IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received August 26, 2021, accepted September 12, 2021, date of publication September 16, 2021, date of current version September 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3113338

Construction of Optimized Dynamic S-Boxes Based on a Cubic Modular Transform and the Sine Function

AMJAD HUSSAIN ZAHID[1], MUSHEER AHMAD[2], AHMED ALKHAYYAT[3], MUHAMMAD JUNAID ARSHAD[4], MIAN MUHAMMAD UMAR SHABAN[1], NAGLAA F. SOLIMAN[5], AND ABEER D. ALGARNI[5]

[1]Department of Informatics and Systems, University of Management and Technology, Lahore 54700, Pakistan
[2]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[3]Department of Computer Technical Engineering, College of Technical Engineering, Islamic University, Najaf 54001, Iraq
[4]Department of Computer Science, University of Engineering and Technology, Lahore 54700, Pakistan
[5]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 84428, Saudi Arabia

Corresponding authors: Musheer Ahmad (musheer.cse@gmail.com) and Naglaa F. Soliman (nfsoliman@pnu.edu.sa)

This research was funded by the Deanship of Scientific Research at Princess Nourah Bint Abdulrahman University through the Fast-track Research Funding Program.

ABSTRACT The protection of sensitive data from illegitimate users is one of the main challenges in today's technological era. To handle prevailing security-related problems and challenges amicably, cryptographic techniques are applied for the fortification of data. State-of-the-art cryptographic ciphers generally use substitution-boxes (S-boxes) that help in accomplishing robust sanctuary of data. Provision of data security by a cipher is proportionate directly to the cryptographic strength of an S-box employed in the respective cipher. This research paper proposes to project a simple and innovative scheme for the generation of dynamic S-boxes by employing a novel cubic modular transformation along with the trigonometric sine function. A pioneering optimization phase, dynamic in nature, is also suggested that improvises the nonlinearity of the initial configuration of S-box. The overall proposed scheme possesses the potential to spawn a large count of strong S-boxes by smearing a minute variation in input parameters used in initial and optimization phases. Cipher key is used to employ values to the input parameters for the creation of dynamic S-boxes. A specimen S-box is presented, and its performance has been achieved through standard criteria of S-box evaluation along with the comparative analysis with some existing S-boxes. Recital and comparative investigations validate that the anticipated S-box possesses the real capability for its usage in cryptosystems for much needed data security.

INDEX TERMS Substitution-box, cubic modular transform, sine function, optimization, cryptography.

I. INTRODUCTION

In the modern technological era, a tremendous volume of data is triggered on daily basis and its communication over public channels from one place to other places has become an obligatory part of our life. Data is a vital asset and must be protected from the attackers so that they are unable to use it maliciously if they obtain or steal it somehow. To prevent data from such hazards, its conversion into a meaningless form is done before its transmission over public channels. Different methods are employed to convert meaningful data into meaningless data. Cryptography is one such domain that helps in this transformation and holds sturdy algorithms known as ciphers to assist in the security of data and information. These ciphers are categorized into two core types namely the Stream ciphers and Block ciphers [1]. The former cipher performs encoding or enciphering one byte/bit to another byte/bit at once. A block cipher performs these operations in a chunk-by-chunk manner. A chunk of data or information mostly contains more than one byte. Nowadays, block ciphers are frequently adopted by organizations to secure their confidential information from invaders due to simple implementation and easy deployment [2], [3]. Few illustrious block ciphers employed in numerous security

