# An algorithm for the construction of substitution box for block ciphers based on projective general linear group

Cite as: AIP Advances **7**, 035116 (2017); https://doi.org/10.1063/1.4978264
Submitted: 23 November 2016 • Accepted: 23 February 2017 • Published Online: 16 March 2017

Anas Altaleb, Muhammad Sarwar Saeed, Iqtadar Hussain, et al.

AIP ADVANCES **7**, 035116 (2017)

# An algorithm for the construction of substitution box for block ciphers based on projective general linear group

Anas Altaleb,[1] Muhammad Sarwar Saeed,[1] Iqtadar Hussain,[2] and Muhammad Aslam[3]
[1]*Department of Mathematics, University of Hail, Saudi Arabia*
[2]*Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia*
[3]*Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan*

(Received 23 November 2016; accepted 23 February 2017; published online 16 March 2017)

The aim of this work is to synthesize 8*8 substitution boxes (S-boxes) for block ciphers. The confusion creating potential of an S-box depends on its construction technique. In the first step, we have applied the algebraic action of the projective general linear group $PGL(2,GF(2^8))$ on Galois field $GF(2^8)$. In step 2 we have used the permutations of the symmetric group $S_{256}$ to construct new kind of S-boxes. To explain the proposed extension scheme, we have given an example and constructed one new S-box. The strength of the extended S-box is computed, and an insight is given to calculate the confusion-creating potency. To analyze the security of the S-box some popular algebraic and statistical attacks are performed as well. The proposed S-box has been analyzed by bit independent criterion, linear approximation probability test, non-linearity test, strict avalanche criterion, differential approximation probability test, and majority logic criterion. A comparison of the proposed S-box with existing S-boxes shows that the analyses of the extended S-box are comparatively better.  [http://dx.doi.org/10.1063/1.4978264]

## I. INTRODUCTION

The field of secure communications is playing a vital contribution to make digital data invulnerable against different types of insecure channel attacks and the subfield of secure communication which is responsible for this is known as Cryptology. The oldest methods to shield information privacy are cryptology,[1–32] steganography[32] and watermarking. The main aim behind all of these methods is data security. Cryptology can be subdivided into two main branches; cryptography and cryptanalysis. Cryptography is the field of making encryption algorithms and Cryptanalysis is the field of breaking encryption algorithms. Cryptography has two main sub-fields, one is symmetric encryption algorithms and the second is asymmetric encryption algorithms. Symmetric encryption algorithms have two main branches namely Block ciphers and Stream ciphers. Some examples of block ciphers are Advanced Encryption Standard (AES),[1] Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) etc. The concept of block cipher was introduced by C. Shannon in 1949.[33] The DES was proposed by the famous International Business Machines (IBM) in 1975 and the government of United States of America (USA) adopted DES as a standard in 1977 for their banking industry, electronic comers, military etc. The inventors of DES claimed in 1975 that it is very difficult to break the code of their proposed system. But in 1998 some university students broke the code of DES in just 24 hours.[2] Therefore, the government of USA decided to change their standard and they asked for an open proposal from the world. Many scientists sent different kinds of encryption algorithms but the decision goes in favor of Belgium cryptographers and the name of the cryptosystem was Rijndael. In 2001, the National Institute of Standards and Technology (NIST) accepted Rijndael as a standard for the USA to present higher safety than Data Encryption Standard

 

(DES). AES is a symmetric key encryption algorithm. From 2001 to till now they are using AES as a standard in the USA and worldwide successfully. The size of the key is vital in measuring the strength level of any encryption algorithms. Hence AES has the flexibility to have three different types of keys such as 128 bits, 192 bits, and 256 bits. It is proved that AES is more secure in terms of encryption as compare to DES because DES has the key size of only 56 bits. One more thing which is very important in measuring the security of any cryptosystem is its number of rounds. Basically, AES is an iterative cryptosystem and has three options for the rounds such as 10, 12 and 14. The number of rounds depends on the key size such as 10, 12 and 14 rounds are for 128 bits, 192 bits, and 256 bits respectively. One round of AES has four steps named SubByte, ShiftRow, MixColumn and AddRoundKey. The only nonlinear part in these four steps is SubByte. The basic operation which goes in this step is S-box transformation. One thing which is important to mention here is that the final round is constituted with stages as previous rounds except the MixColumn.[1]

In block ciphers, S-box and P-box are two important components of a secure block cipher identified by Claude Shannon. The basic purpose of an S-box is to produce confusion between the ciphertext and the secret key and P-box is responsible for diffusion. S-box is the heart of every block cipher cryptosystem. In AES S-box characterizes the nonlinearity of the whole algorithm. Basically, 8*8 S-box is a function from $GF(2^8)$ to $GF(2^8)$, where $GF(2^8)$ is a finite field of order 256. In other words, we can say that an 8*8 S-box is the combination of eight different Boolean functions. The square S-box used in Rijndael is not economical because it is LUT based and during implementation uses more resources.[2] So to overcome this drawback in Rijndael some authors proposed cellular automata S-boxes.[6]

In secure communication the role of the nonlinear component for block ciphers (Substitution box) is imperative. Substitution box plays a central role in providing the task of confusion during the process of enciphering the digital data.[1] It is well known that in block ciphers S-P (Substitution and Permutation) network is central part and if the S-box is not good it means one has to compromise on the quality of encryption. Therefore before using any S-box in a cryptosystem, it is important to measure its strength. To evaluate the properties of prevailing renown boxes some cryptographers have paid attention in the literature.[3,4,6] These analyses include linear approximation probability method (LP), bit independence criterion (BIC), majority logic criterion (MLC),[3] strict avalanche criterion (SAC), non-linearity method, and differential approximation probability method (DP).

