A Novel Method for Designing Substitution Boxes Based on Mobius Group

Bilal Arshad a, Nasir Siddiqui a, Zamir Hussainb

a. Department of Basic Sciences, University of Engineering and Technology, Taxila, Pakistan.
b. Department of Mathematics, University of Wah, Pakistan.

bilalarshad689@gmail.com, nasir.siddiqui@uettaxila.edu.pk, zamir.hussain@uow.edu.pk

Abstract

It is as of now realized that the use of web in the present period is expanding very quickly, numerous users are sharing open and private data over web/internet. They need to ensure security of information. Encryption is one of the most significant viewpoint which is helpful to verify secret data. In encryption, cryptography assume a significant role. There are many algorithms accessible to shield information from unapproved access. In this work, we will use the strategy for cryptography to build up an algorithm which is increasingly viable for correspondence and information trade. In this study, we use a procedure to assemble new substitution boxes (S-boxes) parallel to coset diagram for the action of Mobius group [1] on projective line \( PL(F_7) \) over \( GF(2^8) \). Afterward, the analyses of constructed S-boxes are performed on the basis of algebraic and statistical analysis.

Keywords: Substitution box (S-box), Galois Field \( GF(2^8) \), Mobius Group, Nonlinearity, Linear and Differential Probability, Majority Logic Creation (MLC).

1. Introduction

The term cryptography means the encryption of e-mails, encrypted access to websites, smart cards for banking applications. Cryptography is tightly tied up with modern electronic communication. However, cryptography is an old business. Encryption of a message ensures that the meaning is concealed in it so that someone who reads the message cannot understand any of it unless people crack the message [2]. The substitution box plays a key role in maintaining safe communication. Shannon proposed the idea of a substitution box in 1949 [3]. Substitution box plays a major role in creating uncertainty in data. Several algorithms are available in the literature for construction S-boxes, such as “Data Encryption Standard (DES), Advanced Encryption Standard (AES), Affine Power Affine (APA), Gray, Skipjack, Xyi, and Residue Prime (RP)” S-boxes. A brief description of some of these algorithms is given. The National Bureau Standards (NBS) requested the American company in 1974 to create a cryptosystem that could be used by the government as a standard in unclassified U.S. applications. A system named 'LUCIFER' was designed by IBM. In 1977, this system was altered and rearranged to become DES. DES was made readily available on a speedy processor. This made it better suited for use in large networks of communication. The complete DES program was made public at the time of its launch. DES has been incredibly popular, and remains the most commonly used cryptosystem ever. The data encryption standard has been treated as a standard for symmetrical key encryption, but the biggest downside was that the key length was very small and can easily be hacked [4]. To overcome this problem, in 1997, the
National Institute of Standards and Technology (NIST) launched a contest to find a new symmetric cryptographic algorithm to replace the DES, which will be called the Advanced Encryption Standard. In October 2000, NIST finally revealed that "Rijndael" is the Advanced Encryption Standard (AES) algorithm, its software of two Belgian cryptographers, "Joan Daemen" and "Vincent Rijmen." AES is the most widely used symmetric key algorithm at present [5].

Different researchers have adopted various techniques for constructing S-boxes [6, 7, 8, 9], and a variety of methods have been developed to evaluate the statistical and algebraic structure of S-boxes. [10, 11, 12, 13]. In this research, we use a technique for constructing new S-boxes using coset diagram for Mobius group $M = \langle x, y: x^2 = y^6 = 1 \rangle$ on $PL(F_7)$. After the action of group on $PL(F_7)$ we then applied this on Galois Field $GF(2^8)$ to obtained new S-boxes. Afterward, the analyses of constructed S-boxes is performed on the basis of algebraic and statistical analysis.

This document is organized as follows: The construction process of the new S-boxes is described in Section 2. Analyses of the proposed S-boxes are investigated in section 3. These analyses include nonlinearity (NL), strict avalanche criterion (SAC), bit independence criterion (BIC), linear approximation probability (LAP), and differential approximation probability (DAP). We analyze the protection of the proposed S-boxes in section 4 with the majority logic criterion (MLC). The conclusion of our proposed work is shown in section 5.