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

applications are Advanced Encryption Standard (AES), Blowfish, RC5, Twofish, etc. A block cipher bestows security with the assistance of permutation and substitution operations which are used to translate plaintext form of data into an enigmatic form. In permutation, the bits/bytes of the message are shuffled in such a manner that the permutated message contains the same bits/bytes (of the original message), whereas a substitution method replaces bits/bytes of the original plaintext with some other bits/bytes that are not the constituents of the original message. A substation operation requires a table to assist in the replacement process known as a substitution box (S-box) [4]–[6]. A substitution box (S-box) is a significant element of modern block ciphers to assist in the generation of meaningless data (ciphertext) from the original message (plaintext). S-boxes help in creating a non-linear relationship among input (original message) and output (meaningless form) data to provoke more confusion for the Invaders. If an S-box employed in a particular block cipher is capable to generate more muddle for the attackers in the produced ciphertext, that cipher offers more protection to the plaintext. S-boxes work in a non-linear manner to enhance the protection of data, whereas other elements of a particular cipher operate in a linear style. Therefore, the security offered for the original message by a block cipher using S-boxes as the components directly depends on the cryptographic strength of these S-boxes [7]–[9]. The modern-day cryptosystems utilize two categories of S-boxes named as static and dynamic S-boxes. A static S-box has fixed arrangement of random values and a cipher using such an S-box provides less security to the plaintext as the invaders may be able to get such a static S-box somehow and produce plaintext from the captured ciphertext using it [10]. AES and DES ciphers used static S-boxes in their operation and attackers tried cryptanalytic efforts on these ciphers by exploiting the weaknesses offered by the respective static S-boxes.

To daze the disadvantages and weaknesses of static S-boxes, modern block ciphers utilize dynamic S-boxes to avail the cryptographic fortes associated with them [11], [12]. A dynamic S-box is produced using cipher key and is capable to increase the cryptographic strength offered by a cipher. One can obtain different novel S-boxes by utilizing different values of the key. These dynamic S-boxes are employed in ciphers to improve the security of the sensitive information. As a result, innumerable researchers have proposed new and novel methods to generate key-dependent S-boxes under the control of secret key.

Chaos theory has the capability to produce randomness [13] and authors [14]–[19] have exploited this chaotic characteristic to generate robust S-boxes using various chaotic techniques for the protection of data. However, it was observed that a chaotic system does not disguise and protect data at all times [20]. Most of the hyperchaotic structures possess better complexities and dynamics than chaotic systems and a found another alternative to generate S-boxes. The hyperchaotic systems exhibit more than one positive Lyapunov exponents (LE) compared to the only one LE of a chaotic system [21]. So, a much more intricate attractor and dynamical performances are generated by the hyperchaotic systems as the system dynamics bloat in more than one direction, randomness is increased, and higher unpredictability is achieved [20], [21].

Consequently, authors [22], [23] have engendered cryptographically strong dynamic S-boxes based on hyperchaotic techniques. Another leading domain currently being utilized for the construction of strong S-boxes is DNA computing. Authors [24]–[29] exploited DNA computing and models to create robust and strong S-boxes and more secure ciphers. Investigation of DNA-based S-boxes proved and established their standing against cryptanalytic efforts. Another principal technique to produce dynamic and robust S-boxes is the linear fractional transformation (LFT). Researchers [30]–[33] applied LFT technique based on Galois Field (GF) in different ways to generate strong S-boxes. Many authors [34]–[36] introduced strong S-box generation methods based on simple and efficient transformations than the linear fractional transformations.

Advanced Encryption Standard (AES) is a renowned block cipher that utilized a single static S-box in encryption and a single static inverse S-box in decryption based on Galois Field in its working in each of its rounds. The arrangement of values in these AES static S-boxes is fixed. An invader having the knowledge of these static S-boxes gets the capability to launch attack(s) on the captured ciphertext and hence the protection of data is conceded. Similarly, computation of one value of AES S-box is based on the calculation of multiplicative inverse of one input value using Galois Field that consumes a lot of time and results in less efficient process to construct the resultant S-box. Keeping in view the weaknesses linked to the AES S-box, authors [37]–[41] projected numerous enhancements to the original AES S-box. These novel S-boxes are dynamic and better than AES S-box as a different S-box is employed in each of the AES rounds and linear and differential cryptanalysis efforts are made difficult as compared to the easy cryptanalytical efforts in case of AES static S-boxes.

Many researchers have investigated other domains of knowledge for the generation of S-boxes like optimization techniques [42]–[45], elliptic curve [46], [47], cellular automata [48], graph theory [49], [50], backtracking [51], etc.