The scheme in the assembly of the novel S-boxes make use of the linear fractional transformations, that is, $az + b/cz + d$ where $ad - bc \neq 0$ and permutations of a particular type from the symmetric group of order 256!. After the construction of S-boxes, the most important thing is to analyze its confusion producing ability between the ciphertext and secret key in block ciphers. There are some renowned analyses to measure the strength of S-boxes such as linear approximation probability, differential approximation probability, nonlinearity, strict avalanche criterion, bit independence criterions and majority logic criterions. With these analyses, one can analyze the strength of any n*k S-box but in this paper, we are going to propose 8*8 S-boxes because we are making these boxes particularly for AES.

This paper consists of two parts. In the first part we are proposing new S-boxes and to explain the presented algorithm for the synthesis of S-box we have given one particular example. The second part consists of analyses of S-box which we have proposed in an example of part one. We start by presenting the algebra of general linear groups with that we can calculate the number of boxes which we can construct. Section III explaining the technique of construction of proposed S-boxes. Several analyses are executed on the novel S-boxes, and their particulars are argued in Section IV. The statistical analyses based on image encryption applications are presented in Section V we present the conclusion.

## II. PROJECTIVE GENERAL LINEAR GROUPS

In this section we will discuss some results about a family of linear groups[35] known as *projective general linear groups* denoted by $PGL(n, F)$. If $F$ is a field then we denote by $GL(n, F)$ the group of $n$ matrices having entries from the field $F$. Since the entries of the matrices in $GL(n, F)$ are from the field $F$ so the matrices are invertible. This group has dimension $n$ over $F$ and is known as the general linear group. We denote by $GL(n, F_q)$, the general linear group with entries from the finite field $F_q$. We always assume that $n \geq 2$ for $GL(1, F)$ is simply the multiplicative group $F^*$ of $F$, and is abelian.

**Theorem 1 (35).** $|GL(n, q)| = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-1})$

We are interested to find the order of $PGL(2, q)$. The group $PGL(2, q)$ is the image of $GL(n, q)$ under a homomorphism whose kernel consists of non-zero scalar matrices and so has order $q - 1$.

**Theorem 2 (35).** *The determinant map* $\det : GL(n, F) \to F^*$ *is a homomorphism.*

**Theorem 3 (35).** *The following conditions on a matrix* $A \in GL(n, F)$ *are equivalent:* ***a)*** $A \in Z(GL(n, F))$; ***b)*** *A belongs to the kernel of the action of* $GL(n, F)$ *on* $\Omega$; ***c)*** *A is a scalar matrix, that is,* $A = \lambda A$ *for some* $\lambda \in F^*$.

*Remark.* So from the above results it is clear that the order of $PGL(n, q)$ is

$$|PGL(n, q)| = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-}1)/(q - 1). \tag{1}$$

## III. THE PROPOSED S-BOXES

The assembly of the novel S-boxes depends on two steps. First we will define a group action $f : PGL(2, GF(2^8)) \times GF(2^8) \to GF(2^8)$ of the projective general linear group $PGL(2, F))$ on the Galois field $GF(2^8)$.[34] The function $f$ is a linear fractional transformation, known as Möbious transformation, given as:

$$f(z) = \frac{az + b}{cz + d} \tag{2}$$

So in our case, $f(z)$ is the projective transformation of $PGL(2, GF(2^8))$, where $a, b, c, d \in GF(2^8)$ satisfying $ad - bc \neq 0$. From this action we can construct 16776960 number of S-boxes, the justification of this is given in equation (1).

The S-box is constructed by evaluating $f(z)$ for the fixed values of $a, b, c, d$ chosen from $GF(2^8)$ against the range of $z$ defined as [0, 255]. In addition, the conditions of $ad - bc \neq 0$ and $cz = -d$ are checked and avoided. The numbers obtained as a result of $f(z)$ are then converted in binary form and represented as power of $w$, where $w$ is given as the root of the primitive irreducible polynomial.

In step 2 we will apply a permutation of a particular type on the outcome of step 2 to change the positions of elements and also to destroy the structure of Galois field. This permutation will increase the diffusion capability of that cipher, the permutation is as follows;

TABLE I. The permutation of step 3.