2. Construction Process of Substitution Box

For the manufacturing of novel S-boxes, we shape an adjacency matrix relating to the coset diagram for the action of Mobius group on $PL(F_7)$. The Mobius group is defined as $M = \langle x, y: x^2 = y^6 = 1 \rangle$. For the action of Mobius group $M$ on $PL(F_7)$ we use the following linear fractional transformation $(t)x = -1/3t$ and $(t)y = -1/3(t + 1)$ [1, 14, 15]. $PL$ is the projective line over finite field $F_7$, i.e. $PL(F_7) = F_7 \cup \infty = \{0, 1, 2, 3, 4, 5, 6, \infty\}$. This action yields a permutation group generated by $\bar{x}$ and $\bar{y}$.

$$\bar{x} = (0 \ \infty \ 1 \ 2 \ 3 \ 4 \ 5 \ 6)$$

$$\bar{y} = (0 \ 2 \ 3 \ 4 \ 6 \ \infty \ 1 \ 5)$$

We draw coset diagram by using these permutation. Here $\bar{x}$ has order 2 so the generator $\bar{x}$ is denoted by black edges and bulky black dots denotes the static points of $\bar{x}$ and $\bar{y}$ has order 6, so the generator $\bar{y}$ is represented by blue color which is hexagon whose vertices permuted anticlockwise and the static points of $\bar{y}$ are indicated by bulky blue dots on the coset diagram as displayed in figure.
Figure 1: Coset diagram for modular group on $PL(F_7)$

Presently we structure an adjacency matrix from the above coset graph, for instance assemble an adjacency matrix related to the above coset diagram with the vertices labeled by $0, 1, 2, 3, 4, 5, 6, \infty$. When we perform an action of adjacency matrix on $GF(2^8)$ we do not obtained our desire results. To obtain a unique result we have developed a specific transformation $S(t_n) = At_n + t_{n+128(mod256)}$ named as “Affine Transformation”. This transformation give us different S-boxes having different results. The obtained S-box is shown in Table 1.

Table 1: Proposed S-box in the form of 16x16 matrix

|  54 |  19 | 108 |  80 | 227 | 250 |  24 |  73 |  1 | 222 |  87 | 119 | 229 |  59 | 113 | 247 |
|  18 |  16 |  28 |  40 |  82 | 216 | 173 |  84 | 220 |  63 | 212 | 137 | 208 |  35 | 136 |    |
| 122 |  75 |  23 | 254 |  64 |  51 |  37 |  69 |  4 |  65 | 138 | 225 | 121 |  50 | 102 | 150 |
| 228 | 199 | 226 | 126 | 191 |  90 | 215 | 168 | 158 | 145 |  5 | 182 | 201 | 106 |  92 | 245 |
| 213 |  99 |  81 | 169 | 234 |  80 |  79 |  45 | 142 |  85 | 202 |  6 | 238 |  13 | 200 |  98 |
|  53 | 120 | 198 | 123 | 217 | 179 |  88 | 152 | 161 | 189 | 230 | 232 | 111 |  31 | 104 |  43 |
| 167 | 131 | 196 | 205 | 195 | 139 |  26 | 103 | 146 | 151 |  96 | 171 | 233 |  32 | 224 |  61 |
| 204 |  9  | 177 | 255 | 242 |  8 |  67 | 125 | 101 | 153 |  52 | 149 |  3 | 109 | 155 |  83 |
|  22 | 129 |  38 | 164 | 127 | 134 | 172 | 124 | 170 |  62 | 236 | 251 | 154 | 194 |  10 | 184 |
| 133 | 249 | 156 | 235 | 132 | 185 | 160 |  71 | 105 | 188 |  33 | 143 |  12 |  86 |  14 |  78 |
| 221 | 192 | 239 |  17 | 207 |  57 | 203 | 248 |  30 | 140 |  74 |  46 | 187 |  91 | 128 | 244 |
|  39 |  68 | 243 | 181 |  7 | 159 | 118 | 165 |  90 | 246 |  60 | 107 | 117 | 240 | 148 |  29 |
| 147 |  97 | 110 |  94 | 253 | 241 | 162 | 176 |  93 |  76 |  47 | 218 | 174 |  70 |  25 | 163 |
|  58 | 214 | 183 | 175 | 252 |  77 |  42 | 186 |  2 | 15 | 178 | 211 |  21 |  44 | 55 | 166 |
| 157 | 114 | 141 | 209 |  34 | 237 | 193 |  95 |  48 |  56 | 112 |  72 | 219 |  36 | 144 |  0 |
|  49 | 223 | 116 | 231 | 100 | 130 | 115 |  89 | 210 |  41 | 206 | 135 |  66 |  20 |  11 |  27 |

3. Algebraic Analysis

In this segment, we narrate our S-boxes with some generally used evaluation techniques includes nonlinearity, strict avalanche criterion, differential approximation probability, bit independent criterion, linear approximation probability.

