IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 10, 2021, accepted June 2, 2021, date of publication June 7, 2021, date of current version June 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3086717

Dynamic S-Box Design Using a Novel Square Polynomial Transformation and Permutation

AMJAD HUSSAIN ZAHID[1], HAMZA RASHID[1,2], MIAN MUHAMMAD UMAR SHABAN[1], SOBAN AHMAD[1], EHTEZAZ AHMED[1,3], MUHAMMAD TALLAL AMJAD[1], MUHAMMAD AZFAR TARIQ BAIG[1], MUHAMMAD JUNAID ARSHAD[4], MUHAMMAD NADEEM TARIQ[1], MUHAMMAD WASEEM TARIQ[1], MUHAMMAD AYAZ ZAFAR[1], AND ABDUL BASIT[1]

[1]School of Systems and Technology, University of Management and Technology, Lahore 54700, Pakistan
[2]Ripha International College, Lahore 54700, Pakistan
[3]Punjab Information Technology Board, Lahore 54700, Pakistan
[4]Department of Computer Science, University of Engineering and Technology, Lahore 54700, Pakistan

Corresponding author: Amjad Hussain Zahid (amjad.zahid@umt.edu.pk)

ABSTRACT New era ciphers employ substitution boxes (S-boxes) which assist in the provision of security for the plaintext in the encryption phase and transforming the ciphertext on the receiver side into original plaintext in the decryption phase. The overall security of a given cipher engaging an S-box greatly depends on the cryptographic forte of the respective S-box. Consequently, many researchers have used different innovative approaches to construct robust S-Boxes. In this article, an innovative and modest square polynomial transformation, the very first time, along with a novel affine transformation and a pioneering permutation approach to construct dynamic S-boxes is proposed. The proposed method has the capability to erect a huge number of robust S-boxes by applying minute changes in the parameters of transformation and permutation processes. An example S-Box is generated, and its recital analysis has been done using typical criteria including bijectivity, strict avalanche criterion, nonlinearity, bit independence criterion, linear probability, differential probability, and fixed-point analysis to check its cryptographic forte. This performance of the proposed S-box is placed side by side against state-of-the-art S-boxes to prove its strength. The performance and comparative analyses authenticate that the projected S-box possesses the true competence for its application in modern-day ciphers.

INDEX TERMS Linear fractional transformation, square polynomial transformation, dynamic affine transformation, permutation, substitution box.

I. INTRODUCTION

Today, organizations have a huge volume of data within their data storerooms and systems. Data are involved in scientific research and other fields and are mostly produced in an automatic way. Due to the growth in the volume of data on daily basis, these organizations and common people are facing problems of data security as a result of data leakage or stealth when data are transmitted from one location to other locations through media or channels. If data are sent in a meaningful form over the shared medium, attackers get opportunities to grab and misuse seized data to harm the communicating parties. Sensitivity of data being communicated demands more security and protection from the invaders. Consequently, a sender converts meaningful data by performing different steps into a meaningless form that is useless for attackers. Different techniques are utilized to transform the given data into meaningless form. One such domain to help in this conversion is called cryptography and contemporary cryptographic techniques recognized as ciphers contribute their part for data and information protection.

Two core kind of ciphers being utilized for data security are stream and block ciphers. Stream ciphers convert data into meaningless form by performing different operations at single bit or byte level. Block ciphers transform a block of data at a time whereas a data block mostly comprises of many bits or bytes [1]. Today, block ciphers have arisen as the most applicable technique to protect the sensitive information

The associate editor coordinating the review of this manuscript and approving it for publication was SK Hafizul Islam.

due to their simple and easy implementations [2], [3]. Data Encryption Standard (DES), Triple DES (3DES), Blowfish, Advanced Encryption Standard (AES), Twofish, etc. are few examples of the renowned block ciphers being used in many security applications. These block ciphers employ permutation and substitution operations as the core processes to encrypt the given data and decrypt the subsequent ciphertext. A permutation technique employed in a given cipher shuffles a part of data with another part from the same data being processed by that cipher.

A substitution technique locums a part of the original data with some other data which is not the part of the original data. Such replacements of data are achieved using a substitution box (S-box) [4], [5]. An S-box is a vigorous integral of present-day block ciphers and supports significantly to yield a tousled output (known as ciphertext) by transforming the plaintext. It creates a mapping which helps in the transformation of the plaintext into the ciphertext in such a way that the attackers of the ciphertext get confused [6].

For the provision of more security by a cipher that uses an S-box, it is needed that the particular S-box generates enough confusion in the consequential ciphertext for the attackers. As a result, the protection of plaintext/data using a block cipher with the assistance of an S-box is mostly dependent on the forte of the particular S-box used in the cipher as other parts of a cipher don't contribute much towards the security of data [7], [8].

Today, ciphers use dynamic S-boxes in their operation as compared to static S-boxes. A static S-box is easily guessable by attackers and security provided to the plaintext by the cipher using such an S-box is conceded [9], [10]. DES and AES original S-Boxes are static in nature and invaders attempted attacks on these in past. To overcome such a weakness present in a static S-Box, modern-day ciphers employ dynamic S-boxes that are generated by using cipher-key and own more cryptographic strength.

Consequently, S-box designers have attempted and proposed new methods of dynamic S-box design using cipher-key. One interesting domain being utilized currently for security of data to produce strong S-boxes is chaotic theory which has the competence to generate randomness [11]. Many researchers [12]–[19] employed this chaos field to yield cryptographically robust S-boxes. Hyperchaotic theory has the ability to generate stronger S-boxes than chaotic structures. As a result, hyperchaotic based techniques [20], [21] generated huge number of robust S-Boxes.

DNA computing is another prevalent field being used for the design of robust S-boxes to protect data. Researchers [22]–[27] have employed DNA computing for the design of sturdy S-Boxes to assist the encryption process and resultant S-boxes have proved attack-resilient.

Several investigators have exploited other knowledge domains to produce substitution boxes like elliptic curve [28], [29], graph theory [30], [31], cellular automata [32], wavelet domain [33], optimization techniques [17], [34]–[36], Hilbert curve [37], backtracking [38], feedback systems [39], firefly algorithm [40], chaotic permutation [41], Galois Field [42], etc.

Linear fractional transformation (LFT) is another dominant concept being used to produce dynamic S-boxes. Researchers [43]–[46] utilized LFT domain knowledge to create sturdy S-boxes. However, S-box construction process based on LFT is time consuming and generation of S-box values is a complex process due to the use of Galois Field (GF). Different scholars [47]–[49] have projected efficient and simpler transformation techniques than LFT methods to produce vigorous S-boxes. AES is a well-known block cipher that is symmetric in nature and employs S-boxes in its functionality. AES uses static S-box in its working and consequently tolerates the risks accompanying with such an S-box. Arrangement of values in a static S-box is always fixed and this order does not change even if we change the cipher key. Thus, usage of such an S-box permits invaders to study its features, determine its weaknesses, and ultimately get chance to obtain input data (plaintext/key). Researchers like [50]–[54] have projected several perfections to the sanctuary presented by AES though the improvements in the elementary AES S-box.

