Hindawi
Security and Communication Networks
Volume 2019, Article ID 2847801, 13 pages
https://doi.org/10.1155/2019/2847801

Research Article

Construction of New S-Box Using Action of Quotient of the Modular Group for Multimedia Security

Imran Shahzad,[1] **Qaiser Mushtaq**,[2] **and Abdul Razaq**[3]

[1]*Department of Mathematics, Quaid-I-Azam University, Islamabad, Pakistan*
[2]*The Islamia University of Bahawalpur, Bahawalpur, Pakistan*
[3]*Department of Mathematics, Division of Science and Technology, University of Education, Lahore, Pakistan*

Correspondence should be addressed to Imran Shahzad; imranshahzad@math.qau.edu.pk

Received 22 May 2019; Revised 11 October 2019; Accepted 22 October 2019; Published 30 November 2019

Academic Editor: Emanuele Maiorana

Substitution box (S-box) is a vital nonlinear component for the security of cryptographic schemes. In this paper, a new technique which involves coset diagrams for the action of a quotient of the modular group on the projective line over the finite field is proposed for construction of an S-box. It is constructed by selecting vertices of the coset diagram in a special manner. A useful transformation involving Fibonacci sequence is also used in selecting the vertices of the coset diagram. Finally, all the analyses to examine the security strength are performed. The outcomes of the analyses are encouraging and show that the generated S-box is highly secure.

1. Introduction

With rapid advancement in communication technology, the maintenance of data security has become a great challenge for cryptographers. A number of useful encryption algorithms and techniques are created in interesting papers by Belazi et al. [1, 2] to ensure the safety of transmitted information. In this regard, block encryption algorithm plays an important role in modern cryptographic systems. The important component of block encryption algorithm is the substitution box (S-box). The S-box has been used in many cryptosystems including Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and Advanced Encryption Standard (AES). The security strength of the S-box determines the security strength of the entire cryptosystem. It is therefore established that the S-box is an important nonlinear component for the security of cryptographic schemes.

The DES was proposed by a well-known computer production company in 1977, and the DES investigations drove the refinement in the cryptographic system enormously [3]. Later, a group of university students broke the DES security. This led to the realization that of some other secure and efficient encryption method has to be evolved. In 2002, the Advanced Encryption Standard (AES) was created by Daemen and Rijmen, which is now the standard for the encryption [4]. The S-box has a vital role in quality of encryption. Utilization of a weak S-box is tantamount to compromising on the security of encryption process. Therefore, before using an S-box in a cryptosystem, it is pertinent to assess its strength. The analyses for measuring strength include nonlinearity method (NL), linear approximation probability method (LAP), bit independence criterion (BIC), strict avalanche criterion (SAC), and differential approximation probability method (DAP). Some studies related to the construction of S-box and its strength are in [5, 6]. The analyses of the S-box in image encryption based on majority logic criteria are investigated in [7, 8]. More investigation on the S-box based on a chaotic map is conducted in [9], hyperchaotic system-based S-box in [10], and chaotic neural network-based S-box in [11]. An efficient S-box is constructed in [12] by using a 2D Logistic-adjusted-Sine map, linear fractional transformation, and Gray code. Chen et al. described an S-box based on three-dimensional chaotic baker maps in [13]. Hayat and Azam [14] used elliptic curves to construct an S-box by considering the

ordinate of the curve for this construction. The construction of an S-box by using the projective general linear group was investigated by Altaleb et al. in [15]. Thus, various aspects of construction of an S-box are investigated to get a secure and better S-box which enables better encryption.

The techniques and methods for the generation of S-boxes presented in the literature are either suitable for the creation of static S-boxes or are very complicated and time consuming. Static S-boxes have their own limitations and weaknesses. These S-boxes may help attackers in the cryptanalysis of the captured ciphertext, and hence they may reach the original plaintext. On the other hand, the methods presented in the literature that generate dynamic and key-dependent S-boxes are entirely complex and inefficient. For example, recently, attackers have been successful in breaking the loops of AES. Thus, the need for an efficient method to generate dynamic S-boxes exists. The construction of an S-box using the first time group graphs is presented as an alternative S-box design technique. It exponentially improved security and efficacy which is vividly visible in subsequent work in this paper.

We propose an efficient technique for the construction of an S-box by using action of a quotient of $PSL(2, Z)$ on $PL(F_{257})$. The permutations obtained in this way are used to draw a coset diagram. The vertices of the coset diagram are considered in a special way for constructing an S-box. The S-box generated in this way is highly secure, closely meeting the optimal values of the standard S-box. All the tests for the security strength are performed and compared with other S-boxes confirming that the proposed S-box is highly secure.

2. Preliminaries

The modular group $PSL(2, Z)$ is the free product of two cyclic groups of orders 2 and 3. Its finite presentation is $\langle x, y ; x^2 = y^3 = 1\rangle$ [16]. It is the most studied group, and in the documentation for the award of Abel Prize in 2009, it is described as "one of the most important groups in the modern history of mathematics." Here, x and y are generators of the modular group. These generators are linear fractional transformations defined as $x(a) = (-1/a)$ and $y(a) = 1 - (1/a)$. By adjoining a new element $t(a) = (1/a)$ with x and y, one obtains a presentation $\langle x, y, t : x^2 = y^3 = t^2 = (xt)^2 = (yt)^2 = 1\rangle$ of the extended modular group $PGL(2, Z)$. Its existence is described in Lemma 2. Let q be a power of a prime p. Then, by the projective line over the finite field F_q, denoted by $PL(F_q)$, we mean $F_q \cup \{\infty\}$.

Higman introduced a graph for the modular group $PSL(2, Z)$. It is well known now as a coset diagram for the modular group. The three cycles of y are represented by triangles whose vertices are permuted anticlockwise by y, and any two vertices which are interchanged by x are connected by an edge. The fixed points of x and y, if they exist, are denoted by heavy dots. For more details about coset diagrams, we suggest reading [17–19].

Consider the action of the modular group on $PL(F_{13}) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \infty\}$. We apply x and y on each element of $PL(F_{13})$ to find permutation representation of x and y (see Table 1). Note that, if we apply x or y on any element of $PL(F_{13})$, normally a fraction is obtained. Since in F_{13}, $0 \equiv 13$, we continue to add 13 in the numerator so that an integral value is acquired.

In this way, we obtain the permutation representation of x and y as follows:

$$\begin{aligned} x &= (0, \infty)(1, 12)(2, 6)(3, 4)(5)(7, 11)(8,)(9, 10), \\ y &= (0, \infty, 1)(2, 7, 12)(3, 5, 6)(4,)(8, 9, 11)(10). \end{aligned} \tag{1}$$

Each cycle of length 3 is represented as a triangle, and each cycle of length 2 by an edge connecting vertices of the triangles, producing the following coset diagram. Here, 5, 8 are the fixed points of x and 4, 10 are the fixed points of y. The coset diagram evolved from the above permutations is shown in Figure 1.

