IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received June 22, 2020, accepted July 7, 2020, date of publication July 20, 2020, date of current version August 5, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3010615

Construction of Nonlinear Component of Block Cipher by Action of Modular Group $PSL(2, \mathbb{Z})$ on Projective Line $PL(GF(2^8))$

WEI GAO[1], BAZGHA IDREES[2], SOHAIL ZAFAR[2], AND TABASAM RASHID[2]
[1]School of Information Science and Technology, Yunnan Normal University, Kunming 650092, China
[2]Department of Mathematics, University of Management and Technology, Lahore 54770, Pakistan

Corresponding author: Sohail Zafar (sohailahmad04@gmail.com)

This work was supported in part by NSFC under Grant 11761083.

ABSTRACT Substitution box (S-Box) has a prominent significance being the fundamental nonlinear component of block cipher which fulfils confusion, one of the properties proposed by Claude Shannon in 1949. In this paper, we proposed an S-Box by using the action of modular group $PSL(2, \mathbb{Z})$ on projective line $PL(F_{257})$ over Galois field $GF(2^8)$. In the first step we obtained elements of $GF(2^8)$ by using powers of α, where α is the primitive root of irreducible polynomial $p(x)$ of order 8 over field $\mathbb{Z}_2$, then applied the generators of $PSL(2, \mathbb{Z})$ and followed steps to get rid of infinity from output. In the final step of proposed scheme, one of the permutations of S_{16} is applied which enhanced the possible number of S-Boxes obtained by any single specific irreducible polynomial $p(x)$ over field $\mathbb{Z}_2$ of order 8. We analyzed performance of the proposed 8×8 S-Box under cryptographic properties such as strict avalanche criterion, bit independence criterion, nonlinearity, differential approximation probability, linear approximation probability; and compared obtained results with a number of renowned S-Boxes. Lastly, we performed statistical analysis (which comprises of contrast analysis, homogeneity analysis, energy analysis, correlation analysis, entropy analysis and mean of absolute deviation analysis) on our proposed S-Box and obtained results have been compared with adequate number of S-Boxes.

INDEX TERMS Action of modular group, cryptographic properties' analyses, finite field, majority logic criterion, S-Box.

I. INTRODUCTION

In the present era with digitally advanced technologies and excessive usage of internet, secure transmission of digital data (images, videos, audios, military/office documents, etc.) has become most essential part for secure communication. There are three different ways which are being used for secure communication: cryptography, watermarking and steganography. Cryptography techniques are used to convert an understandable data form into a scrambled, distorted non-understandable form. Steganography techniques provide with embed/hide secret data inside a digital media cover. Although both provides information hiding techniques, but they are different in their working styles. Cryptography keeps content of the confidential data secret, on the other hand, steganography keeps existence of the confidential data secret (see [1]). Whereas, watermarking provides copyright preserving techniques. All of these vary from each other with respect to their working style but each of these have their own significance in secure communication. Cryptography has an important role in secure data transmission from insecure channels. It has various goals such as confidentiality, authentication, integrity, access control and non-repudiation [2].

Cryptography is an essential part for secure transmission of multimedia data (such as documents, images, audios and videos) [3] and there are two main categories of cryptography: symmetric cryptography and asymmetric cryptography. Block ciphers is a branch of symmetric key cryptography, in which both sender and receiver use the same key for encrypting and decrypting the data [4] and substitution box (S-Box), first introduced by Claude Shannon in [5], is the core nonlinear part of block ciphers, which provides confusion. Without developing confusion in a block cipher, it becomes susceptible to different attacks. Therefore, deliberate construction of S-Box is required which must be capable of good confusion. Conventionally, an S-Box is known as look-up

The associate editor coordinating the review of this manuscript and approving it for publication was Yu-Chi Chen.

table and is used to replace one confidential symbol with one element of S-Box. Mathematically, S-Box is merely a mathematical mapping from GF(2^n) to GF(2^m). The main focus in developing a new S-Box is to search out new mathematical structures which may produce confusion in block ciphers. There are renowned modern cryptosystems namely data encryption standard (DES) [6], international data encryption algorithm (IDEA) [7] and advanced encryption standard (AES) which were developed under substitution-permutation network (SPN) [8]–[10] in which Shannon's properties of confusion and diffusion were practiced. Up to now, a number of image encryption schemes have been designed on SPN and other various techniques (see [11]–[34]).

Strength of any block cipher is based on the strength of S-Box. Therefore a number of new techniques have been proposed for the construction of S-Box which utilized different algebraic structures such as symmetric groups, Galois fields, Galois rings, left almost semi-groups, linear fractional transformation, action of projective general linear group, action of projective special linear group and coset diagram (see [26], [35]–[41]). In a research paper [42], the authors proposed an S-Box developed by using action of PGL(2,GF(2^8)) on Galois field. Their proposed S-Box is found to have same nonlinearity as of AES but has two fixed points (output value is equal to the input value) which are 122 and 208. In [43], authors introduced a technique for the construction of S-Box on the basis of coset diagram in which a map is defined in order to remove the fixed points of the substitution box and obtain a bijective S-Box. In [44], the authors studied results of nonlinearity by changing the primitive irreducible polynomial for generating members of Galois field and found that deliberately selected irreducible polynomial may enhance the strength of those S-Boxes which are developed on the grounds of algebraic structure Galois field but their proposed S-Box found non-bijective. Authors in [45] proposed a novel algebraic technique for S-Box construction by group action on ring $\mathbb{Z}_{1024}$. Their illustrated S-Box showed some good result of nonlinearity and offset to SAC but we found that there is one fixed point which is 160. In [46], authors proposed a new algorithm by taking composition of inversion function and action of S_8 symmetric group on Galois field. Their illustrated S-Box found to be highly nonlinear and bijective but had four fixed points which are 0, 1, 48 and 115. In [47], authors first proposed an S-Box on a piecewise linear chaotic map and then provided adaptive improvement technique to improve differential approximation probability of S-Box. In [48], authors proposed a postprocess technique for the improvement of chaos-based S-Boxes. In [49], authors utilized extended logistic map for the generation of S-Box. In [50], authors proposed an S-Box by involving coset diagrams for the action of a quotient of the modular group on the projective line over the finite field and used Fibonacci sequence for the selection of vertices of coset diagram. In [51], authors provided a novel algebraic theoretical approach for improving strength of S-Box and found good results.

Although there are available new approaches for the construction of S-Box on algebraic structures, which even provide highest nonlinearity, i.e., 112 but they do not pass the criterion of having no fixed point.

Recently, authors proposed a novel genetic technique for construction of bijective S-Box in [52] by selecting n Boolean functions (treating as the chromosomes of an S-Box) into $2^n \times n$ matrix.

According to the existing literature, it is evident that research of finding cryptographically strong S-Boxes by novel techniques, based on either chaos theory or algebraic theory, is still in progress.

An S-Box should not only be robust against differential and linear attacks but also be up to the mark under analysis for different properties namely nonlinearity, strict avalanche criterion (SAC) and bit independence criterion (BIC) (see [53]–[56]).

In this paper, we proposed an algorithm for construction of (8×8) S-Box by using the action of modular group PSL(2, $\mathbb{Z}$) on projective line PL(GF(2^8)) and involving the structure of Galois field GF(2^8) in a simple unique way. Furthermore, we evaluated the performance of illustrated S-Box under said criteria. This paper is organized as follows: in Section II we discussed preliminary necessary topics for the construction of proposed S-Box; in Section III algorithm is given for proposed S-Box which is then analyzed in Section IV and finally conclusion is given in Section VI.

II. PRELIMINARIES

Necessary definitions used in the construction of S-Box are given below:

A. GALOIS FIELD

For every prime p, there exist a Galois field GF(p^m) provided that m is a positive non-zero integer. In GF(p^m), every element can be uniquely represented by the linear combination of its standard basis $\{b_0, b_1, b_2, \ldots, b_{m-1}\} = \left\{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{m-1}\right\}$ with co-efficients from GF(p) where α is the primitive element and root of irreducible polynomial $p(x)$, of degree m, over GF(p) [57], so GF(p^m) $= \mathbb{Z}_p[x]/\langle p(x)\rangle$. There are total 16 primitive irreducible polynomials over GF(2), if $p = 2$ and $m = 8$ which are enlisted in Table 1.

All the elements of $\mathrm{GF}\left(2^8\right) = \mathbb{Z}_2[x]/\langle x^8+x^7+x^3+x^2+1\rangle$ in the form of powers of α and their corresponding polynomials form (expressed as binary numbers with left maximum significance bit) are given in Table 2.

There are total 256 monic polynomials over $\mathbb{Z}_2$ of degree 8, of which only 30 are irreducible polynomials and 16 are primitive irreducible polynomials (see [58]). It should be noted that members from $\alpha^{255} = \alpha^0$ to α^7 have same polynomial expression for all 16 primitive irreducible polynomials of Table 1 as calculated in Table 2 where α^8 comes from $p(\alpha) = 0$.

All successive powers of α are obtained and reduced under operations of binary addition (i.e. of modulo 2) and

TABLE 1. Primitive irreducible polynomials over GF(2) of order 8.