3.1 Nonlinearity (NL)

Pieprzyk and Finkelstein first introduced the concept of nonlinearity in 1988 [16]. The nonlinearity of a Boolean function can be described as the distance between the function and the set of affine functions. We may say in another sentence that nonlinearity is the number of bits that should be changed to achieve the nearest affine function in a Boolean function's truth table.
The average value for nonlinearity is 120. The nonlinearity over the \( GF(2^8) \) of the S-box can be defined as,

\[
N(f) = 2^{n-1} - 2^{\frac{n}{2}-1}
\]

The highest nonlinearity is 110, the minimum nonlinearity is 106, and average nonlinearity is 107.25. Table 2 shows that the non-linearity of the proposed S-box is almost equal to that of the famous S-boxes when compared with various well-known S-boxes, and much better than that of the most popular S-boxes.

### Table 2: Non-linearity of the various S-boxes.

| S-boxes             | \( f_0 \) | \( f_1 \) | \( f_2 \) | \( f_3 \) | \( f_4 \) | \( f_5 \) | \( f_6 \) | \( f_7 \) | Avg   |
|---------------------|----------|----------|----------|----------|----------|----------|----------|----------|-------|
| Proposed S-box      | 108      | 110      | 108      | 106      | 108      | 106      | 106      | 106      | 107.25|
| Skipjack S-box [17] | 104      | 104      | 108      | 108      | 104      | 104      | 106      | 106      | 105.75|
| Xyi S-box [18]      | 106      | 104      | 104      | 106      | 104      | 106      | 104      | 106      | 105   |
| Residue Prime [19]  | 94       | 100      | 104      | 104      | 102      | 100      | 98       | 94       | 99.5  |
| Tang et al. [20]    | 100      | 103      | 104      | 104      | 105      | 105      | 106      | 109      | 104.5 |
| Chen et al. [21]    | 100      | 102      | 103      | 104      | 106      | 106      | 108      | 104      | 104.3 |
| Belazi et al. [22]  | 106      | 106      | 106      | 104      | 108      | 102      | 106      | 104      | 105.25|
| Alkhaldi et al. [23]| 108      | 104      | 106      | 106      | 106      | 98       | 104      | 108      | 104   |
| Khan et al. [24]    | 102      | 108      | 106      | 102      | 106      | 106      | 106      | 98       | 104.25|

### 3.2 Strict Avalanche Criterion (SAC)

The strict avalanche criterion depends on changes in input and output bit rates. An S-box meets strict avalanche criterion when a single bit shifts the input, resulting in a shift of half the output bits, an S-box meets the strict avalanche criterion [25].

### Table 3: The suggested S-box’s strict avalanche criterion.

|        | 0.5468 | 0.5312 | 0.4687 | 0.5156 | 0.5000 | 0.5000 | 0.4531 | 0.5000 |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 0.5000 | 0.4843 | 0.5156 | 0.4531 | 0.5000 | 0.5312 | 0.4843 | 0.5000 | 0.5468 |
| 0.5312 | 0.5156 | 0.5156 | 0.5000 | 0.5312 | 0.4843 | 0.5000 | 0.5000 | 0.5468 |
| 0.4843 | 0.5000 | 0.5000 | 0.5000 | 0.4687 | 0.4843 | 0.5468 | 0.5312 |
| 0.5156 | 0.4531 | 0.5312 | 0.5312 | 0.5156 | 0.5000 | 0.4375 | 0.5312 |
| 0.4531 | 0.4687 | 0.5312 | 0.4843 | 0.5312 | 0.5468 | 0.5000 | 0.4375 |
| 0.4843 | 0.5468 | 0.5156 | 0.5312 | 0.5000 | 0.5000 | 0.4843 | 0.4531 |
| 0.5000 | 0.5000 | 0.5468 | 0.4843 | 0.5312 | 0.4375 | 0.5156 | 0.4843 |

Table 3 shows the outcomes of suggested S-box. The suggested S-box’s strict avalanche criterion analysis is, the maximum value is 0.5468, the minimum is 0.4375 and the average value is 0.5017.