A group is called the triangle group if it can be presented as $\langle x, y : x^l = y^m = (xy)^n = 1\rangle$ where l, m, n are the positive integers. It is denoted by $\Delta(l, m, n)$. The triangle groups $\Delta(2, 3, n)$ are particularly important as being one-relator quotients of $PSL(2, Z)$. The triangle groups $\Delta(2, 3, n)$ is finite if $n \leq 5$. The symmetric groups S_3, S_4 and alternating groups A_4, A_5 are finite triangle groups of the form $\Delta(2, 3, n)$.

The purpose of this study is to establish a scheme for S-box construction by taking action of $A_4 = \langle x, y; x^2 = y^3 = (xy)^3 = 1\rangle$ on $PL(F_{257})$. In this construction, we also utilize the Fibonacci sequence as it is one of the most interesting, useful, and close to the real life. A flow chart of the proposed scheme is presented in Figure 2.

3. Parametrization

There are several methods adopted by researchers for the construction of an S-box. Some cryptographers, while constructing an algebraic S-box, considered the action of a group on sets, real, or quadratic lines. But the use of coset diagrams is new in the literature. In the proposed scheme, we take action of A_4 on $PL(F_{257})$, then in the second step, we draw a coset diagram of the action, and finally we construct an S-box by using vertices of the coset diagram. The action of the modular group on $PL(F_p)$ evolves a coset diagram in which each vertex is fixed by $(xy)^p$. In Figure 1, one can see that each vertex of the coset diagram is fixed by $(xy)^{13}$. This coset diagram represents the homomorphic image of the group $\langle x, y : x^2 = y^3 = (xy)^{13} = 1\rangle$. In order to draw a coset diagram for $\langle x, y : x^2 = y^3 = (xy)^n = 1\rangle$, where n is of our own choice, there is a method given in [20], known as parametrization method. It is expressed in the following way.

Lemma 1. *There are just two conjugacy classes of non-degenerate homomorphism from $PGL(2, Z)$ to $PGL(2, q)$ in which $\overline{x}\,\overline{y}$ is of order 2, and the two other in which $\overline{x}\,\overline{y}\overline{t}$ is of order 2.*

Lemma 2. *Either $\overline{x}\,\overline{y}$ is of order 6 or there exists an involution $\overline{t}$ in $PGL(2, q)$ such that $\overline{t}\overline{x}\overline{t} = \overline{t}$ and $\overline{t}\overline{y}\overline{t} = (\overline{y})^2$.*

Table 1: Action of $PSL(2, Z)$ on $PL(F_{13})$.

α	$x(a)$	$y(a)$
∞	$x(\infty) = (-1/\infty) = 0$	$y(\infty) = 1 - (1/\infty) = 1$
0	$x(0) = (-1/0) = \infty$	$y(0) = 1 - (1/0) = \infty$
1	$x(1) = (-1/1) = ((-1 + 13)/1) = 12$	$y(1) = 1 - (1/1) = 0$
2	$x(2) = (-1/2) = ((-1 + 13)/2) = 6$	$y(2) = 1 - (1/2) = ((1 + 13)/2) = 7$
3	$x(3) = (-1/3) = ((-1 + 13)/3) = 4$	$y(3) = 1 - (1/3) = ((2 + 13)/3) = 5$
4	$x(4) = (-1/4) = ((-1 + 13)/4) = 3$	$y(4) = 1 - (1/4) = ((3 + 13)/4) = 4$
5	$x(5) = (-1/5) = ((-1 + 13)/5) = ((-1 + 13 + 13)/5) = 5$	$y(5) = 1 - (1/5) = ((4 + 13)/5) = ((4 + 2(13))/5) = 6$
6	$x(6) = (-1/6) = ((-1 + 13)/6) = 2$	$y(6) = 1 - (1/6) = ((5 + 13)/6) = 3$
7	$x(7) = (-1/7) = ((-1 + 13)/7) = ((-1 + 6(13))/7) = 11$	$y(7) = 1 - (1/7) = ((6 + 13)/7) = ((6 + 6(13))/7) = 12$
8	$x(8) = (-1/8) = ((-1 + 13)/8) = ((-1 + 5(13))/8) = 8$	$y(8) = 1 - (1/8) = ((7 + 13)/8) = ((7 + 5(13))/8) = 9$
9	$x(9) = (-1/9) = ((-1 + 13)/9) = ((-1 + 7(13))/9) = 10$	$y(9) = 1 - (1/9) = ((8 + 13)/9) = ((8 + 7(13))/9) = 11$
10	$x(10) = (-1/10) = ((-1 + 13)/10) = ((-1 + 7(13))/10) = 9$	$y(10) = 1 - (1/10) = ((9 + 13)/10) = ((9 + 7(13))/10) = 10$
11	$x(11) = (-1/11) = ((-1 + 13)/11) = ((-1 + 6(13))/11) = 7$	$y(11) = 1 - (1/11) = ((10 + 13)/11) = ((10 + 6(13))/11) = 8$
12	$x(12) = (-1/12) = ((-1 + 13)/12) = 1$	$y(12) = 1 - (1/12) = ((11 + 13)/12) = 2$

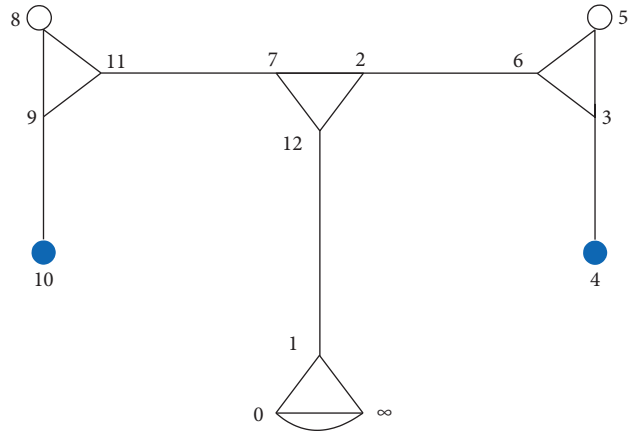

Figure 1: Coset diagram for $PL(F_{13})$.