Nowadays, investigators emphasize on the creation of dynamic S-boxes by means of key used by the cipher. Such dynamic S-boxes offer various level of security to the ciphertext. Some of these techniques for S-box generation follow complex construction process and are less efficient. Other methods lack one or more security criteria like non-bijectiveness, the existence of fixed points, chances of differential cryptanalysis, usage of static permutation and fixed irreducible polynomials, application of static affine transformation employing complex GF inversion process, very less S-box space, etc. Consequently, an innovative, simple, and efficient technique is always desirable to create key-dependent, sturdy, and dynamic S-box.

This research paper presents an innovative technique to yield dynamic S-boxes with the help of cipher-key usage. The presented technique employs a new square polynomial transformation (SPT), a modular multiplicative inversion, a dynamic affine transformation, and a novel permutation technique to create the final S-box.

Followings are the primary contributions of our technique to create dynamic and robust S-boxes:

- A novel square polynomial transformation (SPT) is introduced to generate S-box. The proposed transformation is simpler and much efficient than the prevalent LFT techniques for S-box generation.
- A dynamic affine transformation is proposed that aids in the generation of S-box elements. Proposed transformation is simple and dynamic one and a single bit change in the parameter values of this transformation produces a new S-box.
- A novel permutation technique is introduced and used to create final S-box. Proposed permutation procedure is dynamic one and employs cipher-key in its working.

TABLE 1. Structure of Affine Transformation Matrix (ATM).

$$\begin{bmatrix} X_7 & X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 \\ X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 & X_7 \\ X_5 & X_4 & X_3 & X_2 & X_1 & X_0 & X_7 & X_6 \\ X_4 & X_3 & X_2 & X_1 & X_0 & X_7 & X_6 & X_5 \\ X_3 & X_2 & X_1 & X_0 & X_7 & X_6 & X_5 & X_4 \\ X_2 & X_1 & X_0 & X_7 & X_6 & X_5 & X_4 & X_3 \\ X_1 & X_0 & X_7 & X_6 & X_5 & X_4 & X_3 & X_2 \\ X_0 & X_7 & X_6 & X_5 & X_4 & X_3 & X_2 & X_1 \end{bmatrix}$$

- Final S-box is censoriously investigated using typical S-box assessment criteria along with the existing S-boxes in the literature. Result of this recital investigation validates the remarkable contribution of the proposed technique for S-box generation.

Rest of this paper is organized as follows. Section II describes in detail the proposed method to erect an S-box with the help of an innovative square polynomial transformation, a simple affine transformation, and a new dynamic permutation technique. Section III presents a recital analysis of an example S-box produced using the proposed method and predominant S-boxes. Conclusion is described in section IV.

II. PROPOSED SCHEME FOR S-BOX GENERATION

A substitution box (S-box) assists in establishing a nonlinear mapping between its input and output and it becomes very difficult for an intruder to get the original data from the ciphertext. Consequently, investigators regularly explore such input to output conversions to create sturdy S-boxes. The process to generate a strong S-box should be simple and efficient. However, many prevailing S-box erection methods are intricate and need efficiency improvement too.

In this paper, we demonstrate a novel technique to yield dynamic S-boxes using a new polynomial transformation, a dynamic affine transformation, and an innovative permutation technique to create the final S-box. Complete process of the erection of the proposed S-box involves four modest phases in order as:

1. Innovative Square Transformation
2. Modular Multiplicative Inversion
3. Dynamic Affine Transformation
4. Dynamic Permutation Technique

Each of the above phases involved in the construction of ultimate S-box is described in detail in the following part for better understanding of the process.

A. INNOVATIVE SQUARE TRANSFORMATION

Construction of the proposed n × n S-box is based on an innovative transformation that is a function mathematically defined in Equation (1) as:

$$S(c) = \left(c * A^2 + B\right) \text{MOD } 2^n \quad c \in Z \tag{1}$$

TABLE 2. Product of Affine Transformation Matrix (ATM) and Multiplicative Inverse Matrix (MIM).

$$\begin{bmatrix} B_7 \\ B_6 \\ B_5 \\ B_4 \\ B_3 \\ B_2 \\ B_1 \\ B_0 \end{bmatrix} = \begin{bmatrix} X_7 & X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 \\ X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 & X_7 \\ X_5 & X_4 & X_3 & X_2 & X_1 & X_0 & X_7 & X_6 \\ X_4 & X_3 & X_2 & X_1 & X_0 & X_7 & X_6 & X_5 \\ X_3 & X_2 & X_1 & X_0 & X_7 & X_6 & X_5 & X_4 \\ X_2 & X_1 & X_0 & X_7 & X_6 & X_5 & X_4 & X_3 \\ X_1 & X_0 & X_7 & X_6 & X_5 & X_4 & X_3 & X_2 \\ X_0 & X_7 & X_6 & X_5 & X_4 & X_3 & X_2 & X_1 \end{bmatrix} \times \begin{bmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} \text{(mod 2)}$$

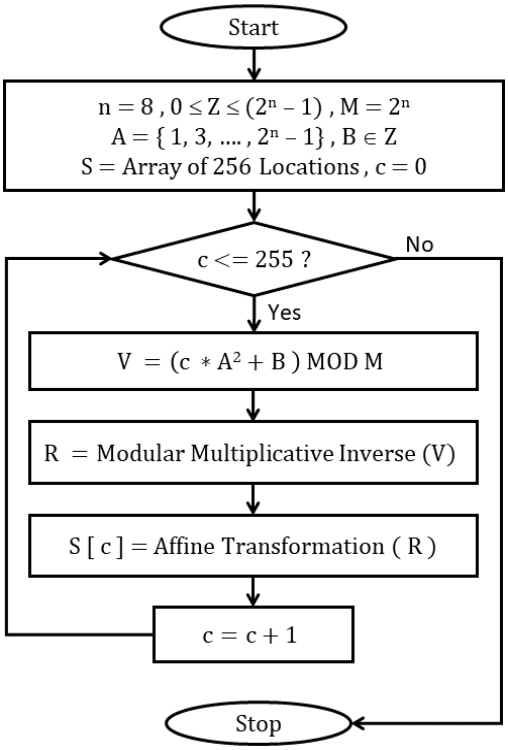


FIGURE 1. Initial S-box construction process for n = 8.

where,

$$A = \{1, 3, \ldots, 2^n - 1\},$$
$$0 \le Z \le (2^n - 1), \quad \textit{and}$$
$$B \in Z.$$

Values of A and B are taken from the cipher key which make this transformation as dynamic one and help in the generation of key-dependent dynamic S-boxes.

B. MODULAR MULTIPLICATIVE INVERSION

This process computes the modular multiplicative inverse (MMI) of a value returned by Eq. (1) using MOD $(2^n + 1)$. Method of MMI computation is elaborated in [49].

C. DYNAMIC AFFINE TRANSFORMATION

This transformation uses an 8 × 8 affine transformation matrix (ATM). Value of each matrix element is either 0 or 1. Affine transformation matrix is filled as follows.