### 3.3 Bit Independent Criterion (BIC)

The bit independent criterion for the first time introduced by “Webstar and Tavares” in [26], which is a desirable cryptographic property. It is used to analyze nonlinear transformation behavior by altering input bits which change at the level of output bits. This implies that, for a
given vector set generated by the complement of a single plaintext bit, the entire avalanche variable must be pair-independent [25]. Table 4 shows the BIC output of the proposed S-box for nonlinearity, and Table 5 shows the SAC of the BIC. It can be observed that the BIC of the proposed S-box has an average value 107.

Table No 4: Non-linearity of bit independence criterion of the proposed S-box.

|     | 102 | 108 | 106 | 110 | 106 | 104 | 106 |
|-----|-----|-----|-----|-----|-----|-----|-----|
| 102 |     |     |     |     |     |     |     |
| 108 |     | 110 |     |     | 108 |     | 110 |
| 106 | 106 |     |     |     | 104 | 108 | 106 |
| 110 | 106 | 110 |     |     | 110 | 110 | 106 |
| 106 | 106 | 108 | 104 | 110 |     | 106 | 104 |
| 104 | 108 | 110 | 108 | 110 | 106 |     | 106 |
| 106 | 110 | 106 | 104 | 106 | 104 | 106 |     |

Table No 5: Strict avalanche creation of bit independent criterion.

|     | 0.4980 | 0.4980 | 0.5097 | 0.4980 | 0.5019 | 0.4882 | 0.4941 |
|-----|--------|--------|--------|--------|--------|--------|--------|
| 0.4980 |     | 0.4824 | 0.5195 | 0.4941 | 0.5156 | 0.5136 | 0.4863 |
| 0.4980 | 0.4824 |     | 0.4746 | 0.5019 | 0.5136 | 0.4804 | 0.5058 |
| 0.5097 | 0.5195 | 0.4746 |     | 0.4824 | 0.4960 | 0.4980 | 0.4824 |
| 0.4980 | 0.4941 | 0.5019 | 0.4824 |     | 0.5039 | 0.5039 | 0.4785 |
| 0.5019 | 0.5156 | 0.5136 | 0.4960 | 0.5039 |     | 0.5234 | 0.5039 |
| 0.4882 | 0.5136 | 0.4804 | 0.4980 | 0.5039 | 0.5234 |     | 0.4941 |
| 0.4941 | 0.4863 | 0.5058 | 0.4824 | 0.4785 | 0.5039 | 0.4941 |     |

3.4 Differential Approximation Probability (DAP)

Throughout the encryption of private information, personal data or documents, the substitution box is called the non-linear constituent. The substitution box recommends differential consistency in optimal situations. $\Delta x$ is known to be a differential input and $\Delta y$ may be indicated as a differential in output. An input differential $\Delta x$ uniquely map to an output differential $\Delta y$.

The differential approximation probability of a given S-boxes i.e. DP is defined as,

$$DP^S(\Delta x \rightarrow \Delta y) = \frac{\#\{x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^m}$$

As shown in Table 6, the average value of the differential approximation probability for the designed S-box is 6.
Table 6: Differential approximation probability of the planned S-box.

|   | 0.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
|---|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| 4.0, 4.0, 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |

3.5 Linear Approximation Probability (LAP)

It is regarded as the greatest value of an event disparity. The input bits and output bits will be given the same uniformity. The \(i^{th}\) bit is independently measured at the input stage and its results are determined in the output bits. In [27], the linear probability for a given S-box is defined as

\[
LP = \max_{\tau_x, \tau_y} \left| \frac{\#\{x|\tau_x = S(x), \tau_y\} - \frac{1}{2^n}}{2^n} \right|
\]

Here \(2^n\) displays the components of the built S-box \(\tau_x, \tau_y\), the two marks used for the parity of the input bits and the output bits. \(X\) contains all possible inputs. The newly proposed S-box's linear approximation probability is 0.1093, which is better than the Xyi and Residue prime S-boxes.