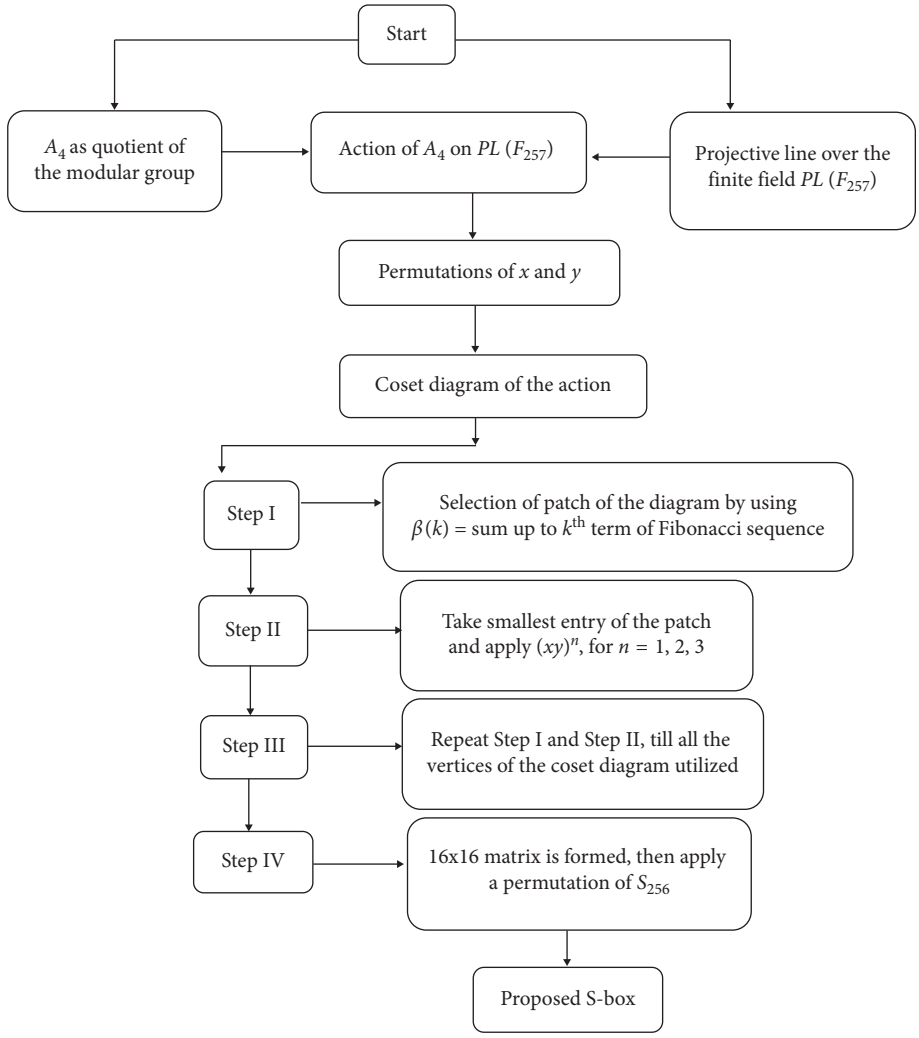

Figure 2: Flow chart of the proposed scheme.

Lemma 3. *Any element (not of order 1, 2 or 6) of $PGL(2, q)$ is the image of xy under some nondegenerate homomorphism of $PGL(2, Z)$ into $PGL(2, q)$.*

Theorem 1. *The conjugacy classes of nondegenerate homomorphism of $PGL(2, Z)$ into $PGL(2, q)$ are in one-to-one correspondence with the element $\theta \neq 0, 3$ of F_q*

under the correspondence which maps each class to its parameter.

For each nondegenerate homomorphism $\sigma : PGL(2, Z) \mid PGL(2, q)$, there exists an action of $PGL(2, Z)$ on $PL(F_q)$. For the generators x, y, and t, we suppose $(x)\sigma = \overline{x}$, $(y)\sigma = \overline{y}$, and $(t)\sigma = \overline{t}$ to have order 2, 3, and 2, respectively. If X and Y are matrices representing $\overline{x}$ and $\overline{y}$, normalized by $\det(Y) = 1$; then, by taking $\theta = (\text{trace}XY)^2/\det(XY)$, we can associate a parameter θ with the homomorphism σ. Assigning the parameter $\theta \in F_q$ with σ is called parametrization. The canonical map $GL(2, q) \mid PGL(2, q)$ associates a matrix M to $hM \in PGL(2, q)$, where h is a scalar. It can be seen that

$$\frac{(\text{trace}M)^2}{\det(M)} = \theta \in F_q, \tag{2}$$

is an invariant of hM. Here, θ will be an invariant if the characteristic equations of all the elements in a conjugacy class of M are the same. If in addition $(XY)^n = 1$, then by Theorem 1 there is a bijection between the elements in F_q and the conjugacy class of σ. Specifically, there is a polynomial $g_n(\theta)$ such that corresponding to each root θ of $g_n(\theta)$, a triplet $\overline{x}, \overline{y}, \overline{t} \in PGL(2, q)$ can be obtained. Lemma 1, 2, and 3 guarantee the presentation of the triangle groups $\Delta(2, 3, n) = \langle \overline{x}, \overline{y} : (\overline{x})^2 = (\overline{y})^3 = (\overline{xy})^n = 1 \rangle$.

If X, Y, and T indicate elements of $GL(2, q)$ corresponding to the elements x, y, and t in $PGL(2, q)$ then by this and the fact that x, y, and t are of orders 2, 3, and 2, respectively, the matrices X, Y, and T are

$$X = \begin{bmatrix} a & kc \\ c & -a \end{bmatrix},$$
$$Y = \begin{bmatrix} d & kf \\ f & -d-1 \end{bmatrix}, \tag{3}$$
$$T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix},$$

where $a, c, d, f, k \in F_q$ with $k \neq 0$. Also, $\det(X) = \Delta = -a^2 - kc^2$. The determinant of matrix Y is fixed to be $\det(Y) = 1$, which gives $d^2 + d + kf^2 + 1 = 0$.

For the conjugacy class of $\overline{xy}$, consider the characteristic equations of the matrices X, Y, and XY, which are

$$X^2 + \Delta I = 0,$$
$$Y^2 + Y + I = 0, \tag{4}$$
$$(XY)^2 - r(XY) + \Delta I = 0,$$

where $\text{trace}(XY) = r = a(2d + 1) + 2ckf$ and $\det(XY) = \Delta$. If $\text{trace}(XYT) = ks = 2afk - kc(2d + 1)$, then $r^2 + ks^2 = 3\Delta$. For $p = 257$ with $n = 3$, the corresponding polynomial is $\theta - 1 = 0$.