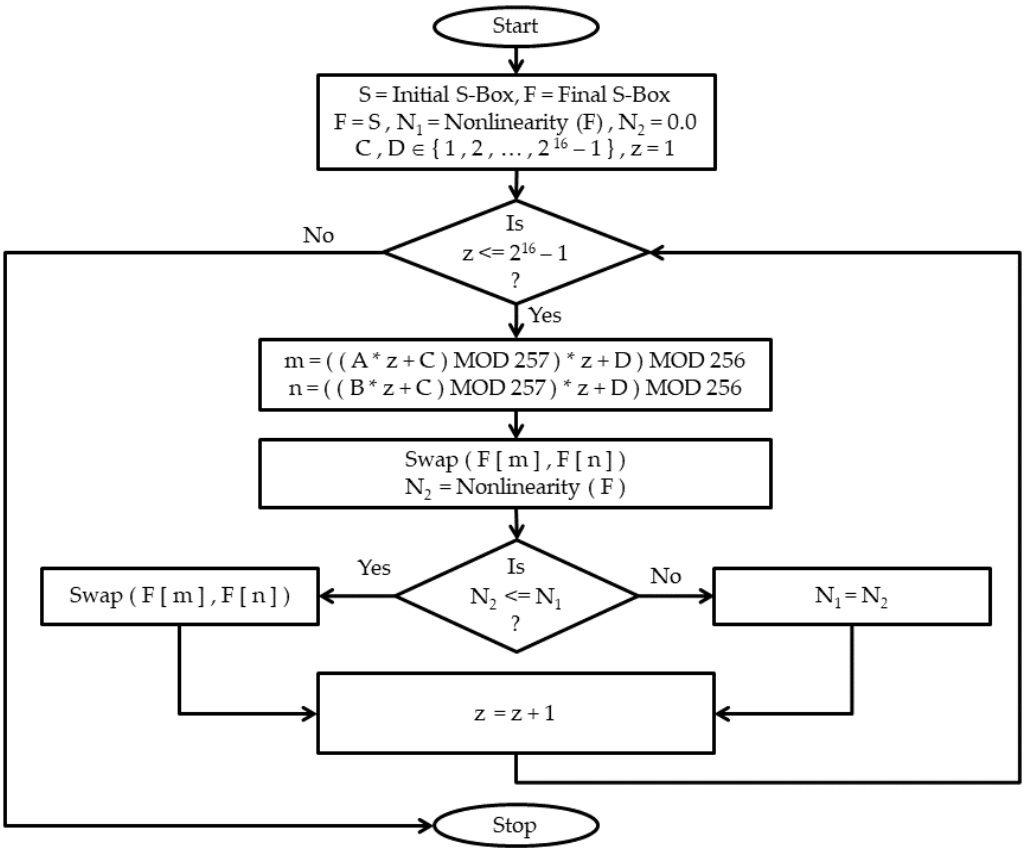


FIGURE 2. Permutation process for final S-box construction.

TABLE 3. Proposed final S-box for a = 201, b = 94, c = 31597, d = 59473.

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

1) One-byte value (0−255) from cipher key is assigned to a variable V with the condition that number of 1's in the binary value of respective byte is odd.

2) First column is filled with the 8-bit binary ($X_7X_6X_5X_4$ $X_3X_2X_1X_0$, where X_7 = Most significant bit (MSB), and X_0 = Least significant bit (LSB)) value of V. MSB

TABLE 4. S-box boolean functions and nonlinearity values.

Boolean Function	st1	st2	st3	st4	st5	st6	st7	st8
NL(st)	112	110	110	112	112	112	112	112

(X_7) is filled in first row and LSB (X_0) is put in last row of the first column.

3) Bits of 1st column are shifted up 1 location in circular way and the shifted result is placed in 2nd column.
4) Rest of the columns are filled in the same way.

An affine transformation matrix looks like Table 1.

Modular multiplicative inverse value yielded in step II-B is converted into 8-bit binary ($b_7b_6b_5b_4b_3b_2b_1b_0$, where b_7 = MSB, and b_0 = LSB) and binary value is put in an 8×1 matrix named as multiplicative inverse matrix (MIM). Multiplication of ATM and MIM matrices and application of modulo 2 operation yield binary value 0 or 1 in each row of the resultant matrix (RM). Bit values are concatenated starting from the 1st row value as the MSB and the last row value as LSB. This 8-bit binary value is converted to its decimal equivalent and stored in the initial S-box.

Process of multiplication of ATM and MIM is demonstrated in Table 2. Construction process of initial S-box design is demonstrated by flowchart given in Figure 1.

D. DYNAMIC PERMUTATION TECHNIQUE

Once an initial S-box is constructed, place of its values is changed using the dynamic permutation as depicted in Figure 2 to get the final S-box. Proposed permutation approach being dynamic in nature helps in creating sturdy and strong S-boxes to defy an attacker's cryptanalytic attempts. In Figure 2, values of the variables A and B used to calculate values m and n are same values used for the computation of an initial S-box S generated using Figure 1. Values of A, B, C, and D (where $0 \leq C, D \leq 2^{2n} - 1$ for $n = 8$) are taken from the cipher key which make this permutation technique as dynamic one and helps to construct robust S-boxes.

To describe the complete procedure of initial S-box erection using Equation (1), Tables 1 and 2, and Figure 1, we have selected a definite type of square transformation as specified in Equation (2). We have $Z = \{0, 1, \ldots, 255\}$, and $M = 2^8 = 256$ for $n = 8$. An example 8×8 initial S-box is produced by employing novel square transformation given in Equation (1) using explicit values of $A = 201$ and $B = 94$.

$$S(c) = \left(c * (201)^2 + 94\right) \text{MOD } 2^8 \quad c \in Z \qquad (2)$$

Final 8×8 S-box is demonstrated using innovative square polynomial transformation in Table 3.

III. SECURITY ASSESSMENT OF PROJECTED S-BOX

A specific substitution box produced using a certain technique may be robust or feeble. To test strength of a given S-box, standard criteria are applied. Here, projected S-box given in Table 3 is examined through succeeding typical criteria which assesses the cryptographic forte of an S-box [15], [18], [55]. Then the complexity of proposed S-box generation with respect to construction time is also analyzed. The cryptographic forte of our projected S-box is compared with the cryptographic forte of other recently published S-boxes.

TABLE 5. NL recital comparison of S-boxes.

S-box Method	Nonlinearity		
	Minimum	Maximum	Average
[41]	106	110	108.0
[49]	104	110	107.5
[56]	106	112	109.5
[57]	102	108	105.0
[58]	100	108	104.0
[59]	104	110	106.9
[60]	98	106	103.5
[61]	104	108	106.3
[62]	106	108	106.5
[63]	100	108	105.0
[64]	104	110	106.3
[65]	96	110	104.0
[66]	104	108	105.0
[67]	97	105	102.9
[68]	106	110	108.5
[69]	106	108	106.8
[70]	106	108	106.5
[71]	108	112	109.3
[72]	102	108	105.0
Proposed	110	112	111.5

A. BIJECTIVENESS

A substitution box should demonstrate a bijective property in a good way. This property ensures that for some unique input, a system should produce unique output. In other words, input-output mapping in a system should be 1-to-1. An S-box of size 8×8 has an 8-bit input and an 8-bit output. Each 8-bit unique input value should create a unique 8-bit output value. S-box as given in Table 3 erected from the novel square polynomial transformation and dynamic permutation confirms bijective property [8], [28] in a very well manner.