**Complete Comparison**

Table 7 affords a complete assessment of our proposed S-boxes’s NL, SAC, BIC, DAP and LAP with different familiar S-boxes. Figure 2 suggests a graphical illustration of NL, SAC, BIC, DAP and LAP of our recommended S-box with some famous S-boxes.
| S-boxes      | NL   | SAC  | BIC  | DAP | LAP  |
|-------------|------|------|------|-----|------|
| Proposed S-box | 107.25 | 0.501 | 107  | 6   | 0.109 |
| Ref. [28]    | 107.75 | 0.497 | 105  | 8   | 0.125 |
| Ref. [29]    | 109.25 | 0.501 | 104  | 8   | 0.093 |
| Ref. [30]    | 106.75 | 0.503 | 100  | 10  | 0.132 |
| Ref. [31]    | 106.75 | 0.494 | 98   | 10  | 0.125 |
| Ref. [32]    | 106.75 | 0.407 | 98   | 10  | 0.132 |
| Ref. [33]    | 105.25 | 0.499 | 104  | 10  | 0.132 |
| Ref. [34]    | 104.75 | 0.495 | 103  | 12  | 0.132 |
| Ref. [35]    | 105.87 | 0.497 | 103.67 | 10 | 0.128 |
| Ref. [36]    | 105.25 | 0.694 | 104.64 | 10 | 0.132 |
| Ref. [37]    | 100   | 0.481 | 101.93 | 16 | 0.179 |
| Ref. [38]    | 107   | 0.501 | 104.2 | 10  | 0.148 |
| Ref. [39]    | 106.75 | 0.503 | 103.64 | 12 | 0.148 |
| Ref. [40]    | 106   | 0.506 | 103  | 12  | 0.144 |
| Ref. [41]    | 102.3 | 0.483 | 101.57 | 14 | 0.167 |
| Ref. [41]    | 106.25 | 0.499 | 103.8 | 10  | 0.125 |
| Ref. [43]    | 106.5 | 0.504 | 104.14 | 10 | 0.132 |
Figure 3: Graphically representation of NL, SAC, BIC, DAP, LAP of our suggested S-box with few famous S-boxes

4. Majority Logic Criterion (MLC)

Right now, we're presenting a few valuable statistical analysis of the brand new and a few well-known S-boxes. We use the majority logic creation (MLC) in order to assess the efficacy of the suggested S-box in image encryption applications. Because of the rapid developments in digital image processing, it is very essential to secure computerized data from various
attacks. By the method of encryption, a distortion in the image is generated; the statistical properties must therefore be addressed. In order to obtain it, a variety of analyses including entropy, contrast, correlation, energy and homogeneity are used.

By means of entropy, the quantity of uncertainty is measured. The degree of entropy in an image is associated with the object arrangement. To measure randomness, entropy is used. Contrast analysis tests the capacity of an image to distinguish objects. On the contrary, a high level of security is required to guarantee solid encryption. Encrypted/scrambled image have higher contrast levels in view of randomness. Effectiveness of S-boxes images are assessed by contrast. The contrast value is zero in the case of a constant image. The statistical characteristics of an S-box can be test through correlation analysis. Via this test, the similarities between the pixel patterns of plain and encoded images are determined. In three distinct ways correlation analysis is carried out. The vertical, the horizontal and the diagonal formats are appointed for this reason. Energy analysis determines the energy measurement of a scrambled image while processed by different S-boxes. This move returns the total of the square elements in the GLCM. The proximity of the distribution of elements in the Grey Level Co-Occurrence Matrix (GLCM) to the GLCM diagonal can be calculated using homogeneity analysis.

The consequences of these research are shown in Table 8 in evaluation with the other well-known S-boxes. The original Lena, Pepper, Baboon and Cameraman images are shown in Figure 4. The result of image encryption with the suggested S-box is shown in Figure 5. In Figures 6, 7, 8, 9, histograms of the original and encrypted images of Lena, Pepper, Baboon and Cameraman are displayed.