| Rows/Columns | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 212 | 16 | 44 | 114 | 149 | 42 | 176 | 240 | 76 | 160 | 96 | 189 | 207 | 251 | 84 | 214 |
| 1 | 112 | 229 | 228 | 230 | 196 | 8 | 201 | 191 | 159 | 106 | 125 | 110 | 164 | 117 | 33 | 249 |
| 2 | 213 | 155 | 248 | 167 | 56 | 116 | 69 | 38 | 177 | 206 | 192 | 58 | 70 | 172 | 87 | 204 |
| 3 | 217 | 168 | 123 | 145 | 238 | 77 | 127 | 173 | 63 | 99 | 80 | 62 | 246 | 133 | 137 | 85 |
| 4 | 244 | 129 | 78 | 83 | 161 | 9 | 209 | 183 | 25 | 59 | 12 | 188 | 90 | 73 | 171 | 113 |
| 5 | 35 | 236 | 130 | 163 | 158 | 242 | 187 | 134 | 57 | 18 | 100 | 225 | 92 | 142 | 13 | 150 |
| 6 | 200 | 24 | 170 | 5 | 237 | 36 | 148 | 147 | 140 | 72 | 71 | 154 | 165 | 174 | 184 | 21 |
| 7 | 239 | 75 | 97 | 151 | 152 | 128 | 256 | 215 | 231 | 51 | 136 | 105 | 232 | 61 | 226 | 107 |
| 8 | 26 | 88 | 182 | 68 | 198 | 143 | 4 | 233 | 54 | 43 | 46 | 120 | 22 | 220 | 52 | 60 |
| 9 | 19 | 181 | 29 | 11 | 30 | 245 | 175 | 89 | 104 | 178 | 79 | 45 | 2 | 103 | 241 | 193 |
| 10 | 47 | 202 | 6 | 223 | 221 | 243 | 3 | 40 | 115 | 95 | 14 | 93 | 64 | 32 | 144 | 81 |
| 11 | 190 | 162 | 141 | 180 | 101 | 119 | 124 | 28 | 254 | 210 | 7 | 253 | 109 | 224 | 37 | 186 |
| 12 | 250 | 74 | 1 | 194 | 205 | 131 | 10 | 219 | 146 | 135 | 23 | 132 | 98 | 126 | 66 | 203 |
| 13 | 41 | 121 | 195 | 252 | 185 | 255 | 208 | 122 | 222 | 227 | 53 | 20 | 86 | 234 | 102 | 211 |
| 14 | 49 | 39 | 138 | 48 | 65 | 139 | 199 | 91 | 179 | 67 | 235 | 15 | 216 | 157 | 247 | 34 |
| 15 | 50 | 108 | 153 | 169 | 197 | 156 | 111 | 27 | 118 | 82 | 218 | 31 | 17 | 55 | 166 | 94 |

With this procedure one can synthesize a large number of S-boxes but, to make the reader understand in an easy way, we will elaborate on technique with the help of an example given below.

*Example** In this example, we will construct a single S-box to elaborate proposed algorithm in more details. Let us consider a particular type of linear fractional transformation such that $f(z) = 35z + 15/9z + 5$, where $35, 15, 9, 5 \in GF(2^8)$. This linear transformation will give us a $16 \times 16$ table by having entries from $GF(2^8)$ using the procedure of Ref. 34, which is given in Table I.

Basically, we are using a particular primitive polynomial for the construction of substitution box. But one can use any primitive polynomial from the list given below and correspond to different primitive polynomials we will get different S-boxes with different algebraic and statistical properties. The procedure is explained in Figure 1.