Ultimately, by using the values of r, s, d, f, and k in the abovementioned equations, the values of the entries of matrices X, Y, and T are

$$X = \frac{45z + 95}{95z - 45},$$
$$Y = \frac{16}{16z - 1}, \tag{5}$$
$$T = \frac{-1}{z}.$$

3.1. Action of A_4 on Projective Line over the Finite Field $PL(F_{257})$. The action of A_4 on the projective line over the finite field $PL(F_{257})$ is defined by the map $A_4 \times PL(F_{257}) \longrightarrow PL(F_{257})$. The linear fractional transformations of the generators $\overline{x}$ and $\overline{y}$ of A_4 act on each element of $PL(F_{257})$ producing the following permutations of $\overline{x}$ and $\overline{y}$:

$\overline{x}$: (055 000)(157 001)(019 002)(183 003)(004 020)(192 005)(006 150)(007 096)(008 024)(009 026)(029 010) (034 011)(012 044)(013 074)(014 inf)(211 015)(016 241)(251 017)(018 256)(021 189)(022 135)(023 093) (025 102)(027 128)(028 230)(203 030)(207 031)(032 182)(092 033)(035 158)(036 058)(037 179)(140 038) (039 063)(071 040)(041 126)(122 042)(043 136)(153 045)(237 046)(047 129)(048 239)(049 049)(098 050) (051 061)(052 053)(141 054)(056 086)(057 168)(184 059)(060 225)(062 077)(064 167)(164 065)(066 171) (067 105)(068 070)(069 083)(072 075)(073 209)(076 212)(078 254)(079 191)(080 200)(081 109)(082 255) (084 160)(085 205)(087 154)(088 166)(116 089)(090 162)(091 100)(094 206)(095 137)(165 097)(099 104) (226 101)(253 103)(106 248)(107 146)(108 161)(110 174)(175 111)(112 155)(113 138)(219 114)(115 133) (117 228)(118 221)(119 197)(188 120)(220 121)(123 195)(124 177)(125 201)(250 127)(130 173)(131 198) (132 240)(134 142)(139 178)(143 151)(144 231)(247 145)(147 172)(148 190)(149 242)(152 170)(156 238) (159 244)(243 163)(169 196)(176 204) (180 218)(181 186)(185 194)(235 187)(193 252)(199 229)(202 216) (208 223)(210 213)(214 245)(215 217)(222 246)(224 234)(227 249)(232 233)(236 236)

$\overline{y}$: (000 241 inf)(121 242 001)(256 120 240)(113 002 100)(239 128 141)(230 070 003)(171 011 238)(004 090 177)(151 237 064)(087 005 049)(236 154 192)(222 027 006)(214 019 235)(190 131 007)(110 051 234) (008 075 209)(166 233 302)(009 072 184)(169 232 057)(010 089 164)(152 231 077)(134 012 101) (229 107 140)(195 162 013)(079 046 228)(014 060 186)(181 227 055)(199 104 015)(137 042 226)(225 016 249) (148 105 017)(136 093 224)(189 084 018)(157 052 223)(074 020 050)(221 167 191)(132 033 021) (208 109 220)(022 115 206)(126 219 035)(145 174 023)(067 096 218)(059 024 045)(217 182 196) (163 056 025)(185 078 216)(153 073 026)(168 088 215)(111 085 028)(156 130 213)(179 029 040)(212 062 201)(095 044 030)(197 146 211)(175 183 031)(058 066 210)(173 034 036)(207 068 205)(116 037 097)(204 125 144)(119 099 038)(142 122 203)(129 039 243)(202 112 255)(147 041

248)(200 094 250) (043 061 247)(180 198 251)(047 102 159)(139 194 082)(150 048 253)(193 091 245)(149 081 053)(160 092 188)(103 054 246)(187 138 252)(086 063 244)(178 155 254)(165 071 065)(170 076 176)(127 133 069)(108 114 172)(135 080 083)(161 106 158)(124 123 098)(118 117 143).

3.2. Coset Diagram of the Action. The coset diagram for the action of A_4 on $PL(F_{257})$ consists of two types of the circuits, given below (Figures 3 and 4):

(i) In Type-I circuit, there are four triangles and this type of circuit occurs twenty-one times in the coset diagram. There is no fix point of $\overline{x}$ nor of $\overline{y}$ in Type-I circuit. Thus, Type-I circuits utilized 252 vertices of the coset diagram.

(ii) In Type-II circuit, there are only two triangles and this type of circuit occurs only once in the coset diagram. In this circuit, there are two fixed points of $\overline{x}$. Thus, Type-II circuit utilized only six vertices of the coset diagram.

4. Construction of S-Box Using a Coset Diagram

After making the coset diagram, we proceed towards construction of the S-box from the coset diagram. There are twenty-two circuits in the coset diagram, so the first step is how to choose a circuit. The second step is the selection of vertices of that circuit in a specific manner. Therefore, for the first part, instead of randomly choosing the circuits we choose the circuits by using a sequence, known as Fibonacci sequence $1, 1, 2, 3, 5, 8, \ldots$. We define mapping as $\beta : PL(F_{257}) \mid PL(F_{257})$ by $\beta(k)$ = Sum of the first k terms of the Fibonacci sequence. Then, choose the circuit in which $\beta(x)$ occurs. By this mapping, we can easily and systematically choose the circuits one by one. For illustration, $\beta(0) = 0$, we pick the circuit of the coset diagram having 0 as the vertex, that is, the circuit shown in Figure 5. Similarly, for $\beta(1) = 1, \beta(2) = 1 + 1 = 2, \beta(3) = 1 + 1 + 2 = 4$, and so on.

Secondly, after choosing the circuit of the coset diagram, now we select the vertices of that circuit in a special manner. We initiate from the vertex $\beta(0)$ and apply xy, $(xy)^2$, and $(xy)^3$ (because of the third relator of A_4) on $\beta(0)$ and note the vertices, which are (0, 181, 14). Then, in the same circuit we choose the smallest number from the remaining vertices of the circuit, which is 16, apply xy and its powers to get (16, ∞, 60). Continue the process by choosing the smallest from the remaining vertices of the circuit and apply xy and its powers so that all the vertices of the circuit are utilized. We can view all the entries of the circuit containing $\beta(0) = 0$ in the first row of Table 2, except infinity. It is important to mention here that if $\beta(x)$ appears in the previous circuit then it means it is already utilized so move on. But, if $\beta(x)$ appears in the new circuit, then apply xy and its powers in the similar fashion and note the permutation. Continue the process till all the vertices of the coset diagram are exhausted yielding 258 entries in an order. Ignore ∞ and 256. Thus, a 16×16 S-box is constructed as shown in Table 2. It is important to mention here that

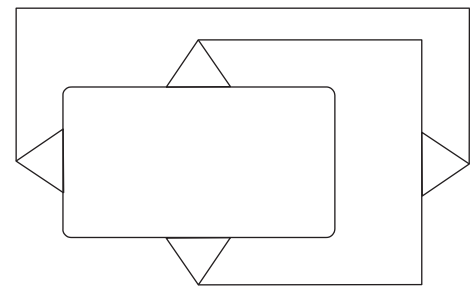

Figure 3: Type-I circuit.

Figure 4: Type-II circuit.