| Images                  | Entropy  | Contrast | Correlation | Energy  | Homogeneity |
|-------------------------|----------|----------|-------------|---------|-------------|
| Plain image a           | 7.4545   | 0.4046   | 0.9114      | 0.1203  | 0.8762      |
| Plain image b           | 7.5989   | 0.4618   | 0.9200      | 0.9995  | 0.8692      |
| Plain image c           | 7.2572   | 0.9298   | 0.6980      | 0.0832  | 0.7324      |
| Plain image d           | 7.0911   | 0.6165   | 0.9189      | 0.1771  | 0.8840      |
| Encrypted image a       | 7.4545   | 8.3900   | 0.1564      | 0.0194  | 0.4824      |
| Encrypted image b       | 7.5989   | 9.0854   | 0.0571      | 0.0178  | 0.4619      |
| Encrypted image c       | 7.2572   | 9.7589   | 0.0159      | 0.0168  | 0.4061      |
| Encrypted image d       | 7.0909   | 9.6683   | 0.1597      | 0.0208  | 0.4963      |
| AES S-box [44]          | 7.2531   | 7.5509   | 0.0554      | 0.0202  | 0.4662      |
| APA S-box               | 7.2264   | 8.1195   | 0.1473      | 0.0183  | 0.4676      |
| Gray S-box [45]         | 7.2301   | 7.5283   | 0.0586      | 0.0203  | 0.4623      |
Figure 4: Original images of Lena, Pepper, Baboon, Cameraman

Figure 5: Encrypted images of Lena, Pepper, Baboon, Cameraman by proposed S-box

Figure 6: Histogram of (a) plan and (b) encrypted image of Lena
Figure 7: Histogram of (a) plan and (b) encrypted image of Pepper

Figure 8: Histogram of (a) plan and (b) encrypted image of Baboon

Figure 9: Histogram of plan and encrypted image of Cameraman
5. Conclusion

In this research, we use a methodology to create new S-boxes relating to coset diagram for the action of Mobius group on projective line $PL(F_7)$ over $GF(2^8)$ to obtained new S-boxes. Next, we analyzed the strength of our planned S-boxes with other notable established S-boxes existing in literature. To calculate the power of our proposed S-boxes, we use algebraic and statistical tests. The algebraic test involves nonlinearity, bit independence criterion, strict avalanche criterion, differential approximation probability, linear approximation probability. In the statistical test, we apply the Majority Logic Criterion (MLC) to assess the efficacy of the proposed S-box in application for image encryption. Statistical tests are “entropy, contrast, correlation, energy and homogeneity”. As our proposed S-box fulfill all the requirements of the analyses, and is taken into consideration as strong S-box for the secure communication. In the statistical test, we follow the Majority Logic Criterion (MLC) to decide the performance of the proposed S-box in application for image encryption. Entropy, contrast, correlation, energy and homogeneity are statistical tests. As our proposed S-box fulfill all of the analytical conditions, it's far taken into consideration an effective S-box for secure communication.

6. Declaration Statement

I would like to submit the manuscript entitled “A Novel Method for Designing Substitution Boxes Based on Mobius Group” by Bilal Arshad, Nasir Siddiqui, Zamir Hussain to be considered for publication as an original article in the Wireless Personal Communications. We declare that this manuscript is original, has not been published before and is not currently being considered for publication elsewhere.

6.1 Funding

There has been no significant financial support for this work.

6.2 Conflicts of Interest/Competing Interests

We know of no conflicts of interest associated with this publication.

6.3 Availability of Data and Material (data transparency)

The data that support the findings of this study are available from the corresponding author, Mr. Bilal Arshad, upon reasonable request.

6.4 Code Availability

Due to the nature of this research, participants of this study did not agree for their code to be shared publicly, so supporting code is not available.

6.5 Author’s Contributions

All authors have made equally contributions to the writing of this research paper.
7. References

[1] Q. Afzal, F. Afzal, “Golden Mean and the Action of Mobius Group M”, International Journal of Mathematics and Computational Science, Vol. 4, No. 4, pp. 124-127, ISSN: 2381-7011 (Print); ISSN: 2381-702X. 2018.

[2] K. Ruohonen, “Mathematical Cryptology”, Translation by J. Kangas and P. Coughlan, page 1, 2014.

[3] C. E. Shannon, “Communication Theory of Secrecy Systems,” Bell Labs Technical Journal, vol. 28, pp. 656–715, 1949.

[4] Mayes M. Hoobi, “Strong Triple Data Encryption Standard Algorithm using Nth Degree Truncated Polynomial Ring Unit”, Journal of Science, Vol. 58, No. 3C, pp: 1760-1771, 2017.