Polynomial Form	Vector Form (v_j)	Hexadecimal Form (h_j)	Decimal Form (δ_j)
$x^8+x^4+x^3+x^2+1$	(1,0,0,0,1,1,1,0,1)	11D	285
$x^8+x^5+x^3+x+1$	(1,0,0,1,0,1,0,1,1)	12B	299
$x^8+x^5+x^3+x^2+1$	(1,0,0,1,0,1,1,0,1)	12D	301
$x^8+x^6+x^3+x^2+1$	(1,0,1,0,0,1,1,0,1)	14D	333
$x^8+x^6+x^4+x^3+x^2+x+1$	(1,0,1,0,1,1,1,1,1)	15F	351
$x^8+x^6+x^5+x+1$	(1,0,1,1,0,0,0,1,1)	163	355
$x^8+x^6+x^5+x^2+1$	(1,0,1,1,0,0,1,0,1)	165	357
$x^8+x^6+x^5+x^3+1$	(1,0,1,1,0,1,0,0,1)	169	361
$x^8+x^6+x^5+x^4+1$	(1,0,1,1,1,0,0,0,1)	171	369
$x^8+x^7+x^2+x+1$	(1,1,0,0,0,0,1,0,1)	187	391
$x^8+x^7+x^3+x^2+1$	(1,1,0,0,0,1,1,0,1)	18D	397
$x^8+x^7+x^5+x^3+1$	(1,1,0,1,0,1,0,0,1)	1A9	425
$x^8+x^7+x^6+x+1$	(1,1,1,0,0,0,0,1,1)	1C3	451
$x^8+x^7+x^6+x^3+x^2+x+1$	(1,1,1,0,0,1,1,1,1)	1CF	463
$x^8+x^7+x^6+x^5+x^2+x+1$	(1,1,1,1,0,0,1,1,1)	1E7	487
$x^8+x^7+x^6+x^5+x^4+x^2+1$	(1,1,1,1,1,0,1,0,1)	1F5	501

multiplication modulo $p(x)$ (see [57]). Finally, all obtained powers of α are represented in the form of decimal numbers and binary numbers.

B. MODULAR GROUP

The set of all Möbius transformations (which are linear fractional transformations) of Poincaré hyperbolic plane $\mathcal{H}^2 = \{z \in \mathbb{C} : z = x + iy, y \geq 0\} \cup \{\infty\}$ defined by $h \mapsto ah + b/ch + d; a, b, c, d \in \mathbb{Z}, ad - cb = 1$, forms a group which is known as modular group Γ (see [3]). Modular group is free product of $\mathbb{Z}_2$ and $\mathbb{Z}_3$ which is isomorphic to projective group PSL(2, $\mathbb{Z}$) of special linear group SL(2, $\mathbb{Z}$) $= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, \begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1 \right\}$ by its center $\{\pm I\}$, i.e. $\Gamma \cong \mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,Z)/\langle \pm \mathrm{I} \rangle$. A finite presentation of modular group is $\Gamma = \langle x, y : x^2 = y^3 = 1 \rangle$ where x and y are linear fractional transformations defined as $g \mapsto \frac{-1}{g}$ and $g \mapsto \frac{g-1}{g}$, respectively (see [59]).

C. ACTION OF PSL(2, $\mathbb{Z}$) ON PL(GF(2^8))

A coset diagram is defined in [60] as merely a graphical representation of permutation action of a finitely-generated group S on a set X (also see [61]–[63]). Projective line $PL\left(F_q\right)$ is a projective space with $q+1$ points, where $p^m = q$ symbols are of form $[z, 1]$; $z \in F_q$ and one additional point is $[1, 0]$, therefore under bijection $[g_1, g_2] \leftrightarrow g_1/g_2$ projective line $\mathrm{PL}(F_q) = F_q \cup \{\infty\} = \{0, 1, 2, \ldots, q-1\} \cup \{\infty\}$ (see [64]). Consider the action of PSL(2, Z) on PL(F_{17}) $= \{0, 1, 2, 3, \ldots, 15, 16, \infty\}$. We apply permutation representation of x and y by calculating $g \longmapsto -1/g$ and $g \mapsto 1-1/g$ respectively (see Table 3). Permutation representation of x and y obtained by the action of modular group on PL(F_{17}) is as follows:

x : (0 ∞)(1 16) (2 8)(3 11)(4)(5 10) (6 14)(7 12)(9 15)(13) .

y : (0 ∞ 1) (2 9 16) (3 12 8) (11 4 5) (13 14 7) (15 10 6) .

Since in image encryption, all possible bytes can be considered as members of GF(2^8) therefore we may consider the action of PSL(2, $\mathbb{Z}$) on PL(GF(2^8)) in the making of nonlinear component of block cipher. To illustrate the proposed algorithm of S-Box, we worked on the members of GF(2^8) which are enlisted in Table 2 and obtained the results of action PSL(2, $\mathbb{Z}$) on GF(2^8) ∪ {∞} = {0, 1, 2, ..., 255, ∞} by applying permutations x and y which are as follows:

x : (0 ∞) (1 1) (2 198) (3 132) (4 99) (5 124) (6 66) (7 234) (8 247) (9 221) (10 62) (11 113) (12 33) (13 153) (14 117) (15 175) (16 189) (17 101) (18 168) (19 141) (20 31) (21 144) (22 254) (23 119) (24 214) (25 103) (26 138) (27 75) (28 252) (29 47) (30 145) (32 152) (34 244) (35 51) (36 84) (37 155) (38 128) (39 158) (40 201) (41 95) (42 72) (43 166) (44 127) (45 57) (46 253) (48 107) (49 250) (50 245) (52 69) (53 123) (54 227) (55 194) (56 126) (58 209) (59 115) (60 142) (61 136) (63 112) (64 76) (65 171) (67 235) (68 122) (70 223) (71 120) (73 167) (74 139) (77 170) (78 79) (80 162) (81 160) (82 233) (83 86) (85 154) (87 232) (88 249) (89 197) (90 218) (91 231) (92 184) (93 237) (94 200) (96 243) (97 110) (98 125) (100 188) (102 215) (104 228) (105 241) (106 251) (108 183) (109 180) (111 242) (114 208) (116 174) (118 255) (121 222) (129 159) (130 147) (131 148) (133 199) (134 179) (135 165) (137 143) (140 169) (146 149) (150 203) (151 207) (156 225) (157 216) (161 163) (164 178) (172 239) (173 204) (176 186) (177 213) (181 182) (185 236) (187 212) (190 210) (191 192) (193 211) (195 226) (196 248) (202 206) (205 238) (217 224) (219 230) (2202 46)(229 240).

TABLE 2. Elements of GF$\left(2^8\right)$ when $p(x) = x^8 + x^7 + x^3 + x^2 + 1$.

Power α^i	Decimal d_i	Binary b_i	Power α^i	Decimal d_i	Binary b_i
α^{0}	1	00000001	α^{1}	2	00000010
α^{2}	4	00000100	α^{3}	8	00001000
α^{4}	16	00010000	α^{5}	32	00100000
α^{6}	64	01000000	α^{7}	128	10000000
α^{8}	141	10001101	α^{9}	151	10010111
α^{10}	163	10100011	α^{11}	203	11001011
α^{12}	27	00011011	α^{13}	54	00110110
α^{14}	108	01101100	α^{15}	216	11011000
α^{16}	61	00111101	α^{17}	122	01111010
α^{18}	244	11110100	α^{19}	101	01100101
α^{20}	202	11001010	α^{21}	25	00011001
α^{22}	50	00110010	α^{23}	100	01100100
α^{24}	200	11001000	α^{25}	29	00011101
α^{26}	58	00111010	α^{27}	116	01110100
α^{28}	232	11101000	α^{29}	93	01011101
α^{30}	186	10111010	α^{31}	249	11111001
α^{32}	127	01111111	α^{33}	254	11111110
α^{34}	113	01110001	α^{35}	226	11100010
α^{36}	73	01001001	α^{37}	146	10010010
α^{38}	169	10101001	α^{39}	223	11011111
α^{40}	51	00110011	α^{41}	102	01100110
α^{42}	204	11001100	α^{43}	21	00010101
α^{44}	42	00101010	α^{45}	84	01010100
α^{46}	168	10101000	α^{47}	221	11011101
α^{48}	55	00110111	α^{49}	110	01101110
α^{50}	220	11011100	α^{51}	53	00110101
α^{52}	106	01101010	α^{53}	212	11010100
α^{54}	37	00100101	α^{55}	74	01001010
α^{56}	148	10010100	α^{57}	165	10100101
α^{58}	199	11000111	α^{59}	3	00000011
α^{60}	6	00000110	α^{61}	12	00001100
α^{62}	24	00011000	α^{63}	48	00110000
α^{64}	96	01100000	α^{65}	192	11000000
α^{66}	13	00001101	α^{67}	26	00011010
α^{68}	52	00110100	α^{69}	104	01101000
α^{70}	208	11010000	α^{71}	45	00101101
α^{72}	90	01011010	α^{73}	180	10110100
α^{74}	229	11100101	α^{75}	71	01000111
α^{76}	142	10001110	α^{77}	145	10010001
α^{78}	175	10101111	α^{79}	211	11010011
α^{80}	43	00101011	α^{81}	86	01010110
α^{82}	172	10101100	α^{83}	213	11010101
α^{84}	39	00100111	α^{85}	78	01001110
α^{86}	156	10011100	α^{87}	181	10110101
α^{88}	231	11100111	α^{89}	67	01000011
α^{90}	134	10000110	α^{91}	129	10000001
α^{92}	143	10001111	α^{93}	147	10010011
α^{94}	171	10101011	α^{95}	219	11011011
α^{96}	59	00111011	α^{97}	118	01110110
α^{98}	236	11101100	α^{99}	85	01010101
α^{100}	170	10101010	α^{101}	217	11011001
α^{102}	63	00111111	α^{103}	126	01111110
α^{104}	252	11111100	α^{105}	117	01110101
α^{106}	234	11101010	α^{107}	89	01011001
α^{108}	178	10110010	α^{109}	233	11101001
α^{110}	95	01011111	α^{111}	190	10111110
α^{112}	241	11110001	α^{113}	111	01101111
α^{114}	222	11011110	α^{115}	49	00110001
α^{116}	98	01100010	α^{117}	196	11000100
α^{118}	5	00000101	α^{119}	10	00001010
α^{120}	20	00010100	α^{121}	40	00101000
α^{122}	80	01010000	α^{123}	160	10100000
α^{124}	205	11001101	α^{125}	23	00010111
α^{126}	46	00101110	α^{127}	92	01011100

TABLE 2. *(Continued.)* Elements of GF$\left(2^8\right)$ when $p(x) = x^8 + x^7 + x^3 + x^2 + 1$.