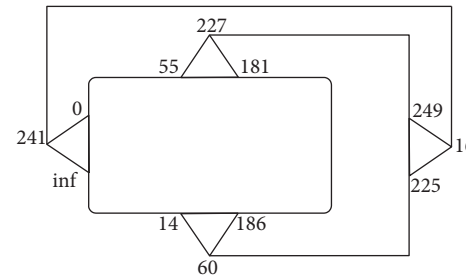

Figure 5: A circuit of the coset diagram containing $\beta(0)$.

whenever $\beta(x) > 256$ take modulo class 257. It seems easy to find $\beta(x)$ in modulo class 257 but this is not so. We had to use an online PowerMod Calculator for these calculations.

The entire scheme of constructing an S-box is based on the action of a finite triangle group A_4, coset diagram, and Fibonacci sequence. These all inculcate the natural patterns in the scheme which gives a very suitable and effective S-box as a result.

For more variability, we apply one of the permutations from S_{256} on the outcome presented in Table 2 to change the positions of the elements. This permutation increases the randomness of the elements and gives the proposed S-box with high nonlinearity, as shown in Table 3. The permutation $\alpha' \in S_{256}$ used here is as follows:

(01 195 199 236 194 185 207 251 082 026 096 155 104 175 052 132 197 030 149 216 233 167 043 118 024 011 221 146 047 241 171 140 090 148 248 121 242 069 008 055 240 042 045 200 143 162 021 142 190 157 131 074 184 161 127 062 218 211 124 208 097 153 039 087 202 041 100 066 072 170 232 178 065 010 073 007 015 059 238 231 122 058 234 182 023 219 061 086 133 051 247 018 048 222 137 098 077 125 228 014 029 220 165 094 214 166 003 244 130 209 112 189 203 169 033 243 187 076 113 145 070 255 053 037 168 107 223 226 224 116 108 044 006 114 068 054 180 103 046 204 201 111 147 159 013 213 181 129 225 078 177 152 115 016 093 019 109 079 227 229 085 192 176 188 057 212 235 063 193 249 105 173 164 102 084 040 253 210 237

Table 2: 16×16 matrix evolved after coset diagram.

0	181	14	16	60	55	241	249	186	227	225	1	52	149	53	223
109	81	220	242	121	208	157	2	235	138	19	100	245	91	113	252
187	214	193	4	50	124	13	20	90	74	195	98	123	162	177	7
218	198	17	180	67	96	190	105	131	251	148	12	30	142	42	203
95	44	101	137	122	226	134	18	120	160	21	84	92	33	188	240
132	189	6	48	128	27	141	246	54	239	253	103	150	222	32	196
232	57	88	233	166	215	182	168	169	217	46	64	191	79	221	117
118	167	151	143	237	228	15	197	99	38	229	104	119	146	140	107
211	199	3	31	68	28	70	205	85	207	175	111	183	230	78	178
194	82	202	185	112	254	216	139	155	255	23	224	110	43	93	145
51	247	174	61	234	136	25	159	86	39	244	47	56	63	243	102
163	129	22	80	94	69	135	115	83	127	200	133	206	250	35	161
114	41	219	172	106	147	108	126	248	158	11	36	66	34	238	130
58	173	213	156	171	210	8	45	73	9	153	59	24	75	184	26
72	209	10	40	65	29	89	37	71	179	97	116	164	165	5	236
154	49	87	192	62	152	76	77	201	144	125	212	176	170	231	204

Table 3: Proposed S-box.

151	129	29	93	81	240	171	105	75	229	78	195	132	216	37	226
79	158	165	69	242	97	131	106	63	252	109	66	163	186	145	38
76	166	249	4	154	208	213	183	148	184	199	77	101	21	152	15
211	230	17	103	205	155	157	173	74	82	248	126	149	190	45	169
64	6	25	98	58	224	34	48	56	1	142	40	191	243	57	42
197	203	114	222	92	95	156	160	180	80	210	46	198	137	9	91
178	212	179	167	3	128	23	107	33	99	204	2	139	227	146	138
24	43	83	162	239	14	59	30	71	245	85	175	119	47	90	223
124	236	244	12	54	150	255	136	192	251	52	147	28	120	177	65
185	26	41	207	189	31	233	117	104	53	219	116	49	118	19	70
247	18	0	86	182	27	254	13	133	87	130	241	67	193	187	84
246	225	5	217	214	8	89	16	172	62	143	51	144	174	32	127
68	100	61	20	250	159	44	196	121	123	221	215	72	110	231	209
234	164	181	50	140	237	55	200	7	36	39	238	11	206	161	96
170	112	73	253	10	220	35	168	134	141	153	108	102	94	88	194
60	135	202	176	218	115	113	125	111	22	228	235	188	232	122	201

239 080 217 099 071 134 034 110 049 135 089 035 032 009 036 215 128 092 191 139 117 138 252 038 245 163 246 160) (000 151 083 172 020 183 028 150 198 230 120 056 067 205 136 027 095 064 002 106 250 174) (005 088 179 141 156 050 154 060 081 158 123 101 025 254 031 012 126 196 091 186 075 206 144 022) (004) (017) (119).

5. Analysis for Evaluating the Strength of S-Box

The criteria generally selected to test the S-box are nonlinearity, strict avalanche criteria, bit independence criteria, linear approximation probability, and differential approximation probability. For testing the strength of the proposed S-box, we discuss each of them in the following. We also compare the results with recently developed S-boxes.

5.1. Nonlinearity. Nonlinearity (NL) is one of the significant criteria for the performance evaluation of the S-box which measures the randomness of the values of the S-box. The NL of proposed S-box is 110.50 which is higher than that of [21–44]. The higher the NL, the stronger the S-box. Hence, the NL of the proposed S-box guarantees a secure communication. The NL of the proposed S-box is expressed in Table 4 and comparison with [21–44] is in Table 7.

5.2. Strict Avalanche Criteria. The concept of strict avalanche criteria (SAC) was introduced by Webster and Tavares [45] which measures the confusion creation of an S-box by measuring the change in output bits due to the change in input bits. The minimum and the maximum value of SAC of the proposed S-box are 0.40625 and 0.578125, whereas the average value is 0.503175 (Table 5) which is much closer to 0.5, the ideal value of SAC. The lesser deviation from 0.5, the stronger the S-box. The comparison of SAC of the proposed S-box with that of [21–44] is in Table 7, which depicts that the proposed S-box has better SAC performance.

5.3. Bit Independence Criteria. Bit independence criteria also measures the strength of the S-box. The BIC value of the generated S-box is 109.21 (Table 6). The comparison with that of [21–44] is in Table 7. This BIC value is sufficiently good and assures secure communication and better encryption in cryptographic application.

Table 4: Nonlinearities of constituent Boolean functions of the proposed S-box.

Boolean function	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
Nonlinearity	112	110	112	110	110	108	112	110

Table 5: Strict avalanche criteria.