B. NONLINEARITY (NL)

An S-box of size 8×8 maps a unique 8-bit input to a unique 8-bit output. This input-output mapping should be nonlinear so as an attacker's efforts to get the original data from

TABLE 6. Dependency matrix of SAC scores of projected S-box.

0.5625	0.4688	0.4531	0.4531	0.5000	0.4844	0.4688	0.5625
0.5000	0.5469	0.5313	0.5313	0.5625	0.5469	0.6094	0.4844
0.4531	0.5156	0.4688	0.5000	0.5781	0.5156	0.4688	0.5000
0.5156	0.4844	0.5313	0.4531	0.4688	0.5625	0.5156	0.5156
0.4688	0.5000	0.4688	0.4688	0.4844	0.5156	0.4688	0.5781
0.4531	0.5625	0.5156	0.5469	0.5313	0.5313	0.4531	0.4688
0.5000	0.4375	0.5313	0.5469	0.5313	0.5000	0.5313	0.5156
0.5781	0.5313	0.5313	0.4844	0.5625	0.5000	0.4688	0.5313

TABLE 7. BIC-SAC scores of projected S-box.

-	0.508	0.500	0.510	0.508	0.484	0.488	0.494
0.508	-	0.492	0.531	0.498	0.459	0.498	0.490
0.500	0.492	-	0.514	0.508	0.500	0.504	0.516
0.510	0.531	0.514	-	0.479	0.520	0.500	0.516
0.508	0.498	0.508	0.479	-	0.488	0.475	0.477
0.484	0.459	0.500	0.520	0.488	-	0.514	0.502
0.488	0.498	0.504	0.500	0.475	0.514	-	0.490
0.494	0.490	0.516	0.516	0.477	0.502	0.490	-

TABLE 8. BIC-NL scores of projected S-box.

-	104	98	104	100	102	104	104
104	-	100	100	106	104	108	102
98	100	-	108	106	104	106	106
104	100	108	-	102	108	106	104
100	106	106	102	-	106	106	104
102	104	104	108	106	-	102	102
104	108	106	106	106	102	-	104
104	102	106	104	104	102	104	-

captured ciphertext are ineffective. An S-box that possesses a nonlinear mapping is stronger to resist such efforts or attacks. This nonlinear mapping (termed as nonlinearity) should be on higher side. To calculate the nonlinearity value (NL) of an 8-bit Boolean function st, Equation (3) is used [55].

$$NL\,(st) = \frac{1}{2}\left[2^8 - (P_{max}\,(st))\right] \tag{3}$$

where, $P_{max}(st)$ denotes Walsh-Hadamard Transformation for Boolean function st. The nonlinearity results of proposed substitution box are 112, 110, 110, 112, 112, 112, 112, and 112 where minimum nonlinearity is 110, maximum nonlinearity is 112, and average nonlinearity is 111.5. Each of the component Boolean function (of projected S-box) and its respective nonlinearity value are specified in Table 4.

TABLE 9. Performance assessment of SAC and BIC scores.

S-box Method	BIC-NL	SAC
[41]	102.9	0.499
[49]	103.5	0.498
[56]	106.9	0.507
[57]	102.9	0.503
[58]	102.6	0.497
[59]	106.1	0.509
[60]	103.5	0.496
[61]	103.6	0.501
[62]	104.1	0.501
[63]	103.0	0.500
[64]	103.9	0.503
[65]	103.0	0.493
[66]	103.5	0.506
[67]	102.7	0.519
[68]	103.9	0.500
[69]	100	0.503
[70]	100	0.503
[71]	104	0.503
[72]	103.4	0.508
Proposed	103.7	0.502

A comparative assessment of freshly published S-box methods and our S-box with respect to nonlinearity values is shown in Table 5. Comparative analysis validates that NL score of proposed S-box surpasses NL scores of many contemporary S-boxes.

C. STRICT AVALANCHE CRITERION (SAC)

This criterion to evaluate the strength of an S-Box guarantees that 50% output bits should change due to a change in one input bit [58], [59], [67]. Consequently, a SAC score of 0.5 for a given S-box is desired. Dependency matrix of SAC scores of our projected S-box is demonstrated in Table 6. It is quite apparent that the average SAC score of our S-Box is equivalent to 0.5 which validates that our S-box fulfills SAC standard in an upright manner.

A comparative assessment between SAC scores of freshly published S-box methods and our S-box is shown in Table 9. It is evident from the comparative analysis that SAC value of proposed S-box is gracefully consistent with the SAC scores of various contemporary S-boxes.

D. BIT INDEPENDENCE CRITERION (BIC)

This criterion to evaluate the strength of an S-Box guarantees that any two output bits change independent of each other

TABLE 10. Differential uniformity values of proposed S-box.

6	6	6	6	6	8	6	6	6	8	6	6	6	6	6	6
10	8	6	6	6	8	6	6	4	6	8	6	6	6	6	6
4	6	8	8	6	6	6	10	8	6	6	6	6	8	6	6
8	8	6	6	8	6	8	4	8	8	8	8	6	6	6	6
6	8	6	6	8	6	6	10	6	6	8	8	6	8	6	6
8	8	8	6	6	6	8	6	6	6	8	6	4	6	6	6
8	8	8	8	8	6	6	4	6	6	6	6	8	6	8	8
8	8	6	8	6	6	6	8	6	6	6	8	6	6	6	8
8	6	6	6	6	6	6	6	6	8	10	8	6	6	6	8
6	8	6	6	6	6	8	6	6	6	8	6	6	6	6	6
6	8	6	6	6	8	6	6	8	8	6	6	6	8	6	6
8	6	6	8	6	6	6	8	6	6	8	8	8	6	6	8
6	6	6	6	8	6	6	8	6	8	8	6	6	6	8	4
8	6	6	6	6	6	8	8	6	8	6	8	6	4	8	6
6	8	6	6	6	8	6	8	6	6	6	8	6	8	6	8
8	8	6	8	6	6	6	6	6	8	8	6	6	6	6	0

due to a change in one input bit [73]. S-box designers try to create S-boxes where output bits don't depend on each other. BIC-SAC and BIC-NL scores of our project S-box are given in Tables 7 and 8 respectively. Average BIC-SAC and BIC-NL scores are 103.9 and 0.5 respectively. These scores indicate a very feeble dependency of output bits with each other. Consequently, proposed S-box satisfies BIC standard quite gracefully. BIC performance of various S-boxes is critically assessed in Table 9.

E. DIFFERENTIAL PROBABILITY (DP)

Ciphertext is transmitted on the shared media and invaders have the possibilities to grasp and investigate it. Attackers try to find the modifications in the ciphertext as well as modifications in the original data. Compounding both the differences aids the invaders to have a clue of partial or whole key or plaintext [74]. A designer of a substitution box tries to lessen the difference between such modifications. To compute such difference, S-box experts assess the differential uniformity (DU) and differential probability (DP) of an S-box. To counterattack the differential cryptanalysis, low scores of differential uniformity (DU) and differential probability (DP) of an S-Box are needed. For an S-box B, differential uniformity is calculated by Eq. (4) [75].

$$\mathrm{DU} = \max_{\Delta_r \neq 0,\, \Delta_q} \left[\#\{r \in \mathrm{N} | \mathrm{B}(\mathrm{r}) \oplus \mathrm{B}(\mathrm{r} \oplus \Delta_r) = \Delta_q\}\right] \quad (4)$$

where $\mathrm{N} = \{0, 1, \ldots, 255\}$, Δ_r and Δ_q represent input and output differentials, respectively.