α^{128}	184	10111000	α^{129}	253	11111101
α^{130}	119	01110111	α^{131}	238	11101110
α^{132}	81	01010001	α^{133}	162	10100010
α^{134}	201	11001001	α^{135}	31	00011111
α^{136}	62	00111110	α^{137}	124	01111100
α^{138}	248	11111000	α^{139}	125	01111101
α^{140}	250	11111010	α^{141}	121	01111001
α^{142}	242	11110010	α^{143}	105	01101001
α^{144}	210	11010010	α^{145}	41	00101001
α^{146}	82	01010010	α^{147}	164	10100100
α^{148}	197	11000101	α^{149}	7	00000111
α^{150}	14	00001110	α^{151}	28	00011100
α^{152}	56	00111000	α^{153}	112	01110000
α^{154}	224	11100000	α^{155}	77	01001101
α^{156}	154	10011010	α^{157}	185	10111001
α^{158}	255	11111111	α^{159}	115	01110011
α^{160}	230	11100110	α^{161}	65	01000001
α^{162}	130	10000010	α^{163}	137	10001001
α^{164}	159	10011111	α^{165}	179	10110011
α^{166}	235	11101011	α^{167}	91	01011011
α^{168}	182	10110110	α^{169}	225	11100001
α^{170}	79	01001111	α^{171}	158	10011110
α^{172}	177	10110001	α^{173}	239	11101111
α^{174}	83	01010011	α^{175}	166	10100110
α^{176}	193	11000001	α^{177}	15	00001111
α^{178}	30	00011110	α^{179}	60	00111100
α^{180}	120	01111000	α^{181}	240	11110000
α^{182}	109	01101101	α^{183}	218	11011010
α^{184}	57	00111001	α^{185}	114	01110010
α^{186}	228	11100100	α^{187}	69	01000101
α^{188}	138	10001010	α^{189}	153	10011001
α^{190}	191	10111111	α^{191}	243	11110011
α^{192}	107	01101011	α^{193}	214	11010110
α^{194}	33	00100001	α^{195}	66	01000010
α^{196}	132	10000100	α^{197}	133	10000101
α^{198}	135	10000111	α^{199}	131	10000011
α^{200}	139	10001011	α^{201}	155	10011011
α^{202}	187	10111011	α^{203}	251	11111011
α^{204}	123	01111011	α^{205}	246	11110110
α^{206}	97	01100001	α^{207}	194	11000010
α^{208}	9	00001001	α^{209}	18	00010010
α^{210}	36	00100100	α^{211}	72	01001000
α^{212}	144	10010000	α^{213}	173	10101101
α^{214}	215	11010111	α^{215}	35	00100011
α^{216}	70	01000110	α^{217}	140	10001100
α^{218}	149	10010101	α^{219}	167	10100111
α^{220}	195	11000011	α^{221}	11	00001011
α^{222}	22	00010110	α^{223}	44	00101100
α^{224}	88	01011000	α^{225}	176	10110000
α^{226}	237	11101101	α^{227}	87	01010111
α^{228}	174	10101110	α^{229}	209	11010001
α^{230}	47	00101111	α^{231}	94	01011110
α^{232}	188	10111100	α^{233}	245	11110101
α^{234}	103	01100111	α^{235}	206	11001110
α^{236}	17	00010001	α^{237}	34	00100010
α^{238}	68	01000100	α^{239}	136	10001000
α^{240}	157	10011101	α^{241}	183	10110111
α^{242}	227	11100011	α^{243}	75	01001011
α^{244}	150	10010110	α^{245}	161	10100001
α^{246}	207	11001111	α^{247}	19	00010011
α^{248}	38	00100110	α^{249}	76	01001100
α^{250}	152	10011000	α^{251}	189	10111101
α^{252}	247	11110111	α^{253}	99	01100011
α^{254}	198	11000110			

TABLE 3. Action of PSL(2, ℤ) on PL (F_{17}).

G	x(g) = −1/g	y(g) = 1 − 1/g
∞	x(∞) = (−1/∞) = 16 × 0 = 0	y(∞) = 1 − (1/∞) = 1 − 0 = 1
0	x(0) = (−1/0) = 16 × ∞ = ∞	y(0) = 1 − (1/0) = 1 − ∞ = ∞
1	x(1) = (−1/1) = 16 × 1 = 16	y(1) = 1 − (1/1) = 1 − 1 = 0
2	x(2) = (−1/2) = 16 × 9 = 8	y(2) = 1 − (1/2) = 1 − 9 = 9
3	x(3) = (−1/3) = 16 × 6 = 11	y(3) = 1 − (1/3) = 1 − 6 = 12
4	x(4) = (−1/4)	y(4) = 1 − (1/4)
	= 16 × 13 = 4	= 1 − 13 = 5
5	x(5) = (−1/5) = 16 × 7 = 10	y(5) = 1 − (1/5) = 1 − 7 = 11
6	x(6) = (−1/6) = 16 × 3 = 14	y(6) = 1 − (1/6) = 1 − 3 = 15
7	x(7) = (−1/7) = 16 × 5 = 12	y(7) = 1 − (1/7) = 1 − 5 = 13
8	x(8) = (−1/8) = 16 × 15 = 2	y(8) = 1 − (1/8) = 1 − 15 = 3
9	x(9) = (−1/9) = 16 × 2 = 15	y(9) = 1 − (1/9) = 1 − 2 = 16
10	x(10) = (−1/10) = 16 × 12 = 5	y(10) = 1 − (1/10) = 1 − 12 = 6
11	x(11) = (−1/11) = 16 × 14 = 3	y(11) = 1 − (1/11) = 1 − 14 = 4
12	x(12) = (−1/12) = 16 × 10 = 7	y(12) = 1 − (1/12) = 1 − 10 = 8
13	x(13) = (−1/13) = 16 × 4 = 13	y(13) = 1 − (1/13) = 1 − 4 = 14
14	x(14) = (−1/14) = 16 × 11 = 6	y(14) = 1 − (1/14) = 1 − 11 = 7
15	x(15) = (−1/15) = 16 × 8 = 9	y(15) = 1 − (1/15) = 1 − 8 = 10
16	x(16) = (−1/16) = 16 × 16 = 1	y(16) = 1 − (1/16) = 1 − 16 = 2

y : (1 0 ∞) (2 199 132) (3 133 198) (4 98 124) (5 12 599) (6 67 234) (7 23 566) (8 246 221) (9 220 247) (10 63 113) (11 112 62) (12 32 153) (13 152 33) (14 116 175) (15 174 117) (16 188 101) (17 100 189) (18 169 141) (19 140 168) (20 30 144) (21 14 531) (22 255 119) (23 118 254) (24 215 103) (25 102 214) (26 139 75) (27 741 38) (28 253 47) (29 46 252) (34 24 551) (35 50 244) (36 85 155) (37 154 84) (38 129 158) (39159128) (40 20 095) (41 94 201) (42 73 166) (43 16 772) (44 12 657) (45 56 127) (48 106 250) (49 251 107) (52 68 123) (53 12 269) (54 226 194) (55 195 227) (58 208 115) (59 114 209) (60 143 136) (61 137 142) (64 77 171) (65 17 076) (70 222 120) (71 121 223) (78) (79) (80 163 160) (81 161 162) (82 23 286) (83 87 233) (88 248 197) (89 196 249) (90 219 231) (91 230 218) (92 185 237) (93 236 184) (96 242 110) (97 111 243) (104 229 241) (105 240 228) (108 182 180) (109 181 183) (130 146 148) (131 149 147) (134 178 165) (135 164 179) (150 202 207) (151 206 203) (156 224 216) (157 217 225) (172 238 204) (173 205 239) (176 187 213) (177 212 186) (190 211 192) (191 193 210).

III. CONSTRUCTION TECHNIQUE FOR S-BOX

We utilized both permutations x and y in construction of 8×8 S-Box. Steps which are taken in the construction of S-Box S_h^8 are as follows:

i. Choose any primitive irreducible polynomial $p(x)$ whose hexadecimal value is h from the list available in Table 1 and prepare members of $GF(2^8)$, as shown in Table 2.
ii. Take $i = 1$, where i is being considered as power of primitive root α.
iii. Convert i into hexadecimal value rc (say) for taking decision of row r and column c of proposed S-Box to enter the output value corresponding to input i.
iv. Convert α^i into its numerical decimal value d_i (say) (as are available in Table 2) and calculate permutation x for d_i, i.e. $(d_i)\,x = t$ (say).
v. Take t as power of primitive root and find out its corresponding decimal value d_t by using Table 2.
vi. Further calculate permutation y twice time for d_t, i.e. $((d_t)\,y)\,y$ and enter in row r and column c which is obtained in Step iii, i.e. $s_{rc} = ((d_t)\,y)\,y$.
vii. Do $i = i + 1$.
viii. Repeat Steps iii-vii until $i = 254$.
ix. In Step iv, if $t = 255$ for some value of i, then set $s_{rc} = 0$.
x. For $i = 255$, do Steps from iii to vi, skip Step iv and set $t = 1$.
xi. Take δ_j, the decimal value (from Table 1), of irreducible polynomial which was chosen in Step i. After dropping the maximum significance bit (MSB), convert δ_j into hexadecimal value $r'c'$; set values of s_{00} equal to value of s_{FF} (which is calculated in step x); set value of s_{FF} equal to the already calculated value of $s_{r'c'}$ and set $s_{r'c'} = 1$.
xii. Apply any one of the permutations (selected deliberately) from symmetric group S_{16} on rows (or columns).

We developed illustrated S-Box and followed steps whose explanation is given below:

i. We opted $p(x) = x^8 + x^7 + x^3 + x^2 + 1$ primitive irreducible polynomial whose hexadecimal value is $h = 18D$, therefore we named it as S_{18D}^8.
ii. We set $i = 1$.
iii. We converted i into hexadecimal form which gave value 01 and taken as $r = 0, c = 1$.
iv. We converted $\alpha^i = \alpha^1$ into its decimal form that is $d_i = d_1 = 2$ and applied x permutation once on it $d_i(x) = d_1(x) = 2(x) = 198 = t$.

TABLE 4. Tentative S-box S^{8}_{18D}.

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

TABLE 5. S-box S^{8}_{18D}, generated by proposed algorithm.