Many modular schemes have been proposed for S-box generation by researchers like [31], [32], [34]–[35]. These proposals have demerits like use of fixed primitive polynomials [31], [32], presence of fixed points [31], lack of bijectivity [32], [34], less cryptographic strength [31], [34], [35], etc. So, there is a need of a novel modular approach that is free of the above-mentioned drawbacks. This research article introduces a novel scheme to create key-dependent strong S-boxes by employing values for the parameters A, B, and C from the cipher key. Each parameter has certain range of values and one has the option to pick any value from this range. This liberty of choosing any values makes the proposed scheme quite dynamic and consequently aids in increasing the cryptographic forte of the proposed S-box along with the augmented confusion for the invaders. The innovative scheme employs a novel cubic modular transformation (CMT) that is dynamic in nature along with the trigonometric Sine function to obtain an initial 8 x 8 S-box. The initial S-box results are further enhanced by employing an innovative heuristic evolution approach and one gets good nonlinear S-boxes having admirable cryptographic forte with respect to standard evaluation criteria.

Following are the principal contributions of our effort:

- A novel and simple cubic modular transformation (CMT), dynamic in nature, along with the trigonometric Sine function is proposed to produce an initial S-box. A large number of strong S-boxes are produced by a minute variation in the parameters' values.
- An innovative heuristic-based optimization approach, dynamic in nature, is suggested that improvises the nonlinearity of the initial S-box. The resultant S-box as the result of this approach has the capability to generate additional muddle in the ciphertext for the invaders.
- Resultant S-box and other prevalent S-boxes are contemptuously evaluated by means of typical S-box criteria. This recital analysis authenticates the remarkable say of the proposed scheme for the generation of dynamic S-boxes.

Rest of the paper has the following organization. Section II narrates the detailed methodology for the generation of S-boxes by employing an innovative cubic modular transform and a new heuristic-based optimization approach. Section III presents the generation of an example S-box and its recital and comparative analysis with some of the existing modern-day S-boxes. Section IV describes the conclusion of the work done in the paper.

II. PROPOSED METHOD FOR S-BOX DESIGN

Today, researchers design and utilize S-boxes in block ciphers to create as much muddle in the ciphertext as possible to create confusion for the invaders. An S-box supports in producing a nonlinear connotation among the plaintext and the ciphertext. This mapping makes it very challenging for an attacker to produce the plaintext from the captured data (ciphertext). As a result, researchers try to explore new and novel transformations that help in the generation of strong S-boxes. Here, we introduce an innovative scheme by employing a novel and dynamic cubic modular transformation, a trigonometric sine function application, and a pioneering heuristic based optimization approach to generate dynamic and strong S-boxes having worthy cryptographic forte. Comprehensive procedure for the generation of the projected S-box involves the following four simple phases which are described in the subsequent section.

1. Innovative Cubic Modular Transformation
2. Trigonometric Sine Function Application
3. Initial S-Box Generation
4. Novel Heuristic Evolution Approach

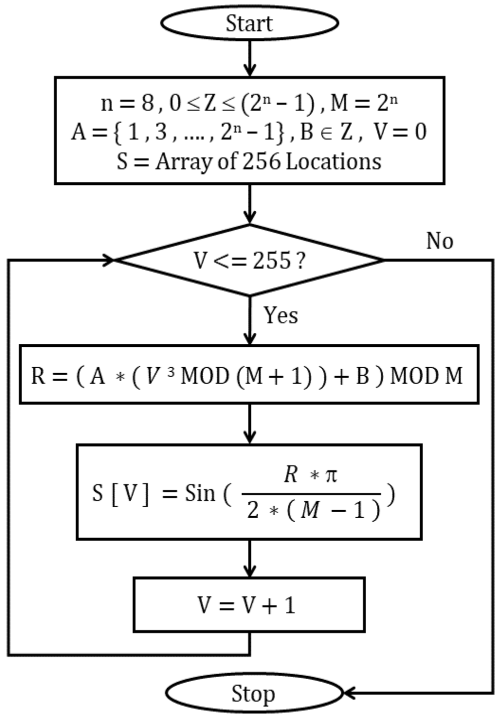

FIGURE 1. Working of Cubic Modular Transformation and Sine Function.