DU scores of resultant S-box are enumerated in Table 10. Maximum value of differential uniformity of our S-box is 10, and its tally is only 4. As a result, value of DP comes out to be $10/256 = 0.039$. Low scores of DU and DP validate that our projected S-box has the capability of mutiny against differential cryptanalysis. A comparative assessment between DP scores of freshly published S-box methods and our S-box is shown in Table 11. It is evident from the comparative analysis that DP value of proposed S-box has consistency with the DP scores of various other contemporary S-boxes.

F. LINEAR PROBABILITY (LP)

Creators of cryptographic algorithms put their best possible efforts to jumble bits of plaintext for the creation of meaningless ciphertext. The most commonly applied component in a cryptographic algorithm to achieve this confusion is an S-box. An S-box designed in a cautious way aids to create a nonlinear association between inputs data bits and output ciphertext bits. The cryptographic strength of this association provided by a specific 8×8 S-box B is computed as linear probability (LP) using Equation (5) [76].

$$LP = \max_{t_x, t_y \neq 0} \left| \frac{\#\{x \in R | x \cdot t_x = B(x) \cdot t_y\}}{2^8} - \frac{1}{2} \right| \quad (5)$$

where, t_x and t_y are input-bit and output-bit masks respectively and $\mathrm{R} = \{0, 1, \ldots, 2^8 - 1\}$ for $\mathrm{n} = 8$.

It is desired to design an S-box in such a way to have a low value of LP for that particular S-box. LP value of S-box given in Table 3 is 0.125 and this low value is an indication that the projected S-box has the decent capability to fight against linear cryptanalysis. A comparative assessment between LP scores of freshly published S-box methods and our S-box is shown in Table 11. It is evident from the comparative analysis that the proposed S-box possesses the cryptographic forte to resist linear cryptanalytic efforts.

G. FIXED POINTS ANALYSIS (FPA)

For an input k such that $0 \leq \mathrm{k} \leq 2^\mathrm{n} - 1$, if an $\mathrm{n} \times \mathrm{n}$ S-box B has somewhere $\mathrm{B(k)} = \mathrm{k}$ for some value(s) of k, that S-box is said to be having one or more fixed points (FP).

TABLE 11. Performance comparison of LP, DP, and FPs of different S-boxes.

S-box Method	LP	DP	FPs
[41]	0.1406	0.047	1
[49]	0.1406	0.039	0
[56]	0.1328	0.031	0
[57]	0.1484	0.047	1
[58]	0.137	0.039	0
[59]	0.113	0.031	2
[60]	0.1328	0.055	0
[61]	0.139	0.039	0
[62]	0.1328	0.039	0
[63]	0.125	0.047	0
[64]	0.1328	0.039	1
[65]	0.125	0.031	1
[66]	0.125	0.039	2
[67]	0.148	0.211	1
[68]	0.109	0.039	1
[69]	0.071	0.039	2
[70]	0.071	0.039	2
[71]	0.035	0.031	0
[72]	0.1406	0.039	1
Proposed	0.125	0.039	0

If a cipher employs one or more S-boxes in its operation and has some fixed points, it offers cryptographic weakness and may support the attackers to get the original plaintext somehow. Presence of such fixed points may lead the attackers to generate some portion of the plaintext from the ciphertext. So, cryptographers carefully design and construct S-boxes having zero or minimum number of fixed point (FP) [57]. Our resultant S-box is free of any fixed point and fulfills FPA criterion elegantly. A comparative fixed-point analysis between our proposed S-box and other prevalent S-boxes is demonstrated in Table 11. Comparative analysis discloses that some of these state-of-the-art S-boxes have the presence of fixed points and their use in ciphers may weaken the protection of data.

H. COMPLEXITY ANALYSIS

To witness the time complexity of the proposed S-box scheme, it is simulated on an Intel core i7 CPU (2.2 GHz) and 4GB RAM running Windows 8 by implementing in Visual C#. AES S-box generation based on Extended Euclidean Algorithm (EEA) and Look-Up Table (LUT) methods was simulated, and time complexity of the proposed scheme was observed for initial and final S-boxes. Construction of final S-box is based on novel dynamic permutation procedure to improvise cryptographic forte of initial S-box. Table 12 compares computational efficiency of these constructions. It is evident from Table 12 that the time of construction of initial S-box is pretty inspiring as equated to that of AES methods. However, time taken to generate final S-box by proposed scheme is a bit higher. Permutation approach used in the proposed technique contributes significantly to enhance the cryptographic forte of our final S-box. As the fortification of one's data is extremely important and a real anxiety, this need of protecting data should not be negotiated seeing speed of recent CPUs. Enhancement in nonlinearity (NL) value of initial S-box using dynamic permutation approach with respect to computation time is depicted in Figure 3.

TABLE 12. S-box construction time (seconds) of AES S-Box and proposed scheme.

AES S-Box		Proposed Scheme	
EFU	LTU	Initial S-Box	Final S-Box
0.415	0.163	0.003	305

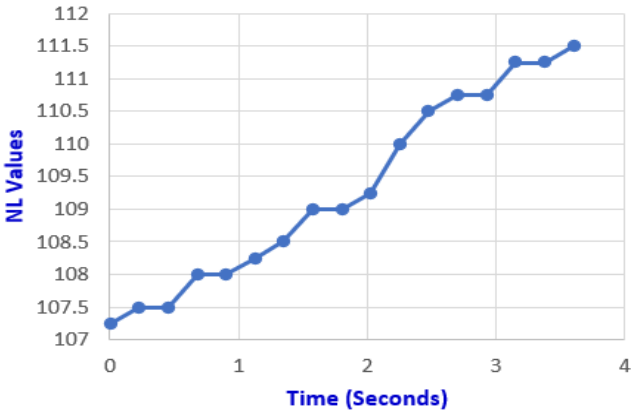


FIGURE 3. Nonlinearity improvisation of initial S-box using permutation process wi.r.t. time.

Although many authors suggested new methods to construct S-Box having nonlinearity >= 112 like AES, these approaches lack one or more security criteria like non-bijectiveness [77], the existence of fixed points [45], [78]–[81], high value of differential probability [82], static permutation [83], usage of fixed irreducible polynomial by [80], [83] and AES, complex construction process [82], etc. Our proposed scheme for construction of S-box uses simple and novel dynamic transformation being the first one of its nature, employs dynamic affine transformation using modular multiplicative inversion as compared to the static affine transformation used in many of the above mentioned techniques employing complex GF inversion process, and a new dynamic permutation procedure in comparison to the

static permutation utilized in these methods. Most of these methods have very small S-box space as compared to the huge S-box space = $\{65535 \times 65535 \times 255 \times 128 = 140, 183, 454, 384, 000\}$ offered by our scheme with the help of parameters C, D $\in \{0, 1, \ldots, 2^{2n}-1\}$, A $\in \{1, 3, \ldots, 2^{n}-1\}$, and B $\in \{1, 2, \ldots, 2^{n}-1\}$ for n = 8. Our scheme gives the liberty to generate dynamic S-boxes and makes an invader's attempts more fruitless keeping in view the drawbacks present in the above-stated techniques.