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

v. We converted $\alpha^{t} = \alpha^{198}$ into its decimal form that is $d_t = d_{198} = 135$.

vi. We applied y permutation twice on it that is $(((d_t)\,y)\,y) = (((135)\,y)\,y) = (164)\,y = 179$ and stored in row $= 0$, column $= 1$ of tentative S-Box.

vii. We increased value of i by 1 and got $i = 2$.

viii. We repeated steps from iii to vii until $i = 254$.

ix. For $i = 97$ we got $t = 255$ in step iv, so we stored $s_{61} = 0$.

x. For $i = 255$,we obtained $r = F$ and $c = F$, set $t = 1$, consequently we got $d_t = d_1 = 2$ and $(((d_t)\,y)\,y) = (((2)\,y)\,y) = (199)\,y = 132$, i.e., $s_{FF} = 132$.

xi. We took δ_{11} that is 397, converting into hexadecimal value with left maximum significant bit and after dropping maximum bit we got decimal value 141 whose hexadecimal value $8D$, that is $r' = 8$ and $c' = D$. We shifted the values of $s_{FF} = 132$ to s_{00}, value of $s_{r'c'} = s_{8D} = 119$ to s_{FF} and set $s_{r'c'} = s_{8D} = 1$. So tentative S-Box is presented in Table 4.

TABLE 6. Balanced, bijective and number of fixed points comparison of various S-boxes.

S-Box	Balanced	Bijective	No. of Fixed Points
Proposed S^{8}_{18D}	✓	✓	0
Ref. [43]	✓	✓	0
Ref. [8]	✓	✓	0
Ref. [45]	✓	✓	1
Ref. [65]	✓	✓	0
Ref. [66]	✓	✓	0
Ref. [22]	✓	✓	0
Ref. [67]	✓	✓	0
Ref. [68]	✓	✓	0
Ref. [69]	✓	✓	1
Ref. [70]	✓	✓	0
Ref. [71]	✓	✓	2
Ref. [72]	✓	✓	0
Ref. [73]	×	×	1

xii. In the final step, we arranged rows of tentative S-Box as R_{16} R_{13} R_{6} R_{10} R_{12} R_{7} R_{8} R_{3} R_{15} R_{14} R_{5} R_{11} R_{9} R_{2} R_{4} R_{1} and obtained the final S-Box which is shown in Table 5.

TABLE 7. Nonlinearity comparison.

S-Box	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Minimum Value	Maximum Value	Average Value
Proposed S_{18D}^8	106	108	106	108	106	106	106	106	106	108	106.5
Ref. [43]	108	106	108	108	108	104	106	106	104	108	106.75
Ref. [8]	112	112	112	112	112	112	112	112	112	112	112
Ref.[45]	108	106	108	108	108	106	108	106	106	108	107.25
Ref. [65]	106	104	106	108	108	106	108	108	104	108	106.75
Ref. [66]	104	108	106	102	106	108	106	108	102	108	106
Ref. [22]	106	108	106	106	106	106	106	106	106	108	106.25
Ref. [67]	104	104	106	106	104	106	102	106	102	106	104.75
Ref. [68]	108	108	108	108	108	108	106	106	106	108	107.5
Ref. [69]	106	106	108	106	106	106	108	108	106	108	106.75
Ref. [70]	106	108	108	108	106	104	106	108	104	108	106.75
Ref. [71]	110	106	108	106	106	106	104	106	104	110	106.5
Ref. [72]	106	106	102	108	108	106	106	106	102	108	106
Ref. [73]	106	107	106	105	106	106	106	106	105	107	106

IV. ANALYSES OF PROPOSED S-BOX

There are a number of characteristics for any S-Box which ensure good performance of nonlinear component in any encryption algorithm. First of all, there should not be any fixed point in S-Box. Other characteristics includes nonlinearity, balanced, strict avalanche criterion (SAC), output bit independence criterion (BIC), differential approximation probability (DAP) and linear approximation probability (LAP). Description of all these characteristics and analysis for S-Box S_{18D}^8 are as follows:

A. BALANCEDNESS AND BIJECTIVITY

A Boolean function is called a balanced function if both the number of preimages mapped to 0 and number of preimages mapped to 1, are equal.

An S-Box is called balanced if all of its component Boolean functions are balanced. Mathematically, $n \times m$ S-Box $S : F_2^n \to F_2^m$ is called balanced if every image has exactly 2^{n-m} preimages (see [74]). An S-Box is called bijective if every output value (image) is associated to a unique input value (preimage). Therefore, n balanced component Boolean functions of $n \times n$ S-Box ensure the bijectivity of the S-Box. Comparison of balanced, bijective and number of fixed points is given in Table 4.

B. NONLINEARITY

To measure the strength of any S-Box, nonlinearity is one of the fundamental tools which was first introduced in [75] by Pieprzyk and Finkelstein. Minimum distance between a function f (say) and every linear function, is known as nonlinearity of that function, denoted by N_f and is calculated by $N_f = 2^n - \max \left|\sum_{x\in F_2^n} (-1)^{\beta f(x)+\alpha.x}\right|; \alpha, \beta \in F_2^n, \beta \neq 0$. The higher nonlinearity implies the strong S-Box. For S-Box s:GF(2^n) $\to$GF(2^n), the upper bound of nonlinearity is $2^{n-1} - 2^{\frac{n}{2}-1}$ (see [58]). In case of $n = 8$, the upper bound is 120 but literature shows that the value of nonlinearity which could be achieved uptill now is 112 (see [8], [58]). Nonlinearity of all component boolean functions of S_{18D}^8 in the comparison of various S-Boxes is given in Table 7.

C. STRICT AVALANCHE CRITERION

Two characteristics, namely completeness and avalanche effect were combined by A. F. Webster and S. E. Tavares in [76]; was named as strict avalanche criterion (SAC), which states that every output bit should change, with a probability of $1/2$, whenever a single input bit is altered. Since proposed S-Box is a map from GF(2^8) to itself, so inputs/outputs are of 8 bits namely $b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7$; and one of 8 output bits may consequently affect/alter whenever anyone of 8 input bits is altered. SAC for all component Boolean functions of S_{18D}^8 is given in Table 8, showing that the average value of SAC is 0.4990 which is up to the mark. According to the bound set available in paper [77], offset value of SAC is acceptable if it is less than or equal to 0.030 and proposed S-Box is showing 0.0330 offset value for SAC. SAC of S_{18D}^8 is compared in IV-F, which shows that average value is very close to desired value 0.5.

D. OUTPUT BIT INDEPENDENCE CRITERION

Out bit independence criterion is also very important criterion which states that if for all bits $i, j, k \in \{0, 1, 2, \ldots, n\}$ such that $j \neq k$, output bits j and k changes independently, whenever i is altered (see [78], [79]). Value of BIC is calculated with the help of correlation co-efficient, if $\rho_{jk}(i)$ be the correlation co-efficient of j^{th} and k^{th} output bits when i^{th} input bit is altered then bit independence criterion between b_j and b_k is given by BIC$(b_j, b_k) = \max_{0\leq i\leq n} |\rho_{jk}(i)|$, hence bit independence of S-Box s is given by BIC$(s) = \max BIC(b_j, b_k); 0 \leq j, k \leq n, j \neq k$ (see [54]).

It is also given in [75] that an S-Box meets with optimal value of BIC if $b_i \oplus b_j$ for all component Boolean functions $b_i, b_j; i \neq j, 1 \leq i, j \leq 8$ are nonlinear and fulfil the SAC. For S-Box S_{18D}^8, it is seen from Table 9 average value of BIC-SAC is 0.5033 and from Table 11 that the average value of BIC-Nonlinearity is 103.5714. Minimum, maximum

TABLE 8. SAC of S^8_{18D}.

0.4688	0.5625	0.4531	0.4531	0.5313	0.4844	0.5156	0.4531
0.4688	0.4688	0.5313	0.5313	0.5313	0.5469	0.4688	0.5313
0.5313	0.5781	0.5	0.4688	0.5469	0.4844	0.4844	0.5
0.4844	0.4688	0.5156	0.4688	0.5469	0.4688	0.4063	0.4531
0.5	0.4375	0.5313	0.5156	0.5	0.4844	0.4219	0.4844
0.5156	0.5	0.5	0.4531	0.4531	0.5	0.5313	0.4219
0.4844	0.4844	0.5469	0.4531	0.5313	0.4844	0.5469	0.5469
0.5625	0.4844	0.4844	0.5313	0.5625	0.5625	0.5469	0.4688

TABLE 9. BIC-SAC of S^8_{18D}.

–	0.4824	0.4863	0.5078	0.4668	0.5078	0.5215	0.5410
0.4824	–	0.5020	0.5059	0.4785	0.5195	0.4980	0.5078
0.4863	0.5020	–	0.4883	0.5098	0.5156	0.5137	0.5117
0.5078	0.5059	0.4883	–	0.5059	0.5000	0.4941	0.5254
0.4668	0.4785	0.5098	0.5059	–	0.5000	0.4980	0.4922
0.5078	0.5195	0.5156	0.5000	0.5000	–	0.5039	0.4961
0.5215	0.4980	0.5137	0.4941	0.4980	0.5039	–	0.5137
0.5410	0.5078	0.5117	0.5254	0.4922	0.4961	0.5137	–

TABLE 10. DDT of S^8_{18D} in compact form.

8	8	6	6	6	8	6	6	6	8	6	8	8	6	6	8
6	6	6	8	6	6	6	8	6	6	8	6	6	6	6	8
8	6	8	6	6	8	6	8	8	6	8	6	8	8	6	8
8	6	4	6	6	6	6	6	6	6	8	10	6	6	6	6
6	6	6	8	6	6	6	6	8	6	8	6	8	6	4	8
6	8	6	6	6	6	6	8	8	6	8	8	6	6	6	6
6	6	6	6	6	6	6	6	6	6	6	6	8	6	6	6
8	6	6	8	6	8	6	4	6	6	6	8	8	8	6	8
8	6	6	6	8	6	6	6	8	6	6	8	6	6	8	8
6	6	6	6	6	6	4	6	10	6	6	6	6	6	6	8
6	6	6	6	8	6	6	8	6	8	6	6	6	10	6	6
6	4	6	8	6	6	6	6	6	6	6	6	6	8	8	6
6	6	6	6	8	6	6	6	6	6	6	6	6	6	6	8
6	6	6	6	6	6	6	6	6	6	4	6	6	6	6	6
8	8	8	6	6	6	10	8	8	8	6	6	6	8	8	6
6	6	6	6	6	6	6	8	6	6	6	6	6	6	6	–

and average values of BIC-SAC and BIC-nonlinearity for various S-Boxes are given in Table 12 and Table 15 respectively.