0	1	2	3	4	5	6	7
0.453125	0.546875	0.484375	0.453125	0.484375	0.515625	0.500000	0.500000
0.484375	0.484375	0.453125	0.484375	0.546875	0.531250	0.453125	0.515625
0.406250	0.515625	0.531250	0.500000	0.515625	0.500000	0.531250	0.56250
0.531250	0.515625	0.437500	0.515625	0.531250	0.421875	0.500000	0.546875
0.531250	0.531250	0.500000	0.515625	0.453125	0.500000	0.468750	0.531250
0.515625	0.515625	0.546875	0.453125	0.515625	0.546875	0.453125	0.515625
0.515625	0.531250	0.484375	0.578125	0.500000	0.453125	0.500000	0.546875
0.468750	0.515625	0.546875	0.484375	0.468750	0.531250	0.546875	0.484375

Table 6: Bit independence criteria.

0	1	2	3	4	5	6
—	106	110	110	108	108	110
106	—	108	110	110	110	106
110	108	—	108	112	110	110
110	110	108	—	108	110	108
108	110	112	108	—	110	110
108	110	110	110	110	—	110
110	106	110	108	110	110	—

Table 7: Outcomes of the analyses.

S-boxes	Nonlinearity	SAC	BIC	DAP	LP
Proposed S-box	110.50	0.5031	109.21	0.0234	0.0860
[21]	103.25	0.5059	104.29	0.0469	0.1250
[22]	104.88	0.4966	102.96	0.0391	0.1328
[23]	105.50	0.5000	103.78	0.0468	0.1250
[24]	106.00	0.5020	103.00	0.0469	0.1250
[25]	110.00	0.4937	103.86	0.0391	0.1250
[26]	106.75	0.5032	103.64	0.0469	0.1484
[27]	104.50	0.4980	104.64	0.0469	0.1250
[28]	110.25	0.50	104	10	0.125
[29]	108	0.5068	96	10	0.1406
[30]	109	0.5026	102	10	0.1406
[31]	107.5	0.4971	106	10	0.125
[32]	107	0.5015	98	10	0.1484
[33]	108	0.5073	100	10	0.1523
[34]	107.5	0.5036	90	10	0.1484
[35]	106.5	0.4995	98	10	0.1172
[36]	107.5	0.4943	98	10	0.125
[37]	108.75	0.4946	94	10	0.1328
[38]	109.25	0.5012	104	8	0.0937
[39]	106.75	0.5034	100	10	0.1328
[40]	107.25	0.5034	98	12	0.1328
[41]	106.75	0.4941	98	10	0.125
[42]	106.75	0.4076	98	10	0.1328
[43]	106	0.5066	96	12	0.1445
[44]	107.75	0.4976	105	8	0.125

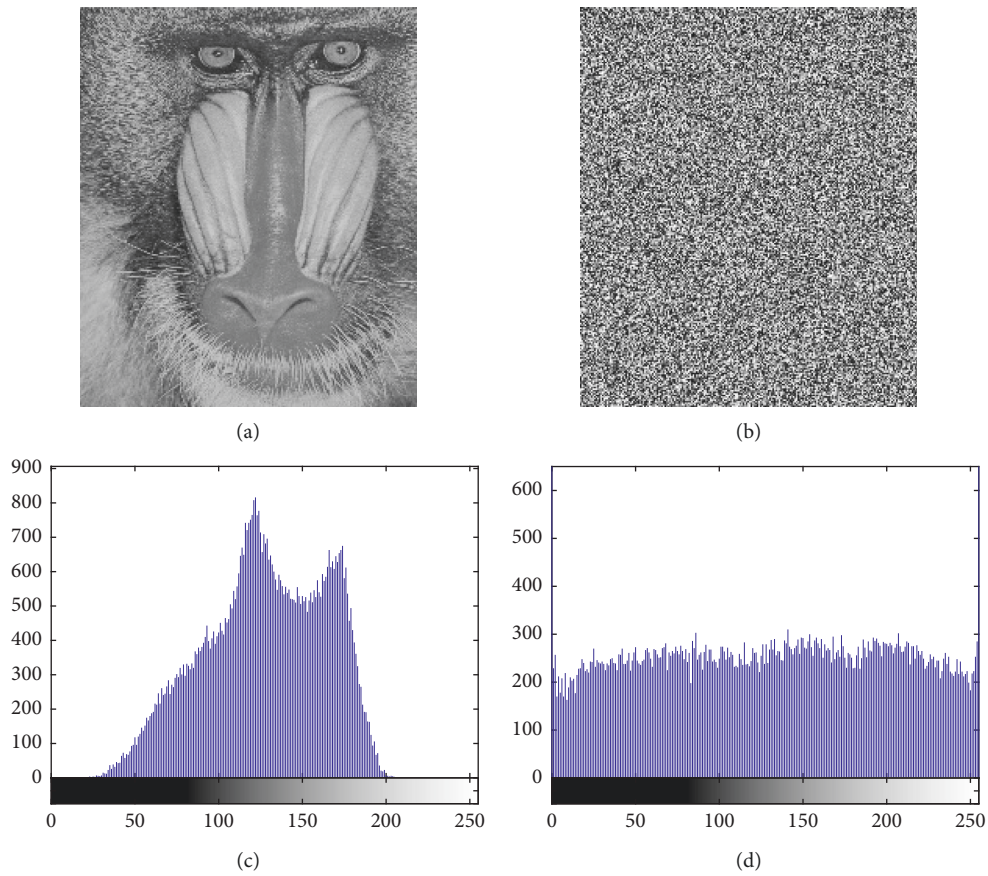

Figure 6: Image encryption with the proposed S-box.

5.4. Linear Approximation Probability. Linear approximation probability (LAP) criteria measure the strength or resistance of the S-box against linear attacks. The smaller the LAP value, the higher the strength of security of the S-box. The LAP of the generated S-box is 0.0859375 which is smaller than that of [21–44]. This depicts that the proposed scheme has ability to generate a strong, efficient, and attack-resistant S-box.

5.5. Differential Approximation Probability. Differential approximation probability (DAP) is a measure to analyse the resistance of the S-box against differential attacks. The smaller the DAP, the higher the resistance against attacks. The DAP of the generated S-box is 0.0234375 which is exceptionally good. This DAP value is near to the optimal value 0.0156. This reflects that the S-box generated by group action and using coset diagrams has the ability of high resistance against differential attacks.

The comparison of NL, SAC, BIC, LAP, and DAP with other known S-boxes is given in Table 7. The NL and the BIC value of the proposed S-box are higher than that of the others. The least values of LAP and DAP show the proposed S-box is highly resistive against the linear as well as differential attacks. And the confusion/diffusion creation criteria SAC is also closer to the standard value 0.5000. Hence, the perfect combination of all (NL, SAC, BIC, LAP, and DAP) shows the proposed S-box is a secure choice for encryption.