IV. CONCLUSION

Many existing S-boxes are deficient in different security criteria like non-bijectiveness, the existence of fixed points, etc. Others employ static permutations, fixed irreducible polynomials, static affine transformations, and follow complex construction processes. Most of these methods have very less S-box space. This paper projected an innovative square polynomial transformation along with a novel affine transformation to construct dynamic S-boxes. A pioneering permutation approach is employed to enhance the nonlinearity performance of the input S-box. The proposed method has the capability to erect a huge number of robust S-boxes by applying minute changes in the values of parameters of transformation and permutation processes. Thus, a huge S-box space is available by the proposed scheme. All the parameters are integers and values in these parameters are taken from the cipher key which assist in creating dynamic S-boxes. An instance S-Box is erected, and its performance analysis has been done using typical S-box criteria. The proposed S-box is free of above-mentioned drawbacks of the existing S-boxes. The performance and comparative analyses authenticate that the proposed S-box has the true competence for its inclusion in modern-day ciphers to provide much needed protection of data.

REFERENCES

[1] C. Paar, J. Pelzl, and B. Preneel, *Understanding Cryptography*, 1st ed. Berlin, Germany: Springer, 2010.
[2] M. M. Lauridsen, C. Rechberger, and L. R. Knudsen, "Design and analysis of symmetric primitive," Tech. Univ. Denmark, Kgs. Lyngby, Denmark, Tech. Rep. 382, 2016.
[3] M. Ahmad, E. Al Solami, X.-Y. Wang, M. Doja, M. Beg, and A. Alzaidi, "Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos," *Symmetry*, vol. 10, no. 7, p. 266, Jul. 2018.
[4] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, Jan. 2017.
[5] A. Belazi, A. A. A. El-Latif, R. Rhouma, and S. Belghith, "Selective image encryption scheme based on DWT, AES S-box and chaotic permutation," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2015, Art. no. 606610.
[6] M. Ahmad, H. Chugh, A. Goel, and P. Singla, "A chaos- based method for efficient cryptographic S-box design," in *Proc. Int. Symp. Secur. Comput. Commun.* Berlin, Germany: Springer, 2013, pp. 130–137.
[7] E. Tanyildizi and F. Ozkaynak, "A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps," *IEEE Access*, vol. 7, pp. 117829–117838, 2019.
[8] M. Ahmad, E. Al-Solami, A. M. Alghamdi, and M. A. Yousaf, "Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures," *IEEE Access*, vol. 8, pp. 110397–110411, 2020.
[9] K. Mohamed, M. Nazran, M. Pauzi, F. Hani, H. M. Ali, S. Ariffin, N. Huda, and N. Zulkipli, "Study of S-box properties in block cipher," in *Proc. Int. Conf. Comp. Commun. Control Tech.*, Langkawi, Malaysia, Sep. 2014, pp. 2–4.
[10] A. Alabaichi and A. I. Salih, "Enhance security of advance encryption standard algorithm based on key-dependent S-box," in *Proc. 5th Int. Conf. Digit. Inf. Process. Commun. (ICDIPC)*, Sierre, Switzerland, Oct. 2015, pp. 7–9.
[11] C.-M. Ou, "Design of block ciphers by simple chaotic functions," *IEEE Comput. Intell. Mag.*, vol. 3, no. 2, pp. 54–59, May 2008.
[12] S. Garg and D. Upadhyay, "S-box design approaches: Critical analysis and future directions," *Int. J. Adv. Res. Comput. Sci. Electron. Eng.*, vol. 2, no. 4, pp. 426–430, 2013.
[13] G. Jakimoski and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 2, pp. 163–169, Feb. 2001.
[14] M. Ahmad, N. Mittal, P. Garg, and M. M. Khan, "Efficient cryptographic substitution box design using travelling salesman problem and chaos," *Perspect. Sci.*, vol. 8, pp. 465–468, Sep. 2016.
[15] M. Ahmad, H. Haleem, and P. M. Khan, "A new chaotic substitution box design for block ciphers," in *Proc. Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Delhi, India, Feb. 2014, pp. 255–258.
[16] 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.
[17] M. Ahmad, M. N. Doja, and M. M. S. Beg, "ABC optimization based construction of strong substitution-boxes," *Wireless Pers. Commun.*, vol. 101, no. 3, pp. 1715–1729, Aug. 2018.
[18] A. A. Alzaidi, M. Ahmad, M. N. Doja, E. A. Solami, and M. M. S. Beg, "A new 1D chaotic map and β-hill climbing for generating substitution-boxes," *IEEE Access*, vol. 6, pp. 55405–55418, 2018.
[19] A. A. Alzaidi, M. Ahmad, H. S. Ahmed, and E. A. Solami, "Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map," *Complexity*, vol. 2018, Dec. 2018, Art. no. 9389065.
[20] J. Peng, S. Jin, L. Lei, and R. Jia, "A novel method for designing dynamical key-dependent S-boxes based on hyperchaotic system," *Int. J. Advancements Comput. Technol.*, vol. 4, no. 18, pp. 282–289, Oct. 2012.
[21] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, Jul. 2018.
[22] F. A. Kadhim, G. H. A. Majeed, and R. S. Ali, "Proposal new S-box depending on DNA computing and mathematical operations," in *Proc. Al-Sadeq Int. Conf. Multidisciplinary IT Commun. Sci. Appl. (AIC-MITCSA)*, Baghdad, Iraq, May 2016, pp. 1–6.
[23] A. H. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. I. Udzir, "A new DNA-based S-box," *Int. J. Eng. Technol.*, vol. 15, no. 4, pp. 1–9, 2015.
[24] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with DNA binary strands," *Biosystems*, vol. 57, no. 1, pp. 13–22, Jun. 2000.
[25] N. H. UbaidurRahman, C. Balamurugan, and R. Mariappan, "A novel DNA computing based encryption and decryption algorithm," *Procedia Comput. Sci.*, vol. 46, pp. 463–475, Jan. 2015.
[26] B. B., J. Frank, and T. Mahalakshmi, "Secure data transfer through DNA cryptography using symmetric algorithm," *Int. J. Comput. Appl.*, vol. 133, no. 2, pp. 19–23, Jan. 2016.
[27] H. Shaw, "A cryptographic system based upon the principles of gene expression," *Cryptography*, vol. 1, no. 3, p. 21, Nov. 2017.
[28] 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.
[29] N. A. Azam, U. Hayat, and I. Ullah, "An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization," *Secur. Commun. Netw.*, vol. 2018, Dec. 2018, Art. no. 3421725.
[30] B. N. Tran, T. D. Nguyen, and T. D. Tran, "A new S-box structure based on graph isomorphism," in *Proc. Int. Conf. Comput. Intell. Secur.*, Beijing, China, Dec. 2009, pp. 463–467.
[31] A. Razaq, H. Alolaiyan, M. Ahmad, M. A. Yousaf, U. Shuaib, W. Aslam, and M. Alawida, "A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups," *IEEE Access*, vol. 8, pp. 75473–75490, 2020.
[32] B. R. Gangadari and S. R. Ahamed, "Design of cryptographically secure AES like S-box using second-order reversible cellular automata for wireless body area network applications," *Healthcare Technol. Lett.*, vol. 3, no. 3, pp. 177–183, Sep. 2016.