E. DIFFERENTIAL APPROXIMATION PROBABILITY

An S-Box should be robust against differential cryptanalysis which ensures differential uniformity, which means that all

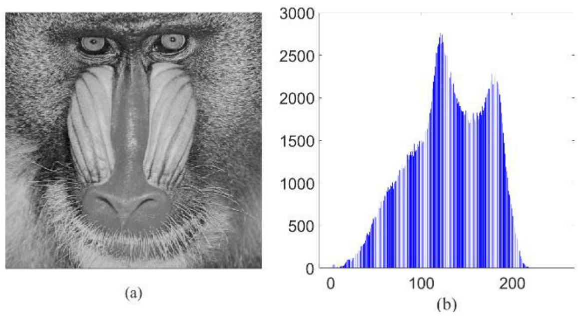

FIGURE 1. Plain image of mandrill baboon and its histogram.

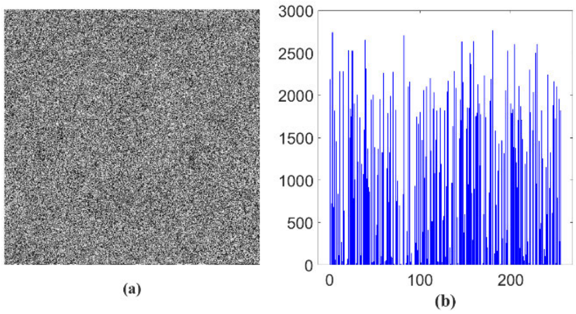

FIGURE 2. Cipher image by $\mathbf{S^8_{18D}}$ and its histogram.

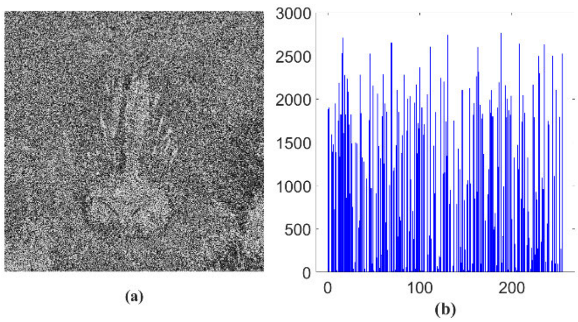

FIGURE 3. Cipher image and its histogram related to Ref. [43].

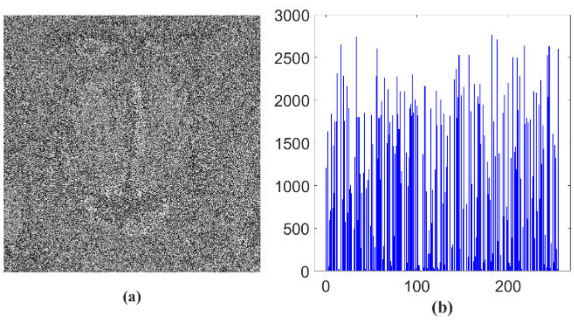

FIGURE 4. Cipher image and its histogram related to Ref. [8].

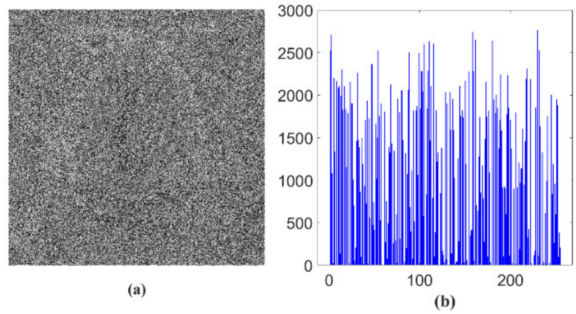

FIGURE 5. Cipher image and its histogram related to Ref. [45].

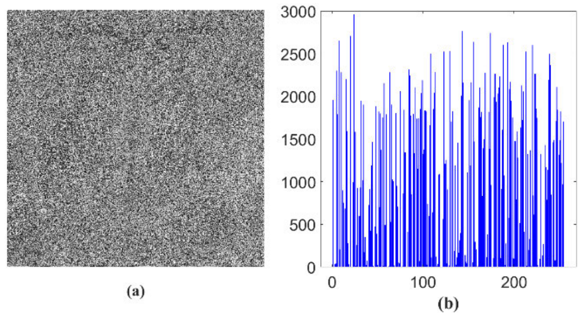

FIGURE 6. Cipher image and its histogram related to ref. [65].

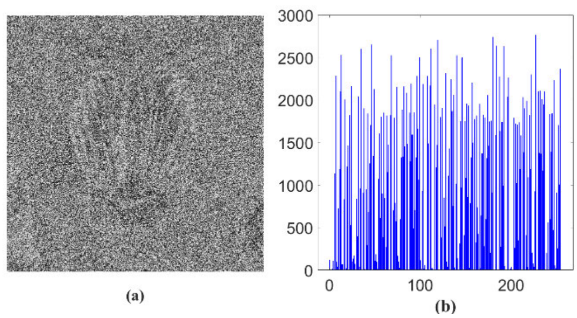

FIGURE 7. Cipher image and its histogram related to Ref. [66].

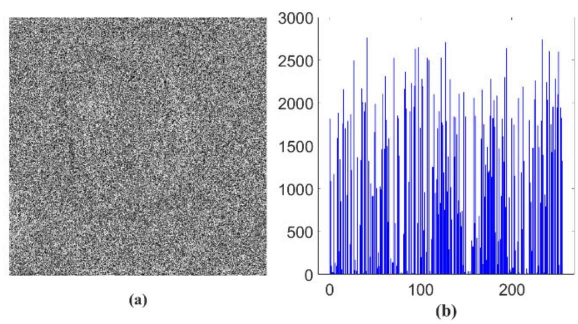

FIGURE 8. Cipher image and its histogram related to Ref. [22].

input differentials Δx and output differentials Δy are associated to each other uniformly and if S-Box s is a map from GF(2^n) to itself the optimal value of robustness is $\varepsilon = 1 - 2^{-(n-2)}$, which is given by $\varepsilon = \left(1 - R \times 2^{-n}\right)\left(1 - L \times 2^{-n}\right)$ where L = largest value in the difference distribution table (DDT) of s, R = number of non-zero entries in first row of DDT, in either cases the first entry, which is 2^n, in the first row is not counted [80].

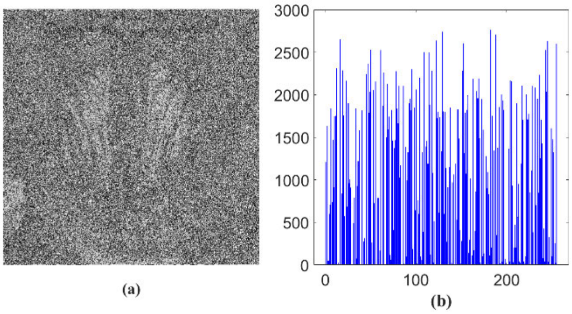

FIGURE 9. Cipher image and its histogram related to Ref. [67].

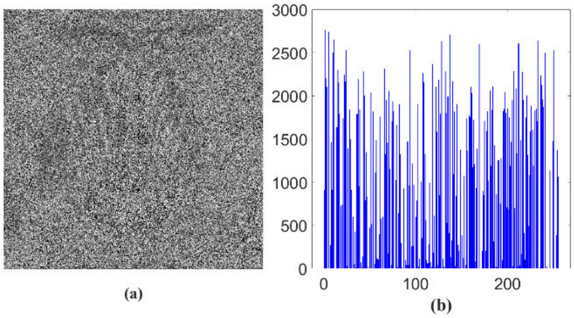

FIGURE 10. Cipher image and its histogram related to Ref. [68].

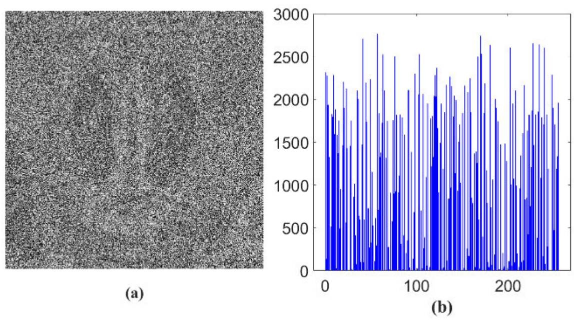

FIGURE 11. Cipher image and its histogram related to Ref. [69].

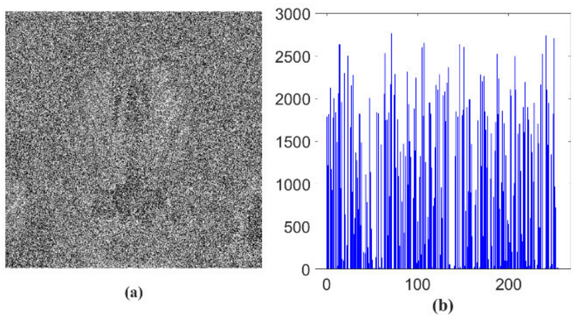

FIGURE 12. Cipher image and its histogram related to Ref. [70].

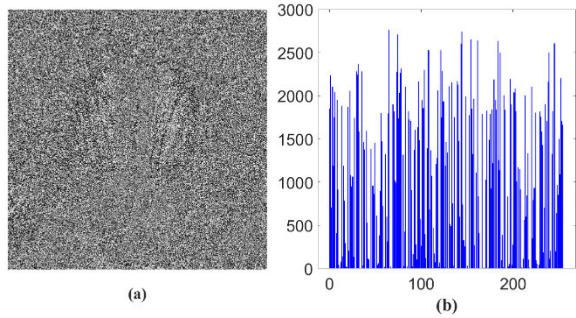

FIGURE 13. Cipher image and its histogram related to Ref. [71].