$$\rho^8 + \rho^4 + \rho^3 + \rho^2 + 1 \tag{3}$$

$$\rho^8 + \rho^5 + \rho^3 + \rho^1 + 1 \tag{4}$$

$$\rho^8 + \rho^5 + \rho^3 + \rho^2 + 1 \tag{5}$$

$$\rho^8 + \rho^6 + \rho^3 + \rho^2 + 1 \tag{6}$$

$$\rho^8 + \rho^6 + \rho^4 + \rho^3 + \rho^2 + \rho^1 + 1 \tag{7}$$

$$\rho^8 + \rho^6 + \rho^5 + \rho^1 + 1 \tag{8}$$

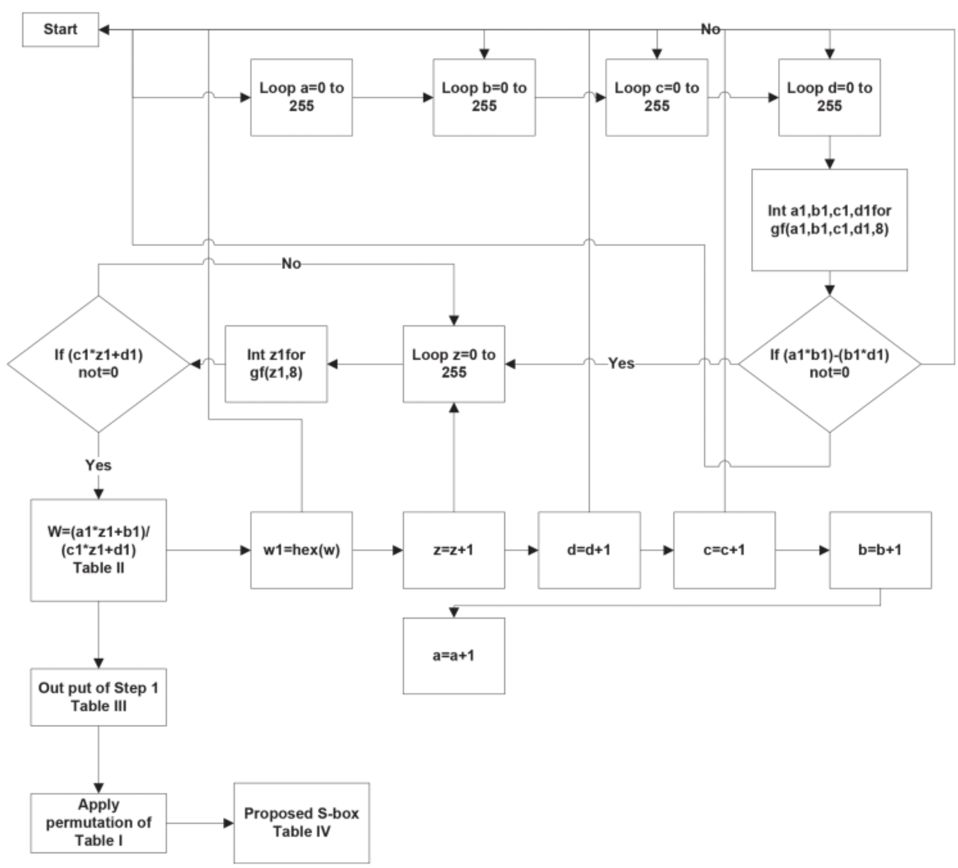


FIG. 1. Flowchart of proposed algorithm.

$$\rho^8 + \rho^6 + \rho^5 + \rho^2 + 1 \tag{9}$$

$$\rho^8 + \rho^6 + \rho^5 + \rho^3 + 1 \tag{10}$$

$$\rho^8 + \rho^6 + \rho^5 + \rho^4 + 1 \tag{11}$$

$$\rho^8 + \rho^7 + \rho^2 + \rho^1 + 1 \tag{12}$$

$$\rho^8 + \rho^7 + \rho^3 + \rho^2 + 1 \tag{13}$$

$$\rho^8 + \rho^7 + \rho^5 + \rho^3 + 1 \tag{14}$$

$$\rho^8 + \rho^7 + \rho^6 + \rho^1 + 1 \tag{15}$$

$$\rho^8 + \rho^7 + \rho^6 + \rho^3 + \rho^2 + \rho^1 + 1 \tag{16}$$

$$\rho^8 + \rho^7 + \rho^6 + \rho^5 + \rho^2 + \rho^1 + 1 \tag{17}$$

$$\rho^8 + \rho^7 + \rho^6 + \rho^5 + \rho^4 + \rho^2 + 1 \tag{18}$$

For example, the elements of $f(z)$ for values of $a$, $b$, $c$, $d$ as 35, 15, 9, 5 respectively and for $z$ as [0, 255] gives the output of first step as shown in Table II. The values of $z$ as $GF(2^8)$ are depicted in column 1, the transformation $f(z)$ is shown in column 2 and the transformed S-box elements are shown in column 3. The S-box as $16 \times 16$ matrix is shown in Table III.

Tables II and III is the output of step 1. After applying step 2 and 3 on Table III we will get Table IV which is our proposed S-box corresponding to a particular type of linear fractional transformation.

## IV. ANALYSES FOR EVALUATING THE STRENGTH OF S-BOX

To find the S-box with fitting confusion creating strength many standards evaluating analyses are presented in literature such as Bijectivity, DP, SAC, BIC, Non-linearity, and LP. We will also use these criteria to test the security of proposed S-box of example*.

### A. Bijectivity

Adamas C et al. pointed out that if the linear sum of the Boolean functions $f_i$ of each component of the designed $n \times n$ S-box is $2^{n-1}$, then $f$ is bijective.[1] Specifically, the expression,

$$wt(a_1 f_1 + a_2 f_2 + \ldots + a_n f_n) \tag{19}$$

where $a_i \in 0, 1, (a_1, a_2, \ldots, a_n) \neq (0, 0, \ldots, 0)$, $wt()$ denotes the Hamming weight. In fact, a reversible S-box generally essential, particularly in a replacement network, the S-box must be bijective.

TABLE II. Construction of S-box using linear fractional transformation.

| $z$ | $f(z) = \frac{(az+b)}{(cz+d)}$ | S-box elements |
|---|---|---|
| 0 | $f(0) = \frac{(35(0)+15)}{(9(0)+5)}$ | 198 |
| 1 | $f(1) = \frac{(35(1)+15)}{(9(1)+5)}$ | 214 |
| ⋮ | ⋮ | ⋮ |
| 254 | $f(254) = \frac{(35(254)+15)}{(9(254)+5)}$ | 6 |
| 255 | $f(255) = \frac{(35(255)+15)}{(9(255)+5)}$ | 76 |

TABLE III. The output of step 1: 16 × 16 matrix resulted from fractional transformation.