[5] A. Fathy, I.F. Tarrad, Hesham F.A. Hamed, A. I. Awad, “Advanced Encryption Standard Algorithm: Issues and Implementation Aspects”, AMLTA 2012, CCIS 322, 2012, pp. 516–523. C-Springer-Verlag Berlin Heidelberg 2012.

[6] A. Anees & Y. P. P. Chen, “Designing Secure Substitution Boxes Based on Permutation of Symmetric Group”, Neural Computing and Applications, 2019.

[7] I. Shahzad, Q. Mushtaq & A. Razaq, “Construction of New S-Box Using Action of Quotient of the Modular Group for Multimedia Security”, Security and Communication Networks, 1–13, 2019.

[8] T. Shah and A. Qureshi *, “S-Box on Subgroup of Galois Field”, Cryptography, 3(2), 13, 2019.

[9] U. Hayat, N. A. Azam, & M. Asif, “A Method of Generating 8 × 8 Substitution Boxes Based on Elliptic Curves”, Wireless Personal Communications, 101(1), 439–451, 2018.

[10] I. Hussain, T. Shah, M. A. Gondal & H. Mahmood, “A Novel Image Encryption Algorithm Based on Chaotic Maps and GF(2^8) Exponent Transformation”, Nonlinear Dynamics, 72(1-2), 399–406, 2013.

[11] J. Rosenthal, “A Polynomial Description of the Rijndael Advanced Encryption Standard”, Journal of Algebra and Its Applications, 02(02), 223–236, 2003.

[12] N. Ferguson, R. Schroeppel & D. Whiting, “A Simple Algebraic Representation of Rijndael”. Lecture Notes in Computer Science, 103–111, 2001.

[13] S. Murphy and M.J.B.Robshaw, “Essential Algebraic Structure With in the AES”, Information Security Group, Royal Holloway, University of London.

[14] F. Afzal, Q. Afzal1, M. Aslam Malik, “Quadratic Fields under the Action of Subgroups of M”, International Journal of Modeling and Optimization, 2013.

[15] M. A. Malik, S. M Husnine, A. Majeed, “Action of the Mobius group M =< x; y: x^2 = y^6 = 1 > on Certain Real Quadratic Fields”, Journal of Mathematics (ISSN 1016-2526), Vol. 44, pp. 31-37. 2012.

[16] J. Pieprzyk and G. Finkelstein, “Towards effective nonlinear cryptosystem design,” IEE Proceedings Part E Computers and Digital Techniques, vol. 135, no. 6, pp. 325–335, 1988.

[17] J. Kim* & R. C. W. Phan**, “Advanced Differential-Style Cryptanalysis of the NSA’s Skipjack Block Cipher”. Cryptologia, 33(3), 246-270. 2009.
[18] X. Yi, S. X. Cheng, X. H. You & K.Y. Lam, “A Method for Obtaining Cryptographically Strong $8 \times 8$ S-boxes”. In GLOBECOM 97. IEEE Global Telecommunications Conference. Conference Record (Vol. 2, pp. 689-693). IEEE. November.

[19] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal & U. Y. Bhatti, “Some Analysis of S-box Based on Residue of a Prime Number”. Proc Pak Acad Sci, 48(2), 111-115. 2011.

[20] G. Tang, X. Liao, and Y. Chen, “A novel method for designing S-boxes based on chaotic maps,” Chaos, Solitons & Fractals, vol. 23, no. 2, pp. 413–419, 2005.

[21] G. Chen, Y. Chen, and X. Liao, “An extended method for obtaining S-boxes based on three-dimensional chaotic baker maps,” Chaos, Solitons & Fractals, vol. 31, no. 3, pp. 571–579, 2007.

[22] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, “Efficient cryptosystem approaches: S-boxes and permutation substitution-based encryption,” Nonlinear Dynamics, vol. 87, no. 1, pp. 337–361, 2017.

[23] A. H. Alkhaldi, I. Hussain, and M. A. Gondal, “A novel design for the construction of safe S-boxes based on TDERC sequence,” Alexandria Engineering Journal, vol. 54, pp. 65–69, 2015.