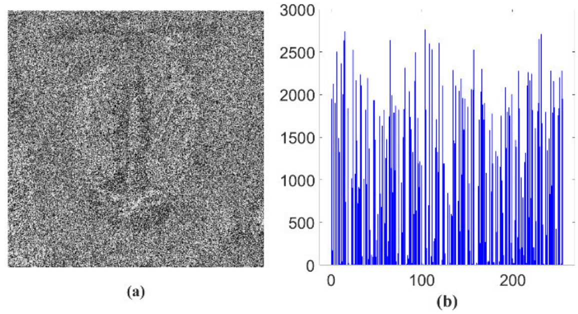

FIGURE 14. Cipher image and its histogram related to Ref. [72].

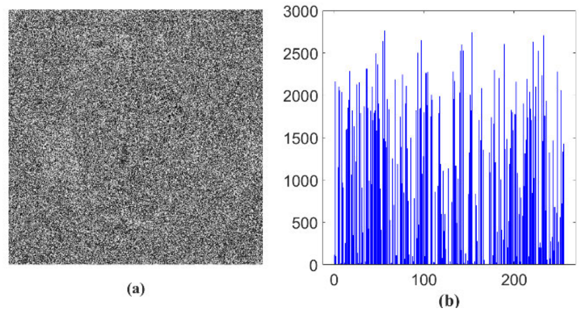

FIGURE 15. Cipher image and its histogram related to Ref. [73].

TABLE 11. BIC-nonlinearity of S^8_{18D}.

–	104	104	104	102	106	108	104
104	–	102	102	98	102	104	102
104	102	–	102	104	104	106	102
104	102	102	–	108	104	100	102
102	98	104	108	–	102	104	106
106	102	104	104	102	–	104	104
108	104	106	100	104	104	–	106
104	102	102	102	106	104	106	–

If n is an even integer then DDT is a matrix of size $2^n \times 2^n$ which can be presented in a compact form having size $2^{n/2} \times 2^{n/2}$. Compact form of S^8_{18D} is presented in Table 10. Differential approximation probability (DAP) is given by $DAP = \#\{x \in D_x : s(x) \oplus s(x + \Delta x) = \Delta y\}/2^n$ (see [53]). Differential approximation probability and robustness against differential attack of S^8_{18D} is given in Table 14 and compared with other substitution boxes.

TABLE 12. Comparison of BIC/SAC.

S-Box	Minimum Value	Maximum Value	Average Value
Proposed S^8_{18D}	0.4668	0.5	0.5033
Ref. [43]	0.4824	0.5098	0.5074
Ref. [8]	0.4805	0.5098	0.5046
Ref. [45]	0.4590	0.4883	0.4980
Ref. [65]	0.4609	0.5039	0.4997
Ref. [66]	0.4648	0.4785	0.5003
Ref. [22]	0.4648	0.5059	0.4984
Ref. [67]	0.4805	0.4941	0.5051
Ref. [68]	0.4648	0.4746	0.4978
Ref. [69]	0.4668	0.4941	0.5008
Ref. [70]	0.4668	0.4883	0.5022
Ref. [71]	0.4746	0.4941	0.5042
Ref. [72]	0.4824	0.5000	0.5023
Ref. [73]	0.4648	0.5020	0.5066

TABLE 13. Comparison of SAC.

S-Box	Min	Max	Average	Off Set
Proposed S^8_{18D}	0.4063	0.5781	0.4990	0.0332
Ref. [43]	0.4375	0.5781	0.5032	0.0310
Ref. [8]	0.4531	0.5625	0.5049	0.0264
Ref.[45]	0.4219	0.6094	0.5034	0.0293
Ref. [65]	0.4063	0.5938	0.5071	0.0344
Ref. [66]	0.4531	0.5938	0.5090	0.0291
Ref. [22]	0.4531	0.5938	0.5132	0.0327
Ref. [67]	0.4063	0.6094	0.5042	0.0359
Ref. [68]	0.4219	0.5781	0.4944	0.0369
Ref. [69]	0.4063	0.5938	0.4971	0.0288
Ref. [70]	0.4063	0.6250	0.4976	0.0303
Ref. [71]	0.4375	0.6406	0.5120	0.0320
Ref. [72]	0.4063	0.5938	0.5022	0.0305
Ref. [73]	0.4141	0.5938	0.5066	0.0317

F. LINEAR APPROXIMATION PROBABILITY

According to Matsui [56], linear approximation probability (LAP) is merely the imbalance of an event, and is used to find out the highest value of imbalance of event's outcome. Mathematically LAP is given by LAP $=$ max $\left|\#\left\{x \in D_x : x.M_x = s\left(x\right).M_y\right\}/2^n - 1/2\right|$ where M_x and M_y are masks applied for the parity of input bits, output bits respectively and $M_x, M_y \neq 0$.

Linear approximation of proposed S-Box is given in Table 16.

TABLE 14. DAP and robustness comparison of various S-boxes.

S-Box	DAP	Differential Uniformity	Robustness Against Differential Attack
Proposed S^8_{18D}	0.0391	10	0.9572
Ref. [43]	0.0469	12	0.9494
Ref. [8]	0.0156	4	0.9805
Ref. [45]	0.0469	12	0.9494
Ref. [65]	0.0546	14	0.9416
Ref. [66]	0.0391	10	0.9572
Ref. [22]	0.0391	10	0.9572
Ref. [67]	0.0391	10	0.9572
Ref. [68]	0.0391	10	0.9572
Ref. [69]	0.0391	10	0.9572
Ref. [70]	0.0391	10	0.9572
Ref. [71]	0.0391	10	0.9572
Ref. [72]	0.0469	12	0.9494
Ref. [73]	0.0469	12	0.9420

TABLE 15. Comparison of BIC/nonlinearity.

S-Box	Min	Max	Average
Proposed S^8_{18D}	98	108	103.5714
Ref. [43]	96	108	103.6429
Ref. [8]	112	112	112
Ref.[45]	98	108	104
Ref. [65]	110	113	111.1786
Ref. [66]	98	108	105.2857
Ref. [22]	98	108	102.9286
Ref. [67]	112	112	112
Ref. [68]	98	108	104.3571
Ref. [69]	98	106	102.9286
Ref. [70]	98	108	103.5714
Ref. [71]	98	108	104.5714
Ref. [72]	96	108	103
Ref. [73]	96	107	103

TABLE 16. LAP comparison of various S-boxes.

S-Box	Maximum Value	Minimum Value	Max LAP
Proposed S^8_{18D}	158	96	0.125
Ref. [43]	162	90	0.1484
Ref. [8]	144	112	0.062
Ref. [45]	162	94	0.1328
Ref. [65]	160	92	0.1406
Ref. [66]	160	96	0.1250
Ref. [22]	162	98	0.1328
Ref. [67]	164	98	0.1406
Ref. [68]	162	96	0.1328
Ref. [69]	164	94	0.1406
Ref. [70]	162	94	0.1328
Ref. [71]	160	94	0.1328
Ref. [72]	160	96	0.1250
Ref. [73]	161	91	0.1445

V. MAJORITY LOGIC CRITERION

In [81], authors proposed a criterion, which studies the image encryption strengths and weaknesses of S-Boxes with the help of statistical analysis and determines the suitability of S-Boxes in image encryption applications. This criterion is named as majority logic criterion (MLC) and consists of six component analyses which are contrast analysis, homogeneity analysis, energy analysis, correlation analysis, entropy analysis and mean of absolute deviation analysis. According to MLC, the above mentioned analyses are applied to cipher images obtained by different S-Boxes' transformations and an S-Box whose cipher image shows smaller correlation, smaller homogeneity, smaller energy, greater entropy, greater contrast and greater mean of absolute deviation among all cipher images obtained by other S-Boxes' transformations, is declared as suitable for image encryption applications.

TABLE 17. Comparison of majority logic criterion results.

Mandrill	Homogeneity	Energy	Correlation	Contrast	Entropy	MAD
Plain Image	0.7873	0.0890	0.8306	0.6178	7.3583	-
Proposed S^8_{18D}	0.4005	0.0163	0.0075	10.5005	7.3583	71.2226
Ref. [43]	0.4062	0.0166	0.0569	10.4158	7.3583	71.3197
Ref. [8]	0.4053	0.0161	0.0239	10.4086	7.3583	71.2156
Ref.[45]	0.4094	0.0165	0.0176	9.8992	7.3583	71.8425
Ref. [65]	0.4057	0.0163	0.0234	10.0883	7.3433	70.4696
Ref. [66]	0.4088	0.0163	0.0267	9.4156	7.3583	66.8848
Ref. [22]	0.4040	0.0168	0.0052	10.5320	7.3583	69.5640
Ref. [67]	0.4084	0.0161	0.0343	9.8414	7.3583	67.0389
Ref. [68]	0.4048	0.0168	0.0171	11.2483	7.3583	72.4740
Ref. [69]	0.4025	0.0163	0.0265	10.6417	7.3583	75.7859
Ref. [70]	0.4043	0.0164	0.0221	10.2033	7.3583	70.6633
Ref. [71]	0.4092	0.0167	0.0135	10.0461	7.3583	67.2953
Ref. [72]	0.4018	0.0164	0.0345	10.8808	7.3583	69.6049
Ref. [73]	0.4055	0.0168	0.0130	10.7985	7.3580	75.4576

We used 512 × 512 PNG image of Mandrill Baboon as a sample and calculated results of component analyses of MLC, which are shown in Table 17. Original image of Mandrill Baboon and cipher images after different S-Box transformations along with their corresponding histograms, are presented in Fig. 1 upto Fig. 15.

VI. CONCLUSION

In this article, a novel technique is proposed for the construction of bijective strong S-Box S^8_h. Construction is based on the action of modular group PSL$(2, \mathbb{Z})$ on projective line PL(GF(2^8)) and depends upon the selection of primitive irreducible polynomial h, for the generation of members of GF(2^8). Constructed S-Box S^8_h is then passed through an adequate number of existing tests to analyze its cryptographic strength; obtained results show that proposed technique is capable of constructing S-Boxes which possess high resistance against linear attack and differential attack. All coding is completed in MatlabR2019a and found that the proposed technique for generation of S-Box is easy and simple to implement.

