S-box

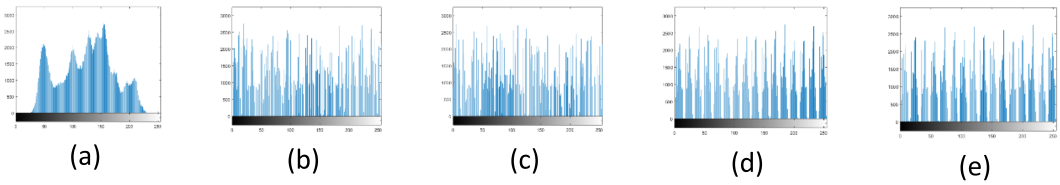


Fig. 2. Histograms (a) Plain image, (b) Encrypted image using AES S-box, (c) Encrypted image using $S_8$ AES S-box, (d) Encrypted image using small $8 \times 8$ S-box, (e) Encrypted image using $8 \times 8$ $S_4$ S-box.

*Table 10*

**Results of statistical analyses used by the majority logic criterion**

| Analyses | Plain image | AES S-box | $S_8$ AES S-box | Small $8 \times 8$ S-box | $8 \times 8$ $S_4$ S-box |
|---|---|---|---|---|---|
| Entropy | 7.4451 | 7.4451 | 7.4451 | 7.4451 | 7.4451 |
| Contrast | 0.2288 | 10.5914 | 9.2531 | 10.3525 | 10.5013 |
| Correlation | 0.9503 | 0.0666 | 0.1216 | 0.0175 | 0.0117 |
| Energy | 0.1318 | 0.0172 | 0.0174 | 0.0160 | 0.0161 |
| Homogeneity | 0.9058 | 0.4352 | 0.4452 | 0.4054 | 0.4070 |
| MAD | 19.8828 | 33.9488 | 32.0243 | 31.9990 | 32.1252 |

## 5. Conclusions

In literature, the idea of generation of new S-boxes by the action of symmetric group of permutations $S_8$ on the elements of $8 \times 8$ S-boxes has been practiced by the researchers. But when this idea is applied on the constructions over algebraic substructure, we come 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 performing the action of symmetric group of permutations $S_4$ and obtained S-boxes with reasonable complexity and confusion creating capability.

## R E F E R E N C E S

[1] *E. S. Abuelyman, A. S. Alsehibani*, "An optimized implementation of the S-Box using residue of prime numbers", International Journal of Computer Science and Network Security, **8**(4) (2008) 304-309.

[2] *I. Benjamini, O. Schramm, D. B. Wilson*, "Balanced Boolean functions that can be evaluated so that every input bit is unlikely to be read", Proceedings of the thirty-seventh annual ACM symposium on Theory of computing, May 22-24, 2005, Baltimore, MD, USA.

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

[4] *C. Carlet*, "Nonlinearity of Boolean functions", in: *C. A. van Tilborg, S. Jajodia* (Eds.), Encyclopedia of Cryptography and Security, 2nd Edition, Springer US (2011) pp. 848-849.

[5] *L. Cui, Y. Cao*, "A new S-box structure named Affine-Power-Affine", International Journal of Innovative Computing, Information and Control, **3**(3) (2007) 751-759.

[6] *J. Daemen, V. Rijmen*, “The Design of Rijndael, AES - The Advanced Encryption Standard”, Springer-Verlag, 2002.
[7] *N. Ferguson, R. Schroeppel, D. Whiting*, “A simple algebraic representation of Rijndael”, in: *S. Vaudenay, Amr M. Youssef* (Eds.), Selected Areas in Cryptography SAC’01, Lecture Notes in Computer Science, **vol. 2259**, Springer, Berlin, Heidelberg (2001) pp. 103-111.
[8] *I. Hussain, T. Shah, H. Mehmood*, “A new algorithm to construct secure keys for AES”, International Journal of Contemporary Mathematical Sciences, **5**(26) (2010) 1263-1270.
[9] *J. Kim, R. C. W. Phan*, “Advanced differential-style cryptanalysis of the NSA’s Skipjack block cipher”, Cryptologia, **33**(3) (2009) 246-270.
[10] *J. Lui, B. Wai, X. Cheng, X. Wang*, “An AES S-box to increase complexity and cryptographic analysis”, Proceedings of the $19^{th}$ International Conference on Advanced Information Networking and Applications - Volume 01, March 25-30, 2005, Washington, DC, USA.
[11] *M. Matsui*, “Linear cryptanalysis method of DES cipher”, in: *T. Helleseth* (Eds.), Advances in Cryptology - EUROCRYPT’ 93, Lecture Notes in Computer Science, **vol. 765**, Springer, Berlin, Heidelberg, 2001, pp. 386-397
[12] *S. Murphy, M. J. Robshaw*, “Essential algebraic structure within the AES”, in: *M. Yung* (Eds.), Advances in Cryptology – Crypto 2002, Lecture Notes in Computer Science, **vol. 2442**, Springer, Heidelberg (2002) pp. 1-16.
[13] *T. Ritter*, “Measuring Boolean function nonlinearity by Walsh transform”, http://www.ciphersbyritter.com/ARTS/MEASNONL.HTM, 1998.
[14] *T. Shah, I. Hussain, M. A. Gondal, H. Mahmood*, “Statistical analysis of S-box in image encryption applications based on majority logic criterion”, International Journal of the Physical Sciences, **6**(16) (2011) 4110-4127.
[15] *T. Shah, S. Jahangir, A. A. de Andrade*, “Design of new $4 \times 4$ S-box from finite commutative chain rings”, Computational and Applied Mathematics, (2015) 1-15.
[16] *T. Shah, A. Qamar, I. Hussain*, “Substitution box on maximal cyclic subgroup of units of a Galois ring”, Zeitschrift fur Naturforschung A, **68**(8-9) (2013) 567-572.
[17] *C. E. Shannon*, “Communication theory of secrecy systems”, The Bell System Technical Journal, **28**(4) (1949) 656-715.
[18] *X. Yi, S. Xin Cheng, X. Hu You, K. Yan Lam*, “A method for obtaining cryptographically strong $8 \times 8$ S-boxes”, International Conference on Information Networking and Applications, **2** (3) (2002) 14-20.
[19] *M. T. Tran, D. K. Bui and A. D. Doung*, “Gray S-box for Advanced Encryption Standard”, Proceedings of the 2008 International Conference on Computational Intelligence and Security - Volume 01, December 13-17, 2008, Washington, DC, USA.
[20] *A. F. Webster, S. E. Tavares*, “On the design of S-boxes”, in: *H. C. Williams* (Eds.), Advances in Cryptology - Crypto '85, Lecture Notes in Computer Science, **vol. 218**, Springer, Berlin, Heidelberg (1985) pp. 523–534.