6. Majority Logic Criteria

Majority logic criteria measure image encryption strength of the S-box. Entropy, correlation, contrast, energy, and homogeneity are the components of MLC. We used JPEG image of a baboon for this analysis. Figures 6(a) and 6(c) show the original image and the histogram, while Figures 6(b) and 6(d) show the encrypted image and encrypted histogram. Specially, the entropy value which is 7.9832 is better than that of [4, 24, 26, 46, 47]. The entropy value is very close to the ideal value, which is 8. The values of contrast, correlation, energy, and homogeneity also indicate the proposed scheme provides a strong S-box which is suitable for encryption applications. The results of this analysis in comparison with well-known S-boxes are in Table 8.

7. Application of Proposed S-Box in Multimedia Security

The generated S-box is also being applied for watermarking technique to determine its application in multimedia security. From the outcomes of the analyses (Table 9), it can be seen that our S-box has the tendency to create confusion.

Table 8: Comparison of MLC for the proposed S-box.

Baboon image	Entropy	Contrast	Correlation	Energy	Homogeneity
Proposed S-box	7.9832	10.4027	0.00073	0.0157	0.3909
Ullah et al. [24]	7.9824	8.7348	-0.0043	0.0172	0.4074
Razaq et al. [26]	7.9551	8.5267	0.00044	0.0174	0.4088
Daemen and Rijmen [4]	7.9325	7.2240	0.0815	0.0211	0.4701
Khan et al. [46]	7.9612	8.1213	−0.0512	0.0210	0.4011
Belazi et al. [47]	7.9252	8.0391	0.0119	0.02219	0.4428

Table 9: Statistical analyses of the host image and watermarked image.

Statistical	Lena		Pepper		Baboon	
	Host	Watermarked	Host	Watermarked	Host	Watermarked
Homogeneity	0.8653	0.8628	0.9317	0.9317	0.7844	0.7836
Contrast	0.4144	0.4191	0.2219	0.2214	0.6155	0.6191
Energy	0.0944	0.0936	0.1556	0.1560	0.0652	0.0653
Entropy	0.5854	0.5859	0.7852	0.7856	0.6960	0.6960
Correlation	0.9444	0.9437	0.9484	0.9488	0.8994	0.8987

(a) (b) (c)

Figure 7: Host images. (a) Lena. (b) Baboon. (c) Peppers.

Figure 8: Watermark.

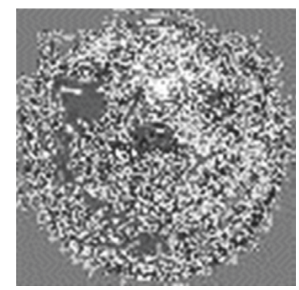

Figure 9: S-box substituted.

Therefore, it meets the necessary requirements to be reliable in multimedia applications. In watermarking scheme, the watermark is first encrypted with the proposed S-box and then embedded into the host image. This additional encryption would provide additional security as the inverse of S-box is required for the extraction of watermark. This will add more security to our scheme and will support copyrights protection. As frequency domain technique is more robust as compared to spatial domain, discrete cosine transform is used for watermarking technique and S-box-substituted watermark is embedded into the DCT-transformed host image (Figures 7–10).

(a) (b) (c)

Figure 10: Watermarked images. (a) Lena. (b) Baboon. (c) Peppers.

8. Results and Discussion

Table 7 shows the performance comparison of our S-box with other S-boxes based on the cryptographic properties. Our findings are as follows:

(1) A high value of nonlinearity provides resistance against linear cryptanalysis. The average nonlinearity of our S-box is superior to the rest of the S-boxes in Table 7. This results in decent confusion, and makes the proposed S-box resilient against linear cryptanalysis.

(2) The SAC value near 0.5 (the perfect value for SAC) is the ultimate goal of every S-box designer. Table 7 depicts that our SAC value (0.503) is very close to this perfect value. We can say that our S-box satisfies the SAC.

(3) Similarly, the BIC value of our S-box is better than the BIC values of all other S-boxes in Table 7.

(4) Any S-box with a lesser value of DAP is more resilient against differential cryptanalysis. The DAP value of our S-box is 0.0234, which is better than the DAP values of other S-boxes in Table 7. This value of DAP reflects the strength of our S-box.

(5) To defy linear cryptanalysis, a smaller value of LAP for a given S-box is desired by S-box designers. The LAP value of our S-box is 0.086, better than all S-boxes developed in [21–44]. Due to this small value, we can say that our S-box is resistant to linear cryptanalysis.

(6) The JPEG image of the baboon is used for this MLC. The values of entropy, contrast, correlation, energy, and homogeneity show that our S-box is suitable for encryption applications.

9. Conclusions

An efficient scheme for the construction of an S-box is presented in this paper. The proposed S-box is constructed by taking action of a quotient of the modular group on the projective line over the finite field $PL(F_{257})$. The newly constructed S-box is applied for image encryption and watermarking schemes as well. The proposed S-box has high resistance against linear attacks as well as for differential attacks. The results of security strength measuring tests: NL, SAC, BIC, LAP, and DAP all are very close to ideal values. This depicts that the proposed scheme is highly preferable for constructing an S-box for cryptographic applications.

Data Availability

The evaluation data used to support the findings of this study are available from the corresponding author upon request.

Disclosure

This article has been taken from the Ph.D. thesis of Imran Shahzad supervised by Prof. Dr. Qaiser Mushtaq.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Dr. Abdul Razaq reviewed the paper and gave helpful suggestions.

References

[1] A. Belazi, A. A. A. El-Latif, R. Rhouma, and S. Belghith, "Selective image encryption scheme based on DWT, AES S-box and chaotic permutation," in *Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 606–610, IEEE, Dubrovnik, Croatia, August 2015.

[2] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[3] D. E. Standard, *National Bureau of Standards, NBS FIPS PUB 46*, National Bureau of Standards. US, Department of Commerce, Gaithersburg, MD, USA, 1977.

[4] J. Daemen and V. Rijmen, *The Design of Rijndael: AES-The Advanced Encryption Standard*, Springer Science & Business Media, Berlin, Germany, 2013.

[5] L. Cui and Y. Cao, "A new S-box structure named affine-power-affine," *International Journal of Innovative Computing, Information and Control*, vol. 3, no. 3, pp. 751–759, 2007.

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

[7] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, "Statistical analysis of S-box in image encryption applications based on majority logic criterion," *International Journal of Physical Sciences*, vol. 6, no. 16, pp. 4110–4127, 2011.

[8] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal, and U. Y. Bhatti, "Some analysis of S-box based on residue of prime number," *Proceedings of the Pakistan Academy of Sciences*, vol. 48, no. 2, pp. 111–115, 2011.

[9] M. Asim and V. Jeoti, "Efficient and simple method for designing chaotic S-boxes," *ETRI Journal*, vol. 30, no. 1, pp. 170–172, 2008.

[10] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, 2018.