For simulation of proposed technique, S-Box S^8_{18D} is constructed; which is then analyzed through different tests and found that S^8_{18D} has high nonlinearity and is strong enough to stand against different attacks. Generated S-Box significantly depends upon the selection of primitive irreducible polynomial h for generation of GF(2^8), therefore one may generate total sixteen different S-Boxes.

REFERENCES

[1] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Secur. Privacy*, vol. 1, no. 3, pp. 32–44, May 2003, doi: 10.1109/MSECP.2003.1203220.

[2] M. Khan and T. Shah, "A literature review on image encryption techniques," *3D Res.*, vol. 5, no. 4, Dec. 2014, Art. no. 29, doi: 10.1007/s13319-014-0029-0.

[3] A. Rafiq and M. Khan, "Construction of new S-boxes based on triangle groups and its applications in copyright protection," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 15527–15544, Jun. 2019, doi: 10.1007/s11042-018-6953-x.

[4] S. Kala and R. Thangaraj, "A study on different image encryption algorithms," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 2, pp. 1204–1206, 2014.

[5] C. E. Shannon, "Communication theory of secrecy systems*," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[6] IBM, "Data encryption standard," presented at the Int. Bus. Mach. Corp., 1977.

[7] J. Massey and X. Lai, "International data encryption algorithm," Signal Inf. Process. Lab., Eidgenössische Technische Hochschule (ETH) Zürich, Zürich, Switzerland, Tech. Rep. 9752, 1991.

[8] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. New York, NY, USA: Springer-Verlag, 2002, pp. 1–45, doi: 10.1007/978-3-662-04722-4.

[9] X. Lai and J. L. Massey, "A proposal for a new block encryption standard," in *Advances in Cryptology—EUROCRYPT*, vol. 473. 1991, pp. 389–404, doi: 10.1007/3-540-46877-3_35.

[10] E. F. Brickell, J. H. Moore, and M. R. Purtill, "Structure in the *S*-boxes of the DES (extended abstract)," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, vol. 263. Berlin, Germany: Springer, 1987, doi: 10.1007/3-540-47721-7_1.

[11] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.*, vol. 56, pp. 83–93, May 2014, doi: 10.1016/j.optlaseng.2013.12.003.

[12] R. Hamza and F. Titouna, "A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map," *Inf. Secur. J., Global Perspective*, vol. 25, nos. 4–6, pp. 162–179, Dec. 2016, doi: 10.1080/19393555.2016.1212954.

[13] A. Kadir, A. Hamdulla, and W.-Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik*, vol. 125, no. 5, pp. 1671–1675, Mar. 2014, doi: 10.1016/j.ijleo.2013.09.040.

[14] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011, doi: 10.1016/j.optcom.2011.04.001.

[15] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *Int. J. Bifurcation Chaos*, vol. 14, no. 10, pp. 3613–3624, Oct. 2004, doi: 10.1142/S021812740401151X.

[16] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Triple chaotic image scrambling on RGB–a random image encryption approach," *Secur. Commun. Netw.*, vol. 8, no. 18, pp. 3335–3345, Dec. 2015, doi: 10.1002/sec.1257.

[17] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012, doi: 10.1016/j.sigpro.2011.10.023.

[18] H. M. Waseem and M. Khan, "Information confidentiality using quantum spinning, rotation and finite state machine," *Int. J. Theor. Phys.*, vol. 57, no. 11, pp. 3584–3594, 2018, doi: 10.1007/s10773-018-3872-6.

[19] X. Wu, K. Wang, X. Wang, and H. Kan, "Lossless chaotic color image cryptosystem based on DNA encryption and entropy," *Nonlinear Dyn.*, vol. 90, no. 2, pp. 855–875, Oct. 2017, doi: 10.1007/s11071-017-3698-4.

[20] B. Yang and X. Liao, "A new color image encryption scheme based on logistic map over the finite field ZN," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 21803–21821, Aug. 2018, doi: 10.1007/s11042-017-5590-0.

[21] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools Appl.*, vol. 75, no. 11, pp. 6303–6319, Jun. 2016, doi: 10.1007/s11042-015-2573-x.

[22] N. A. Azam, U. Hayat, and I. Ullah, "Efficient construction of a substitution box based on a mordell elliptic curve over a finite field," *Frontiers Inf. Technol. Electron. Eng.*, vol. 20, no. 10, pp. 1378–1389, Oct. 2019, doi: 10.1631/FITEE.1800434.

[23] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Process.*, vol. 155, pp. 391–402, Feb. 2019, doi: 10.1016/j.sigpro.2018.10.011.

[24] U. Hayat, N. A. Azam, and M. Asif, "A method of generating 8×8 substitution boxes based on elliptic curves," *Wireless Pers. Commun.*, vol. 101, no. 1, pp. 439–451, Jul. 2018, doi: 10.1007/s11277-018-5698-1.

[25] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175–54188, 2020, doi: 10.1109/ACCESS.2020.2979827.

[26] Z. Gan, X. Chai, K. Yuan, and Y. Lu, "A novel image encryption algorithm based on LFT based S-boxes and chaos," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8759–8783, Apr. 2018, doi: 10.1007/s11042-017-4772-0.

[27] P. Cheng, H. Yang, P. Wei, and W. Zhang, "A fast image encryption algorithm based on chaotic map and lookup table," *Nonlinear Dyn.*, vol. 79, no. 3, pp. 2121–2131, Feb. 2015, doi: 10.1007/s11071-014-1798-y.

[28] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016, doi: 10.1016/j.sigpro.2016.03.021.

[29] J. B. Lima and L. F. G. Novaes, "Image encryption based on the fractional Fourier transform over finite fields," *Signal Process.*, vol. 94, pp. 521–530, Jan. 2014, doi: 10.1016/j.sigpro.2013.07.020.

[30] S. Yao, L. Chen, G. Chang, and B. He, "A new optical encryption system for image transformation," *Opt. Laser Technol.*, vol. 97, pp. 234–241, Dec. 2017, doi: 10.1016/j.optlastec.2017.07.005.

[31] N. Zhou, X. Liu, Y. Zhang, and Y. Yang, "Image encryption scheme based on fractional Mellin transform and phase retrieval technique in fractional Fourier domain," *Opt. Laser Technol.*, vol. 47, pp. 341–346, Apr. 2013, doi: 10.1016/j.optlastec.2012.08.033.

[32] V. Rozouvan, "Modulo image encryption with fractal keys," *Opt. Lasers Eng.*, vol. 47, no. 1, pp. 1–6, Jan. 2009, doi: 10.1016/j.optlaseng.2008.09.001.

[33] W. Gao, J. Sun, W. Qiao, and X. Zhang, "Digital image encryption scheme based on generalized mandelbrot-julia set," *Optik*, vol. 185, pp. 917–929, May 2019, doi: 10.1016/j.ijleo.2019.02.007.

[34] Y. Wang, K.-W. Wong, X. Liao, and T. Xiang, "A block cipher with dynamic S-boxes based on tent map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 14, no. 7, pp. 3089–3099, Jul. 2009, doi: 10.1016/j.cnsns.2008.12.005.

[35] I. Hussain, T. Shah, M. A. Gondal, W. A. Khan, and H. Mahmood, "A group theoretic approach to construct cryptographically strong substitution boxes," *Neural Comput. Appl.*, vol. 23, no. 1, pp. 97–104, Jul. 2013, doi: 10.1007/s00521-012-0914-5.

[36] I. Hussain, T. Shah, M. A. Gondal, M. Khan, and W. A. Khan, "Construction of new S-box using a linear fractional transformation," *World Appl. Sci. J.*, vol. 14, no. 12, pp. 1779–1785, 2011.

[37] I. Younas and M. Khan, "A new efficient digital image encryption based on inverse left almost semi group and lorenz chaotic system," *Entropy*, vol. 20, no. 12, p. 913, Nov. 2018, doi: 10.3390/e20120913.

[38] A. Razaq, H. A. Al-Olayan, A. Ullah, A. Riaz, and A. Waheed, "A novel technique for the construction of safe substitution boxes based on cyclic and symmetric groups," *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, Oct. 2018, doi: 10.1155/2018/4987021.

[39] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "An efficient approach for the construction of LFT S-boxes using chaotic logistic map," *Nonlinear Dyn.*, vol. 71, pp. 133–140, Jan. 2013 2013, doi: 10.1007/s11071-012-0646-1.

[40] N. Siddiqui, U. Afsar, T. Shah, and A. Qureshi, "A novel construction of S16 AES S-box," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 8, pp. 810–818, 2016.

[41] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, "A projective general linear group based algorithm for the construction of substitution box for block ciphers," *Neural Comput. Appl.*, vol. 22, no. 6, pp. 1085–1093, May 2013, doi: 10.1007/s00521-012-0870-0.

[42] 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 Adv.*, vol. 7, no. 3, Mar. 2017, Art. no. 035116, doi: 10.1063/1.4978264.

[43] 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," *Secur. Commun. Netw.*, vol. 48, p. 16, Nov. 2017, doi: 10.1155/2017/5101934.

[44] S. Mahmood, S. Farwa, M. Rafiq, S. M. J. Riaz, T. Shah, and S. S. Jamal, "To study the effect of the generating polynomial on the quality of nonlinear components in block ciphers," *Secur. Commun. Netw.*, vol. 2018, pp. 1–8, 2018, doi: 10.1155/2018/5823230.

[45] A. Ullah, S. S. Jamal, and T. Shah, "A novel algebraic technique for the construction of strong substitution box," *Wireless Pers. Commun.*, vol. 99, no. 1, pp. 213–226, Mar. 2018, doi: 10.1007/s11277-017-5054-x.

[46] Y. Naseer, T. Shah, D. Shah, and S. Hussain, "A novel algorithm of constructing highly nonlinear S-p-boxes," *Cryptography*, vol. 3, no. 1, p. 6, Jan. 2019, doi: 10.3390/cryptography3010006.

[47] Z. Bin Faheem, A. Ali, M. A. Khan, M. E. Ul-Haq, and W. Ahmad, "Highly dispersive substitution box (S-box) design using chaos," *ETRI J.*, Mar. 2020, doi: 10.4218/etrij.2019-0138.