| Rows/Columns | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 198 | 214 | 241 | 163 | 130 | 165 | 217 | 127 | 179 | 123 | 111 | 197 | 43 | 141 | 237 | 3 |
| 1 | 168 | 201 | 17 | 121 | 142 | 101 | 232 | 174 | 11 | 249 | 16 | 156 | 10 | 50 | 183 | 65 |
| 2 | 72 | 184 | 200 | 132 | 58 | 47 | 27 | 159 | 231 | 189 | 8 | 18 | 206 | 194 | 177 | 31 |
| 3 | 193 | 92 | 122 | 192 | 85 | 137 | 243 | 49 | 178 | 170 | 36 | 135 | 230 | 95 | 100 | 128 |
| 4 | 13 | 109 | 227 | 0 | 224 | 144 | 208 | 78 | 173 | 32 | 139 | 234 | 107 | 82 | 172 | 81 |
| 5 | 51 | 233 | 12 | 154 | 94 | 161 | 244 | 55 | 07 | 34 | 251 | 225 | 153 | 93 | 254 | 138 |
| 6 | 102 | 240 | 115 | 242 | 110 | 134 | 124 | 79 | 157 | 160 | 90 | 238 | 73 | 53 | 169 | 250 |
| 7 | 136 | 118 | 112 | 48 | 40 | 114 | 22 | 246 | 46 | 131 | 23 | 69 | 52 | 235 | 248 | 2 |
| 8 | 116 | 91 | 117 | 26 | 166 | 25 | 219 | 59 | 54 | 229 | 120 | 245 | 89 | 185 | 99 | 226 |
| 9 | 105 | 45 | 60 | 199 | 164 | 191 | 228 | 202 | 37 | 104 | 143 | 209 | 220 | 147 | 44 | 186 |
| 10 | 145 | 125 | 203 | 29 | 38 | 41 | 215 | 108 | 64 | 88 | 119 | 74 | 213 | 96 | 211 | 83 |
| 11 | 218 | 146 | 196 | 205 | 67 | 152 | 129 | 175 | 84 | 158 | 207 | 176 | 80 | 62 | 150 | 86 |
| 12 | 57 | 155 | 195 | 216 | 75 | 19 | 1 | 87 | 33 | 68 | 71 | 236 | 239 | 255 | 35 | 212 |
| 13 | 148 | 188 | 133 | 15 | 204 | 187 | 42 | 182 | 97 | 56 | 24 | 221 | 252 | 30 | 77 | 181 |
| 14 | 4 | 247 | 167 | 21 | 9 | 222 | 180 | 190 | 151 | 140 | 39 | 171 | 14 | 126 | 66 | 253 |
| 15 | 103 | 223 | 70 | 98 | 28 | 20 | 63 | 162 | 61 | 113 | 149 | 210 | 106 | 5 | 6 | 76 |

TABLE IV. The proposed S-box.

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

## B. Nonlinearity

*Definition 1.* Let $f(x): GF(2^n) \to GF(2)$ be an $n$th Boolean function. The nonlinearity[1] of $f(x)$ can take the form,

$$H_f = min_{l \in L_n} d_H(f, l) \tag{20}$$

where, $L_n$ is a set of the whole linear and affine functions, and $d_H(f, l)$ denotes the Hamming distance between $f$ and $l$.

The nonlinearity denoted by the Walsh spectrum can take the form,

$$N_f = 2^{-n}(1 - max_{\omega \in GF(2^n)} |S_{\langle f \rangle}(\omega)|) \tag{21}$$

The cyclic spectrum of the function $f(x)$ is,

$$S_{\langle f \rangle}(\omega) = 2^{-n} \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus x.\omega} \tag{22}$$

where, $\omega \in GF(2^n)$, and $x.\omega$ denotes the dot product of $x$ and $w$. The larger the nonlinearity $N_f$ of the function $f$, the stronger the ability of its resistance to the linear attacks, vise versa. The nonlinearity of one proposed S-box is given in Table V.

### C. Strict avalanche criterion

SAC depicts information that once a single unit of eight length byte of plaintext converted from 0 to 1 or vise versa, the altering likelihood of each binary unit in the output is 0.5. This analysis is very important evaluate the confusion ability of S-box.[35] The SAC of one proposed S-box is given in Table VI.

### D. Bit independent criterion

Let $f_j$ be a Boolean function and let $f_k$ be a two bits output of an S-box. If $f_j \oplus f_k$ is highly nonlinear and meets the SAC, then the correlation coefficient of each output bit pair may be close to 0 when one input bit is inverted. Thus, we can check the BIC of the S-box by verifying whether $f_j \oplus f_k$ $(j \neq k)$ of any two output bits of the S-box meets the nonlinearity and SAC.[1] The BIC of one proposed S-box is given in Table VII.

### E. Differential approximation probability

The Differential approximation probability $DP_f$ can be a sign of the $XOR$ sharing of the initial seed and output of the Boolean function. The minor the $DP_f$ the greater the capability of nonlinear component of the block cipher to show resistance next to the differential type of cryptanalysis attacks, vice-versa.[2] The DP of one proposed S-box is given in Table VIII.