[24] M. Khan, T. Shah, and M. A. Gondal, “An efficient technique for the construction of substitution box with chaotic partial differential equation,” Nonlinear Dynamics, vol. 73, no. 3, pp. 1795–1801, 2013.

[25] I. Hussain, T. Shah, M.A. Gondal, M. Khan, W.A. Khan “Construction of New S-box using a Linear Fractional Transformation”, World Applied Sciences Journal 14 (12): 1779-1785, 2011 ISSN 1818-4952© IDOSI Publications, 2011.

[26] J. Detombe & S. Tavares, “Constructing Large Cryptographically Strong S-boxes”, Lecture Notes in Computer Science, 165–181, 1993.

[27] N. Siddiqui, U. Afsar, T. Shah, A. Qureshi, “A Novel Construction of S16 AES S-boxes”, International Journal of Computer Science and Information Security (IJCIS), Vol. 14, No. 8, August 2016.

[28] L. Yi, X. Tong, Z. Wang, M. Zhang, H. Zhu, & J. Liu, “A Novel Block Encryption Algorithm Based on Chaotic S-Box for Wireless Sensor Network”, IEEE Access, 7, 53079–53090, 2019.

[29] D. Lambic, “A novel method of S-box design based on chaotic map and composition method”, Chaos, Solitons & Fractals, 58, 16–21. 2014.

[30] D. Lambic, “A novel method of S-box design based on discrete chaotic map”, Nonlinear Dynamics, 87(4), 2407–2413, 2016.

[31] F. Ozkaynak, “Construction of robust substitution boxes based on chaotic systems”. Neural Computing and Applications, 2017.

[32] T. Ye, & L. Zhimao, “Chaotic S-box: six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling”, Nonlinear Dynamics, 2018.

[33] F. Riaz, N. Siddiqui, “Design of an Efficient Cryptographic Substitution Box by using Improved Chaotic Range with the Golden Ratio”, International Journal of Computer Science and Information Security (IJCIS), Vol. 18, No. 1, 2020.
[34] A. Naseer, N. Siddiqui, “A Novel Approach for Construction of S-box using Modified Pascal’s Triangle”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 18, No. 1, 2020.

[35] W. Ifitikhar, N. Siddiqui, “An Effective Technique of Substitution-box Construction using Recurrence Relation with Logistic Map”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 18, No. 3, 2020.

[36] N. Siddiqui, U. Afsar, T. Shah, A. Qureshi, “A Novel Construction of S16 AES S-boxes”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, 2016.

[37] M. Khan, T. Shah, S. I. Batool, “Construction of S-box based on chaotic Boolean functions and its application in image encryption”, Neural Comput. Appl., 27, 677–685, 2015.

[38] M. Ahmad, D. Bhatia, Y. Hassan, “A Novel Ant Colony Optimization Based Scheme for Substitution Box Design”, Procedia Computer Science, 57, 572–580, 2015.

[39] A. Razaq, A. Youaf, U. Shuaib, N. Siddiqui, A. Ullah, A. Waheed, “A Novel Construction of Substitution Box Involving Coset Diagram and a Bijective Map”, Security and Communication Network, 1–16, 2017.

[40] V. M. Silva-Garcia, R. Flores-Carapia, C. Renteria-Marquez, B. Luna-Benoso, M. Aldape-Perez, “Substitution box generation using Chaos: An image encryption application”, Applied Mathematics and Computation, 332, 123–135, 2018.

[41] S. S. Jamal, M. U. Khan, T. Shah, “A Watermarking Technique with Chaotic Fractional S-Box Transformation”. Wireless Pers. Commun. 90, 2033–2049, 2016.

[42] Q. Lu, C. Zhu, G. Wang, “A Novel S-Box Design Algorithm Based on a New Compound Chaotic System”, Entropy, 21, 1004, 2019.

[43] N. A. Azam, U. Hayat, I. Ullah, “Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field”. Frontiers of Information Technology & Electronic Engineering, 20, 1378–1389, 2019.

[44] J. Daemen, & V. Rijmen, “The Design of Rijndael: AES-the Advanced Encryption Standard”, Springer Science & Business Media. 2013.

[45] M. T. Tran, D. K. Bui, A. D. Duong, “Gray S-box for Advanced Encryption Standard”. International Conference on Computational Intelligence and Security (Vol. 1, pp. 253-258). IEEE. 2008.