[48] F. Artuğer and F. Özkaynak, "A novel method for performance improvement of chaos-based substitution boxes," *Symmetry*, vol. 12, no. 4, p. 571, Apr. 2020, doi: 10.3390/sym12040571.

[49] B. B. Cassal-Quiroga and E. Campos-Cantón, "Generation of dynamical S-boxes for block ciphers via extended logistic map," *Hindawi Math. Problems Eng.*, vol. 2020, p. 12, 2020, Art. no. 2702653, doi: 10.1155/2020/2702653.

[50] I. Shahzad, Q. Mushtaq, and A. Razaq, "Construction of new S-box using action of quotient of the modular group for multimedia security," *Hindawi Secur. Commun. Netw.*, vol. 2019, p. 13, 2019, Art. no. 2847801, doi: 10.1155/2019/2847801.

[51] M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar, and A. Razaq, "Comparison of pre and post-action of a finite Abelian group over certain nonlinear schemes," *IEEE Access*, vol. 8, pp. 39781–39792, 2020, doi: 10.1109/ACCESS.2020.2975880.

[52] Y. Wang, Z. Zhang, L. Y. Zhang, J. Feng, J. Gao, and P. Lei, "A genetic algorithm for constructing bijective substitution boxes with high nonlinearity," *Inf. Sci.*, vol. 523, pp. 152–166, Jun. 2020, doi: 10.1016/j.ins.2020.03.025.

[53] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, Jan. 1991, doi: 10.1007/BF00630563.

[54] I. Vergili and M. D. Yücel, "Avalanch and bit independence properties for the ensembles of randomly chosen n×n S-boxes," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 9, pp. 137–145, Sep. 2001.

[55] J. Seberry, X.-M. Zhang, and Y. Zheng, "Systematic generation of cryptographically robust s-boxes," presented at the Comput. Commun. Secur. (CCS), Fairfax, VA, USA, Aug. 10, 1993.

[56] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 1994, pp. 386–397.

[57] J. A. Gallian, *Contemporary Abstract Algebra*. Boston, MA, USA: Cengage Learning, 2017.

[58] T. Shah and D. Shah, "Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over $\mathbb{Z}_2$," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 1219–1234, Jan. 2019.

[59] Q. Mushtaq, "Some remarks on coset diagrams for the modular group," *Math. Croonicle*, vol. 16, pp. 69–77, Dec. 1987.

[60] Q. Mshtaq, "Coset diagrams for the modular group," Ph.D. dissertation, Dept. Math. Inst., Univ. Oxford, Oxford, U.K., 1983.

[61] A. Razaq, Q. Mushtaq, and A. Yousaf, "The number of circuits of length 4 in PSL(2,ℤ)-space," *Commun. Algebra*, vol. 46, no. 12, pp. 5136–5145, Dec. 2018, doi: 10.1080/00927872.2018.1461880.

[62] Q. Mushtaq and A. Razaq, "Homomorphic images of circuits in PSL(2,ℤ)-space," *Bull. Malaysian Math. Sci. Soc.*, vol. 40, no. 3, pp. 1115–1133, Jul. 2017, doi: 10.1007/s40840-016-0357-8.

[63] Q. Mushtaq, A. Razaq, and A. Yousaf, "On contraction of vertices of the circuits in coset diagrams for PSL(2,ℤ)," *Proc.-Math. Sci.*, vol. 129, no. 1, pp. 353–369, Feb. 2019, doi: 10.1007/s12044-018-0450-z.

[64] Q. Mushtaq and A. Rafiq, "Transformation of coset diagrams of action of PSL(2,ℤ) on Q($\sqrt{n}$)* into coset diagrams of action of PSL(2,ℤ)on PL(F_q)," in *Proc. 15th Int. Pure Math. Conf.*, Islamabad, Pakistan, 2014.

[65] A. Zahid and M. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, Mar. 2019, doi: 10.3390/sym11030437.
[66] S. S. Jamal, Attaullah, T. Shah, A. H. AlKhaldi, and M. N. Tufail, "Construction of new substitution boxes using linear fractional transformation and enhanced chaos," *Chin. J. Phys.*, vol. 60, pp. 564–572, Aug. 2019, doi: 10.1016/j.cjph.2019.05.038.
[67] B. Idrees, S. Zafar, T. Rashid, and W. Gao, "Image encryption algorithm using S-box and dynamic Hénon bit level permutation," *Multimedia Tools Appl.*, vol. 79, nos. 9–10, pp. 6135–6162, Mar. 2020, doi: 10.1007/s11042-019-08282-w.
[68] H. A. Ahmed, M. F. Zolkipli, and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7201–7210, Nov. 2019, doi: 10.1007/s00521-018-3557-3.
[69] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3317–3326, Aug. 2019, doi: 10.1007/s00521-017-3287-y.
[70] T. Ye and L. Zhimao, "Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling," *Nonlinear Dyn.*, vol. 94, no. 3, pp. 2115–2126, Nov. 2018, doi: 10.1007/s11071-018-4478-5.
[71] T. Farah, R. Rhouma, and S. Belghith, "A novel method for designing S-box based on chaotic map and teaching–learning-based optimization," *Nonlinear Dyn.*, vol. 88, no. 2, pp. 1059–1074, Apr. 2017, doi: 10.1007/s11071-016-3295-y.
[72] 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 Dyn.*, vol. 88, no. 4, pp. 2757–2769, Jun. 2017, doi: 10.1007/s11071-017-3409-1.
[73] 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," *Appl. Math. Comput.*, vol. 332, pp. 123–135, Sep. 2018, doi: 10.1016/j.amc.2018.03.019.
[74] D. Souravlias, K. E. Parsopoulos, and G. C. Meletiou, "Designing bijective S-boxes using algorithm portfolios with limited time budgets," *Appl. Soft Comput.*, vol. 59, pp. 475–486, Oct. 2017, doi: 10.1016/j.asoc.2017.05.052.
[75] J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," *IEE Proc. E-Comput. Digit. Techn.*, vol. 135, no. 6, pp. 325–335, Nov. 1988 1998.
[76] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, in LNCS. Santa Barbara, CA, USA: Springer, 1970, pp. 523–534, doi: 10.1007/3-540-39799-X_41.
[77] D. Lambic and M. Zivkovic, "Comparison of random S-box generation methods," *Publications de L'Institut Mathématique Nouvelle série, Tome*, vol. 93, no. 107, pp. 109–115, 2013, doi: 10.2298/PIM1307109L.
[78] A. F. Webster and S. E. Tavares, "On the design of S-box," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 218. Berlin, Germany: Springer, 1986, pp. 523–534.
[79] J. Detombe and S. Tavares, "Constructing large cryptographically strong S-boxes," in *Advances in Cryptology—AUSCRYPT*, vol. 718. Berlin, Germany: Springer, 1992, pp. 165–181, doi: 10.1007/3-540-57220-1_60.
[80] J. Seberry, X.-M. Zhang, and Y. Zheng, "Systematic generation of cryptographically robust S-boxes," presented at the 1st ACM Conf. Comput. Commun. Secur., 1993.
[81] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, "Statistical analysis of s-box in image encryption applications based on majority logic criterion," *Int. J. Phys. Sci.*, vol. 6, no. 16, pp. 4110–4127, 2011, Art. no. E34816025906, doi: 10.5897/IJPS11.531.

WEI GAO received the Ph.D. degree from the Mathematical Department, Soochow University, China, in 2012. He worked with the School of Information Science and Technology, Yunnan Normal University. His research interests are graph theory, theoretical chemistry, and statistical learning theory, computation topics on energy and environmental science, and artificial intelligence. He is currently a Committee Member of the China Society of Industrial and Applied Mathematics (CSIAM) Graph Theory and Combinatorics with Applications Committee, International Association of Engineers (IAENG), Asia Society of Applied Mathematics and Engineering (Asia-SAME), and act as an Academic Adviser of the Center for Energy Research, Iran. He is an Editor of several journals, and also the Chair of ICED 2017 and ISGTCTC 2018. Among his more than 100 publications in SCI index journals, eight of them are included in Essential Science Indicators as Highly Cited Papers (top 1% citations), three of them are honored with Hot Papers (top 0.1% citations).

BAZGHA IDREES received the M.Sc. degree in mathematics from the University of Education, Pakistan, in 2010, and the M.Phil. degree in mathematics from Minhaj University Lahore, Pakistan, in 2014. She is currently pursuing the Ph.D. degree with the University of Management and Technology Lahore, Pakistan. From 2014 to 2016, she was a Lecturer with the Department of Mathematics, University of Sargodha, Pakistan. Since 2016, she has been a Subject Specialist of mathematics with the Punjab School Education Department, Pakistan. Her research interest includes cryptography, computational algebra, graph theory, and computer sciences. She has also some well-known research publications. She received the Acquisition of Gold Medal for her M.Phil. degree.

SOHAIL ZAFAR received the B.S. degree from the Department of Mathematics, Punjab University Lahore, Pakistan, in 2008, and the Ph.D. degree from the Abdus Salam School of Mathematical Sciences, Lahore, Pakistan, in 2013. Since 2013, he has been with the University of Management and Technology (UMT), Lahore, Pakistan, where he is currently an Associate Professor. Since the first UMT international conference on pure and applied mathematics, he has been the conference secretary of all the conferences held in UMT related to mathematics. His research interests include computational algebra, graph theory, cryptography, and fuzzy mathematics.

TABASAM RASHID received the Ph.D. degree in mathematics from the National University of Computer and Emerging Sciences, Pakistan, in 2015. He has been teaching Mathematical Courses, since January 2010. He is currently working as an Associate Professor with the University of Management and Technology, Lahore, Pakistan. He has authored more than 70 journal articles to professional journals. He is also a Reviewer of the American Mathematical Society and peer reviewer of several international journals. He has been selected as the Best Researcher with the University of Management and Technology, in 2015, 2017, and 2018. His field of interest and specialization is versatile in nature. It covers many areas of mathematics, economics, engineering, clustering algorithms, decision theory, computer science, similarity measures, aggregation operators, preference relations, and social sciences.