TABLE V. The non-linearity of proposed S-box.

| Functions of S-box | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Nonlinearity | 112 | 112 | 112 | 112 | 112 | 112 | 112 | 112 |

TABLE VI. Strict avalanche criterion of proposed S-box.

| Rows/Columns | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0.515625 | 0.515625 | 0.453125 | 0.562500 | 0.453125 | 0.500000 | 0.453125 | 0.484375 |
| 1 | 0.468750 | 0.484375 | 0.562500 | 0.500000 | 0.484375 | 0.531250 | 0.500000 | 0.453125 |
| 2 | 0.515625 | 0.515625 | 0.500000 | 0.468750 | 0.562500 | 0.500000 | 0.531250 | 0.500000 |
| 3 | 0.531250 | 0.531250 | 0.468750 | 0.453125 | 0.500000 | 0.546875 | 0.500000 | 0.531250 |
| 4 | 0.453125 | 0.500000 | 0.453125 | 0.515625 | 0.500000 | 0.531250 | 0.546875 | 0.500000 |
| 5 | 0.453125 | 0.515625 | 0.515625 | 0.468750 | 0.468750 | 0.531250 | 0.531250 | 0.546875 |
| 6 | 0.531250 | 0.531250 | 0.468750 | 0.515625 | 0.468750 | 0.484375 | 0.531250 | 0.531250 |
| 7 | 0.515625 | 0.562500 | 0.515625 | 0.531250 | 0.484375 | 0.515625 | 0.484375 | 0.531250 |

TABLE VII. Bit independent criterion of proposed S-box.

| Rows/Columns | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | | 112 | 112 | 112 | 112 | 112 | 112 | 112 |
| 1 | 112 | | 112 | 112 | 112 | 112 | 112 | 112 |
| 2 | 112 | 112 | | 112 | 112 | 112 | 112 | 112 |
| 3 | 112 | 112 | 112 | | 112 | 112 | 112 | 112 |
| 4 | 112 | 112 | 112 | 112 | | 112 | 112 | 112 |
| 5 | 112 | 112 | 112 | 112 | 112 | | 112 | 112 |
| 6 | 112 | 112 | 112 | 112 | 112 | 112 | | 112 |
| 7 | 112 | 112 | 112 | 112 | 112 | 112 | 112 | |

TABLE VIII. Differential approximation probability of proposed S-box.

| Rows/ Columns | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 1 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 2 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 3 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 4 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 5 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 6 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 7 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 8 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 9 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 10 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 11 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 12 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 13 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 14 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 |
| 15 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | 0.015625 | |

### F. Linear approximation probability

Given two randomly selected masks $\Gamma x$ and $\Gamma y$, we use $\Gamma x$ to calculate the mask of all possible values of an input $x$, and use $\Gamma y$ to calculate the mask of the output values $S(x)$ of the corresponding S-box. After masking the input and the output values, the maximum linear approximation that can be computed by the following equation,[2]

$$LP_f = max_{\Gamma x,\Gamma y\neq 0}\left|\frac{\{x\in X|x.\Gamma x = S(x).\Gamma y\}}{2^n} - \frac{1}{2}\right| \tag{23}$$

where, $\Gamma x$ and $\Gamma y$ are the mask values of the input and output, respectively, $X$ is a set of all possible input values of $x$, having $2^n$ elements. The smaller the LP, the stronger the ability of the S-box for fighting against linear cryptanalysis attacks, vise versa.

### G. Majority logic criterion

This analysis criterion is used to know about the image encryption strength of an S-box based on statistical analyses such as correlation analyses, homogeneity analyses, contrast analyses, entropy analysis, energy analysis and mean absolute deviation. This criterion uses these six statistical analyses to execute on the plaintext and S-box transformed images. The basic function of MLC is to determine the distortions produced by S-box transformation in plaintext image. A decision criterion is identified and the outcomes of above mentioned six statistical analyses are used to decide the most powerful S-box that is producing high deformation in plaintext image. In this paper, we are using the image

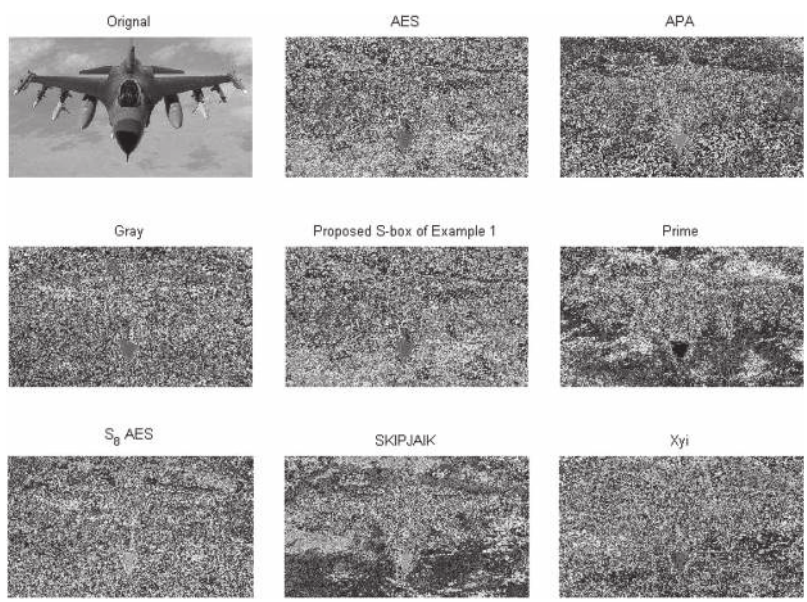


FIG. 2. S-box transformation results of MLC for renown and proposed S-boxes.