[33] A. Shafique and F. Ahmed, "Image encryption using dynamic S-box substitution in the wavelet domain," *Wireless Pers. Commun.*, vol. 115, no. 3, pp. 2243–2268, Dec. 2020.

[34] Y. Wang, K.-W. Wong, C. Li, and Y. Li, "A novel method to design S-box based on chaotic map and genetic algorithm," *Phys. Lett. A*, vol. 376, nos. 6–7, pp. 827–833, Jan. 2012.

[35] D. Zhu, X. Tong, M. Zhang, and Z. Wang, "A new S-box generation method and advanced design based on combined chaotic system," *Symmetry*, vol. 12, no. 12, p. 2087, Dec. 2020.

[36] 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.

[37] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, and A. Alzamil, "Implementing a symmetric lightweight cryptosystem in highly constrained IoT devices by using a chaotic S-box," *Symmetry*, vol. 13, no. 129, pp. 1–20, 2021.

[38] V. Angelova and Y. Borissov, "Plaintext recovery in DES-like cryptosystems based on S-boxes with embedded parity check," *Serdica J. Comput.*, vol. 7, no. 3, pp. 257–270, 2013.

[39] N. A. Khan, M. Altaf, and F. A. Khan, "Selective encryption of JPEG images with chaotic based novel S-box," *Multimedia Tools Appl.*, vol. 80, no. 6, pp. 9639–9656, Mar. 2021.

[40] H. S. Alhadawi, D. Lambić, M. F. Zolkipli, and M. Ahmad, "Globalized firefly algorithm and chaos for designing substitution box," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102671.

[41] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A new design of cryptosystem based on S-box and chaotic permutation," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19129–19150, Jul. 2020.

[42] W. Gao, B. Idrees, S. Zafar, and T. Rashid, "Construction of nonlinear component of block cipher by action of modular group PSL(2, Z) on projective line PL(GF(2^8))," *IEEE Access*, vol. 8, pp. 136736–136749, 2020.

[43] S. Farwa, T. Shah, and L. Idrees, "A highly nonlinear S-box based on a fractional linear transformation," *SpringerPlus*, vol. 5, no. 1, p. 1658, Dec. 2016.

[44] 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.* , vol. 14, no. 2, pp. 1779–1785, 2011.

[45] 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.

[46] M. Sarfraz, I. Hussain, and F. Ali, "Construction of S-box based on Mobius transformation and increasing its confusion creating ability through invertible function," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, pp. 187–199, Feb. 2016.

[47] A. Zahid, M. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Entropy*, vol. 21, no. 3, p. 245, Mar. 2019.

[48] A. Zahid and M. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, Mar. 2019.

[49] A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," *IEEE Access*, vol. 8, pp. 150326–150340, 2020.

[50] S. Sahmoud, W. Elmasry, and S. Abudalfa, "Enhancement the security of AES against modern attacks by using variable key block cipher," *Int. Arab J. e-Tech.*, vol. 3, pp. 17–26, Jan. 2013.

[51] J. Cui, L. Huang, H. Zhong, C. Chang, and W. Yang, "An improved AES S-box and its performance analysis," *Int. J. Innov. Comput., Inf. Control*, vol. 7, no. 5, pp. 2291–2302, 2011.

[52] P. Agarwal, A. Singh, and A. Kilicman, "Development of key-dependent dynamic S-boxes with dynamic irreducible polynomial and affine constant," *Adv. Mech. Eng.*, vol. 10, no. 7, pp. 1–18, 2018.

[53] E. M. Mahmoud, A. Abd, T. A. E. El Hafez, and T. A. El Hafez, "Dynamic AES-128 with key-dependent S-box," *Int. J. Eng. Res. Appl.*, vol. 3, no. 1, pp. 1662–1670, Jan./Feb. 2013.

[54] M. S. M. Malik, M. A. Ali, M. A. Khan, M. Ehatisham-Ul-Haq, S. N. M. Shah, M. Rehman, and W. Ahmad, "Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices," *IEEE Access*, vol. 8, pp. 35682–35695, 2020.

[55] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. Amsterdam: Elsevier, 2009.

[56] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami, and W. Alhakami, "Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications," *IEEE Access*, vol. 8, pp. 116132–116147, 2020.

[57] 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.

[58] Z. B. Faheem, A. Ali, M. A. Khan, M. E. Ul-Haq, and W. Ahmad, "Highly dispersive substitution box (S-box) design using chaos," *ETRI J.*, vol. 42, no. 4, pp. 1–14, 2020.

[59] S. Hussain, S. S. Jamal, T. Shah, and I. Hussain, "A power associative loop structure for the construction of non-linear components of block cipher," *IEEE Access*, vol. 8, pp. 123492–123506, 2020.

[60] A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Sci. Rep.*, vol. 10, no. 1, p. 116, Dec. 2020.

[61] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dyn.*, vol. 99, no. 4, pp. 3041–3064, Mar. 2020.

[62] D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlinear Dyn.*, vol. 100, no. 1, pp. 699–711, Mar. 2020.

[63] H. Liu, A. Kadir, and C. Xu, "Cryptanalysis and constructing S-box based on chaotic map and backtracking," *App. Math. Comp.*, vol. 376, pp. 1–11, Jul. 2020.

[64] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

[65] I. Hussain, T. Shah, M. A. Gondal, and W. A. Khan, "Construction of cryptographically strong 8×8 S-boxes," *World App. Sc. J.*, vol. 13, no. 11, pp. 2389–2395, 2011.

[66] N. Siddiqui, A. Naseer, and M. Ehatisham-Ul-Haq, "A novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve," *Wireless Pers. Commun.*, vol. 116, no. 4, pp. 3015–3030, Feb. 2021.

[67] A. Alghafis, N. Munir, and M. Khan, "An encryption scheme based on chaotic Rabinovich-Fabrikant system and S_8 confusion component," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 7967–7985, Feb. 2021.

[68] H. S. Alhadawi, M. A. Majid, D. Lambić, and M. Ahmad, "A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 7333–7350, Feb. 2021.

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

[70] D. Lambić, "S-box design method based on improved one-dimensional discrete chaotic map," *J. Inf. Telecommun.*, vol. 2, no. 2, pp. 181–191, Apr. 2018, doi: 10.1080/24751839.2018.1434723.

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

[72] J. Wang, Y. Zhu, C. Zhou, and Z. Qi, "Construction method and performance analysis of chaotic S-box based on a memorable simulated annealing algorithm," *Symmetry*, vol. 12, no. 2115, pp. 1–14, 2020.

[73] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Crypto. Tech.*, Santa Barbara, CA, USA, Aug. 1986, doi: 10.1007/3-540-39799-X_41.

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

[75] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. Abd EL-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci.*, vol. 515, pp. 191–217, Apr. 2020.

[76] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Adv. Cryptol.*, Lofthus, Norway, 1994, pp. 386–397.