[11] Y. Wang, L. Yang, M. Li, and S. Song, "A method for designing S-box based on chaotic neural network," in *Proceedings of the 2010 6th International Conference on Natural Computation*, vol. 2, pp. 1033–1037, IEEE, Yantai, China, August 2010.

[12] J. Peng, A. A. A. El-Latif, A. Belazi, and Z. Kotulski, "Efficient chaotic nonlinear component for secure cryptosystems," in *Proceedings of the 9th International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 989–993, IEEE, Milan, Italy, July 2017.

[13] 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.

[14] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, 2019.

[15] A. Altaleb, M. S. Saeed, I. Hussain, and M. Aslam, "An algorithm for the construction of substitution box for block ciphers based on projective general linear group," *AIP Advances*, vol. 7, no. 3, Article ID 035116, 2017.

[16] G. Higman and Q. Mushtaq, "Coset diagrams and relations for $PSL(2, Z)$.," *The Arab Gulf Journal of Scientific Research*, vol. 1, no. 1, pp. 159–164, 1983.

[17] Q. Mushtaq, "Modular group acting on real quadratic fields," *Bulletin of the Australian Mathematical Society*, vol. 37, no. 2, pp. 303–309, 1988.

[18] A. Rafiq and Q. Mushtaq, "Coset diagrams of the modular group and continued fractions," *Comptes Rendus Mathematique*, vol. 357, no. 8, pp. 655–663, 2019.

[19] A. Torstensson, "Coset diagrams in the study of finitely presented groups with an application to quotients of the modular group," *Journal of Commutative Algebra*, vol. 2, no. 4, pp. 501–514, 2010.

[20] Q. Mustaq, "Parametrization of all homomorphisms from $PGL(2Z)$ into $PGL(2, q)$," *Communications in Algebra*, vol. 20, no. 4, pp. 1023–1040, 1992.

[21] G. Jakimoski and L. Kocarev, "Chaos and cryptography: block encryption ciphers based on chaotic maps," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 2, pp. 163–169, 2001.

[22] 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.

[23] A. Belazi and A. A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Optik*, vol. 130, pp. 1438–1444, 2017.

[24] A. Ullah, S. S. Jamal, and T. Shah, "A novel construction of substitution box using a combination of chaotic maps with improved chaotic range," *Nonlinear Dynamics*, vol. 88, no. 4, pp. 2757–2769, 2017.

[25] Y. Wang, P. Lei, and K. W. Wong, "A method for constructing bijective S-box with high nonlinearity based on chaos and optimization," *International Journal of Bifurcation and Chaos*, vol. 25, no. 10, Article ID 1550127, 2015.

[26] A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah, and A. Waheed, "A novel construction of substitution box involving Coset diagram and a bijective map," *Security and Communication Networks*, vol. 2017, Article ID 5101934, 16 pages, 2017.

[27] L. Liu, Y. Zhang, and X. Wang, "A novel method for constructing the S-box based on spatiotemporal chaotic dynamics," *Applied Sciences*, vol. 8, no. 12, p. 2650, 2018.

[28] A. A. Alzaidi, M. Ahmad, M. N. Doja, M. Maftab Khan, and M. S. Beg, "A new 1D chaotic map and β-hill climbing for generating substitution-boxes," *IEEE Access*, vol. 6, pp. 55405–55418, 2018.

[29] Y. Wang, K. W. Wong, C. Li, and Y. Li, "A novel method to design S-box based on chaotic map and genetic algorithm," *Physics Letters A*, vol. 376, no. 6-7, pp. 827–833, 2012.

[30] W. Yong and L. Peng, "An improved method to obtaining S-box based on chaos and genetic algorithm," *HKIE Transactions*, vol. 19, no. 4, pp. 53–58, 2012.

[31] R. Guesmi, C. L. P. Farah, A. Kachouri, and M. Samet, "A novel design of chaos based S-boxes using genetic algorithm techniques," in *Proceedings of the IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*, pp. 678–684, IEEE, Doha, Qatar, November 2014.

[32] M. Ahmad, D. Bhatia, and Y. Hassan, "A novel ant colony optimization-based scheme for substitution box design," *Procedia Computer Science*, vol. 57, pp. 572–580, 2015.

[33] Y. Tian and Z. Lu, "S-box: six-dimensional compound hyperchaotic map and artificial bee colony algorithm," *Journal of Systems Engineering and Electronics*, vol. 27, no. 1, pp. 232–241, 2016.

[34] M. Ahmad, N. Mittal, P. Garg, and M. M. Khan, "Efficient cryptographic substitution box design using travelling salesman problem and chaos," *Perspectives in Science*, vol. 8, pp. 465–468, 2016.

[35] T. Özkaynak, R. Rhouma, and S. Belghith, "A novel method for designing S-box based on chaotic map and teaching–learning-based optimization," *Nonlinear Dynamics*, vol. 88, no. 2, pp. 1059–1074, 2017.

[36] H. A. Ahmed, M. F. Zolkipli, and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," *Neural Computing and Applications*, vol. 30, no. 171, pp. 1–10, 2018.

[37] T. Zhang, C. P. Chen, L. Chen, X. Xu, and B. Hu, "Design of highly nonlinear substitution boxes based on I-Ching operators," *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3349–3358, 2018.

[38] D. Lambić, "A novel method of S-box design based on chaotic map and composition method," *Chaos, Solitons & Fractals*, vol. 58, pp. 16–21, 2014.

[39] D. Lambić, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dynamics*, vol. 87, no. 4, pp. 2407–2413, 2017.

[40] A. Ullah, S. S. Jamal, and T. Shah, "A novel algebraic technique for the construction of strong substitution box," *Wireless Personal Communications*, vol. 99, no. 1, pp. 213–226, 2018.

[41] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," *Neural Computing and Applications*, vol. 31, no. 8, pp. 3317–3326, 2019.

[42] T. Ye and L. Zhimao, "Chaotic S-box: six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling," *Nonlinear Dynamics*, vol. 94, no. 3, pp. 2115–2126, 2018.

[43] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, and M. Aldape-Pérez, "Substitution box generation using chaos: an image encryption application," *Applied Mathematics and Computation*, vol. 332, pp. 123–135, 2018.

[44] L. Yi, X. Tong, Z. Wang, M. Zhang, H. Zhu, and J. Liu, "A novel block encryption algorithm based on chaotic S-box for wireless sensor network," *IEEE Access*, vol. 7, pp. 53079–53090, 2019.

[45] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proceedings of the 1985 Conference on the Theory and Application of Cryptographic Techniques*, pp. 523–534, Springer, Linz, Austria, April 1985.

[46] M. Khan, T. Shah, and S. I. Batool, "Construction of S-box based on chaotic Boolean functions and its application in image encryption," *Neural Computing and Applications*, vol. 27, no. 3, pp. 677–685, 2016.

[47] 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.