TABLE IX. Results of statistical analysis used by majority logic criterion.

| S-boxes/Analyses | Entropy | Contrast | Correlation | Energy | Homogeneity | MAD |
|---|---|---|---|---|---|---|
| AES[1] | 7.9325 | 7.2240 | 0.1294 | 0.0211 | 0.4701 | 43.4554 |
| APA[6] | 7.8183 | 8.9114 | 0.1004 | 0.0193 | 0.4665 | 62.0698 |
| Gray[5] | 7.9299 | 7.7961 | 0.0902 | 0.0198 | 0.4567 | 53.0894 |
| Proposed | 7.9325 | 7.2240 | 0.1294 | 0.0211 | 0.4701 | 43.4554 |
| Prime[4] | 7.8811 | 6.9646 | 0.2516 | 0.0198 | 0.4728 | 58.3894 |

of F-16 as a test to carry out MLC. Figure 2 shows the S-box transformation of the standard image of F-16 with the use of different renown S-boxes and their corresponding readings are presented in Table IX.

## V. CONCLUSION AND FUTURE DISCUSSION

This work is related to construction of S-boxes. The scheme has two steps, the first step is based on a projective general linear group acting on Galois field and step two consists of permutation shuffling of step one units with particular elements of the group the $S_{256}$. The proposed method has many advantages such as when we apply the action of projective general linear group on Galois field we are intended to break the structure of Galois field, because Galois field is basically a cyclic group if we will not break the structure, it means one can construct all other elements of S-box with only one generator. The second advantage is that it is well known in the field of secure communication that permutation induce diffusion so the second step of permutation shuffling improve the diffusion creating ability of the cipher if one will use the proposed S-boxes. In section II of the paper, we have given an introduction about the linear group it is clear from equation (1) that with proposed method we can construct 16777216 numbers of S-boxes if we use only one permutation of $S_{256}$ in step 2. To verify the strength of generated S-boxes, we have taken 3000 S-boxes randomly and analyze their strengths on renowned cryptographic criteria. We have concluded that 98 percent boxes have very good cryptographic properties such as non-linearity, BIC, LP, DP, and SAC. In section III of the paper, we have given one example to explain the construction procedure and we have shown by analyses that the S-box in the example is very good to use in the block cipher encryption algorithm. So one can use proposed boxes for secure communication.

In future, we are planning to use proposed S-boxes in AES algorithm. It is well known that AES has only one S-box in its Byte Sub step and it uses the same box in all its rounds depending upon its key length. Now we have 16777216 number of boxes with good properties, we believe that these huge number of boxes has a vital application in block cipher encryption algorithms. We have given a comparison between the AES algorithm and proposed future algorithm on which we are planning to work. One can see in Figure 3 that at Byte Sub step we have a huge number of options.

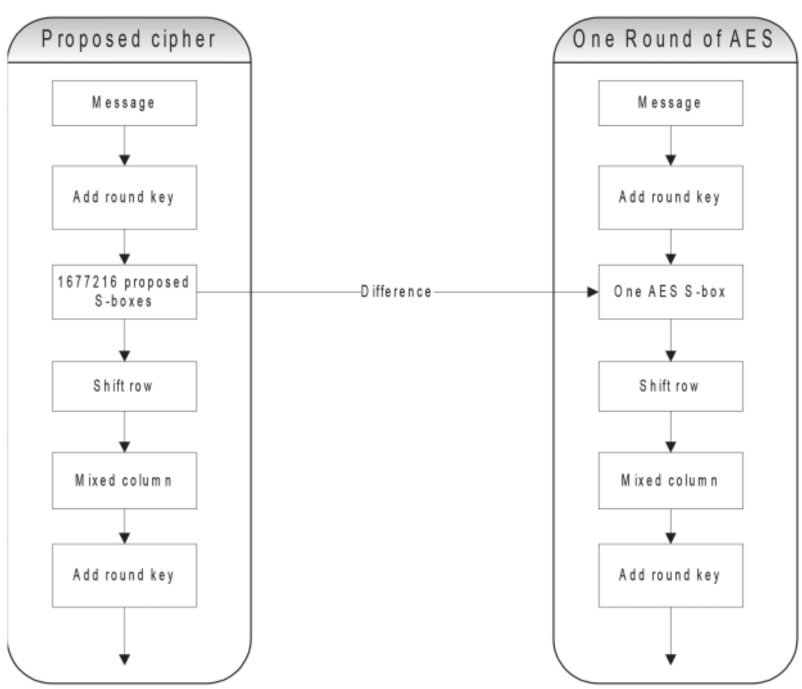


FIG. 3. Comparison between AES and future algorithm.

## ACKNOWLEDGMENTS

This research work is funded by University of Hail, Saudi Arabia via research grant number 0150360.