[77] 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, Apr. 2018.

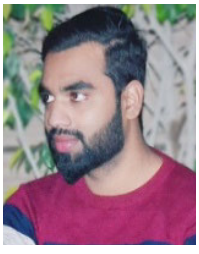
[78] Attaullah, S. S. Jamal, and T. Shah, "A novel algebraic technique for the construction of strong substitution box," *Wireless Pers. Commun.*, vol. 99, no. 1, pp. 213–226, Mar. 2018.

[79] 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, 2019.

[80] B. Arshad and N. Siddiqui, "Construction of highly nonlinear substitution boxes (S-boxes) based on connected regular graphs," *Int. J. Comp. Sc. Info. Sec.*, vol. 18, no. 4, pp. 109–122, 2020.
[81] N. Siddiqui, F. Yousaf, F. Murtaza, M. E. Haq, M. U. Ashraf, A. M. Alghamdi, and A. S. A. S. Alfakeeh, "A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field," *PLoS ONE*, vol. 15, no. 11, pp. 1–16, 2020.
[82] S. Ibrahim and A. M. Abbas, "A novel optimization method for constructing cryptographically strong dynamic S-boxes," *IEEE Access*, vol. 8, pp. 225004–225017, 2020.
[83] L. C. N. Chew and E. S. Ismail, "S-box construction based on linear fractional transformation and permutation function," *Symmetry*, vol. 12, no. 826, pp. 1–16, 2020.

AMJAD HUSSAIN ZAHID received the Ph.D. degree in computer science (information security) from the University of Engineering and Technology, Lahore, Pakistan. He is currently working as an Assistant Professor with the University of Management and Technology (UMT), Lahore. He is also the Program Advisor of B.S. (IT) program and a member of many academic bodies. He has more than 23 years of qualitative experience in teaching. He is vigorous in academic research and his research interests include information security, programming languages, algorithm design, enterprise architecture, technology management, IT infrastructure, and blockchain. He is also serving as an efficient and effective reviewer in several reputed international research journals of high impact factor in the domain of information security. He possesses quality monitoring and maintaining capabilities along with the strong interpersonal, leadership, and team management skills. He has been an Active Member of Higher Education Commission (HEC) National Curriculum Revision Committee (NCRC), Pakistan. He has also been an Active Member of faculty board of studies for the Punjab University College of Information Technology (PUCIT) and the Virtual University of Pakistan.

HAMZA RASHID received the B.S. degree in software engineering from the University of Sargodha, Sargodha, Pakistan, and the M.S. degree in software engineering from the University of Management and Technology (UMT), Lahore, Pakistan. He is currently working as a Lecturer with the Riphah International College, Lahore. He is also the Program Advisor of ADP (CS) program. His current research interests include cryptography, cybersecurity, data science, information technology, computer networks, and software quality assurance.



MIAN MUHAMMAD UMAR SHABAN received the B.S. degree in computer science from Government College University (GCU) Faisalabad, Pakistan, and the M.S. degree in computer science from the University of Management and Technology (UMT), Lahore, Pakistan. His current research interests include information security, ethical hacking, cryptanalysis, and blockchain.

SOBAN AHMAD received the B.S. and M.S. degrees in software engineering from the University of Management and Technology (UMT), Lahore. His current research interests include cryptography and computer networks.

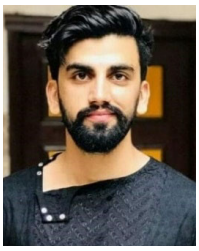
EHTEZAZ AHMED received the B.S. degree in software engineering from COMSATS University Islamabad, Islamabad, Pakistan, in 2017, and the M.S. degree in software engineering from the University of Management and Technology (UMT), Lahore, Pakistan, in 2021. He is currently working as a Software Developer with Punjab Information and Technology Board (PITB), Lahore. He has more than three years of experience in the Software Development Industry. He has exceptional interpersonal and intrapersonal skills. Having strong professional skills in software project management, web development, database management, problem solving, and technical logics. His research interests include information security, cryptography, requirement engineering, software project management, database management, and cloud computing.

MUHAMMAD TALLAL AMJAD received the B.S. degree in software engineering from COMSATS University Islamabad, Islamabad, Pakistan, and the M.S. degree in software engineering from the University of Management and Technology (UMT), Lahore, Pakistan. His current research interests include cryptography, information technology, user authentication, computer networks, and software quality assurance.

MUHAMMAD AZFAR TARIQ BAIG received the B.S. degree in computer science from COMSATS University Islamabad–Sahiwal, Pakistan, in 2017, and the M.S. degree in computer science from the University of Management and Technology (UMT), Lahore, Pakistan, in 2020. He did M.S. thesis in the field of cryptography. His research interests include information security and cryptography.

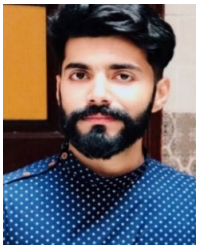
MUHAMMAD JUNAID ARSHAD is currently working as an Associate Professor with the University of Engineering and Technology (UET), Lahore. He is also the HEC Approved Ph.D. Supervisor and very much active in research. He has more than 50 national and international publications to his credit. He is working on three funded research proposals approved by HEC and UET Lahore. He is also an Advisor with the Punjab Public Service Commission and the Federal Public Service Commission. He has supervised more than 50 B.S. research projects, 60 M.Sc./M.Phil. theses, and also supervising five Ph.D. scholars. His research interests include protocols and algorithms for heterogeneous networks, data centre networks, multi-homed networks focusing on performance, computer architecture, mobile ad-hoc networks, simulation and modelling, information security, and cloud computing. He is also a member of the IEEE Computer Society and the IEEE Communications Society Korea Information and Communications Society (KICS). He is also serving as an editor/reviewer for many reputed international research journals.

MUHAMMAD NADEEM TARIQ received the B.S. degree in computer science with a focus on security and privacy from the Federal Urdu University of Arts, Science and Technology, Islamabad. He is currently pursuing the M.S. degree with the University of Management and Technology (UMT), Lahore, Pakistan. His research interests include information security and cryptography.



MUHAMMAD WASEEM TARIQ received the B.S. degree in information technology from Ghazi University, Dera Ghazi Khan, Pakistan. He is currently a Student of Information System (Data Sciences) with the University of Management and Technology, Lahore. He is also working in information security domain.

MUHAMMAD AYAZ ZAFAR received the B.S. degree in computer science from Lahore Garrison University (LGU), Lahore, Pakistan, in 2019. He is currently pursuing the M.S. degree in computer science from the University of Management and Technology (UMT), Lahore, and doing a thesis on sign language conversation. He is also working as a Lecturer with the Riphah International College, Lahore. He is also the Batch Advisor of the ADP (CS) program. His research interest includes the communication of Deaf and Dumb people with normal people with natural language processing. His research also interests include natural language processing (NLP), information retrieval techniques, cryptography, the Internet of Things (IoT), and the security of IoT.



ABDUL BASIT received the B.S. degree in information technology from Ghazi University, Dera Ghazi Khan, Pakistan. He is currently pursuing the M.S. degree in information technology with the University of Management and Technology (UMT), Lahore. He is also working in information security domain.