[1] J. Daemen and V. Rijmen, *The Design of Rijndael: AES-The Advanced Encryption Standard*, Information Security and Cryptography (Springer-Verlag, 2002), p. 238.
[2] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in Proceedings of Advances in CryptologyCRYPTO 85. Lecture Notes in Computer Science (Springer-Verlag, 1986), Vol. 218, pp. 523–534.
[3] 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 **6**(16), 4110–4127 (2011).
[4] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal, and U. Y. Bhatti, "Some analysis of S-box based on residue of prime number," Proc Pak Acad Sci **48**(2), 111–115 (2011).
[5] M. T. Tran, D. K. Bui, and A. D. Doung, "Gray S-box for advanced encryption standard," Int Conf Comp Intel Secur, 253–256 (2008).
[6] L. Cui and Y. Cao, "A new S-box structure named Afne-Power-Afne," Int J Innov Comput I **3**(3), 45–53 (2007).
[7] S. Nidhi and V. Sandip, "A hybrid cryptosystem for image using chaotic mapping," Int J Comput Sci Bus Inform **5**, 110 (2013).
[8] T. Pan and D. Li, "A novel image encryption using Arnold cat," Int J Secur Appl **7**, 377–386 (2013).
[9] P. K. Narendra, "Design and analysis of a novel digital image encryption scheme," Int J Netw Secur Appl **4**, 95–108 (2012).
[10] J. Alireza and M. Abdolrasoul, "An image encryption approach using chaos and stream cipher," J Theor Appl Inf Tech **19**, 117–123 (2010).
[11] S. I. Shatheesh, P. Devaraj, and R. S. Bhuvaneswaran, *Chaos based image encryption scheme based on enhanced logistic map*, Int Con Distr Comp Internet Tech, 2011, Vol. 6536, pp. 290–300.
[12] M. Prasad and K. L. Sudha, "Chaos image encryption using pixel shuffling," in First International Conference on Computer Science Engineering and Applications, 15-17 July 2011 (CCSEA, Chennai, India, 2011), pp. 169–179.
[13] Z. Linhua, L. Xiaofeng, and W. Xuebing, "An image encryption approach based on chaotic maps," Chaos Soliton Fract **24**, 759–765 (2005).
[14] Y. Ruisong, "A highly secure image encryption scheme using compound chaotic maps," J Emerg Comput Inf Sci **4**, 532–544 (2013).
[15] A. I. Ismail, A. Mohammed, and D. Hossam, "A digital image encryption algorithm based on composition of two chaotic logistic maps," Int J Netw Secur **11**, 110 (2010).
[16] A. Musheer and A. M. Shamsher, "A new algorithm of encryption and decryption of images using chaotic mapping," Int J Comput Sci Eng **2**, 46–50 (2009).
[17] S. A. Anto and S. Dipesh, "Modified algorithm of encryption and decryption of images using chaotic mapping," Int J Sci Res **2**, 77–81 (2013).
[18] P. V. Om, N. Munazza, and A. Musheer, "Modified multi-chaotic systems that are based on pixel shuffle for image encryption," J Inf Process Syst **9**, 271–286 (2013).
[19] F. K. Tabash, M. Q. Rafiq, and M. Izharrudin, "Image encryption algorithm based on chaotic map," Int J Comput Appl **64**, 1–10 (2013).
[20] S. Aradhana and K. A. Anuja, "A novel image encryption approach using an indexbased chaos and DNA encoding and its performance analysis," Int J Comput Appl **47**, 1–6 (2012).
[21] F. Chong, C. Jun-jie, Z. Hao, M. Wei-hong, Z. Yong-feng, and Y. Ya-wen, "A chaos based digital image encryption scheme with an improved diffusion strategy," Opt Express **20**, 2363–2378 (2012).
[22] K. S. Vani and G. Neelima, "An efficient image cryptographic technique by applying chaotic logistic map and Arnold cat map," Int J Adv Res Comput Sci Software Eng **3**, 1210–1215 (2013).
[23] B. Pankesh, "Image encryption using pixel shuffling," Int J Adv Res Comput Sci Software Eng **2**, 279–282 (2012).
[24] Y. Ruisong, "A highly secure image encryption scheme using compound chaotic maps," J Emerg Comput Inf Sci **4**, 532–544 (2013).
[25] H. Xiaoling, Y. Guodong, and W. W. Kwok, "Chaotic image encryption algorithm based on circulant operation," Abstr Appl Anal, 1–8 (2013), 384067.
[26] E. B. Shahram and E. Mohammad, "Chaotic image encryption design using Tompkins-Paige algorithm," Math Probl Eng, 1–22 (2009), 762652.
[27] L. Khaled, C. Jean-Yves, and B. Abdellah, "A secure image encryption algorithm based on rubik's cube principle," J Ele Com Eng, 1–13 (2012), 173931.
[28] D. Adrian-Viorel and L. Khaled, "An improved secure image encryption algorithm based on rubik's cube principle and digital chaotic cipher," Math Probl Eng, 1–10 (2013), 848392.
[29] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. Balaguru Rayappan, "Medical data sheet in safe havens - A tri-layer cryptic solution," Computers in Biology and Medicine **62**, 264–276 (2015).
[30] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Pixelscattering matrix formalism for image encryption-A key scheduled substitution and diffusion approach," AEU - International Journal of Electronics and Communications **69**(2), 562–572 (2015).
[31] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Triple chaotic image scrambling on RGB - a random image encryption approach," Security and Communication Networks (2015) (in press).
[32] R. Balakrishnan and A. Rengarajan, "Stego on FPGA: An IWT approach," The Scientific World Journal **2014**(9) (2014), 192512.
[33] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J. **28**(4), 656–715 (1949).

[34] I. Hussain, "A projective general linear group based algorithm for the construction of substitution box for block ciphers," Neural Comput Applic **22**, 1085–1093 (2013).
[35] R. A. Wilson, *The Finite Simple Groups*, Graduate Texts in Mathematics 251, Chapter 1: Introduction (Springer-Verlag, Berlin, New York, 2009), p. 251.