A. INNOVATIVE CUBIC MODULAR TRANSFORMATION

The proposed scheme erected substitution-boxes of size n × n using a novel cubic modular transformation (CMT) defined as a mathematical function in Eq. (1):

$$R = C(v) = \left(A * \left(V^3 \text{MOD } (2^n + 1\right) + B\right) \text{MOD } 2^n \quad (1)$$

where,

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

The cipher key employs the values for the variables A and B which make the CMT transformation given in Eq. (1) dynamic. This dynamism of the above transformation helps in the erection of dynamic S-boxes. With simple variation in values of parameters A and B, entirely different S-box can be easily obtained.

B. SINE FUNCTION APPLICATION

The well-known trigonometric sine function is applied to the value R obtained from Eq. (1). This makeover is given in Eq. (2) as:

$$S(R) = \text{Sin}\left((R * \pi)/(2 \times (2^n - 1))\right) \quad (2)$$

The working methodology of Eq. (1) and (2) is also demonstrated in the flowchart given in Figure 1.

C. INITIAL S-BOX GENERATION

The initial 8 × 8 S-box for $n = 8$ construction procedure using Eqs (1) and (2) is presented in Algorithm 1 and also

TABLE 1. Initial S-Box using Parameters' values A = 13, and B = 94.

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

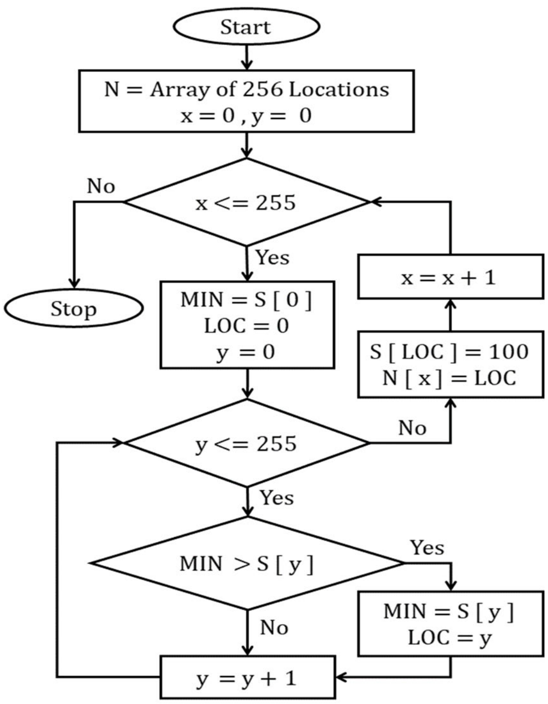

FIGURE 2. Initial S-box construction procedure.

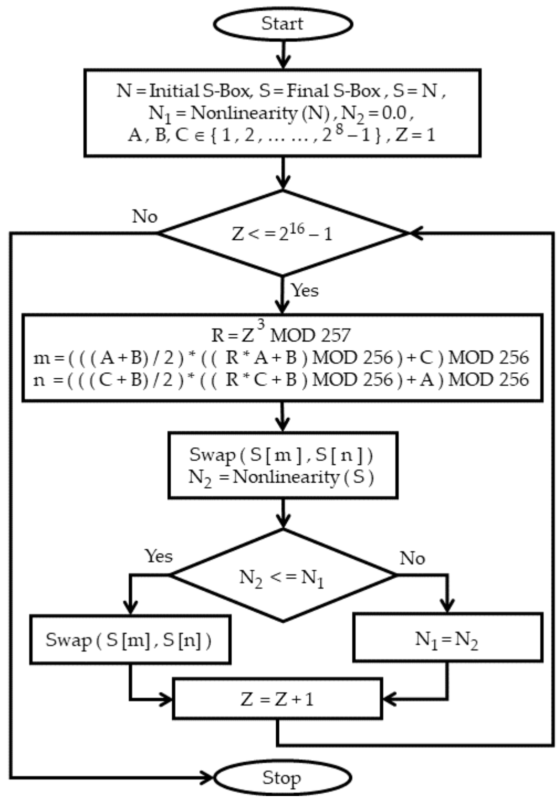

FIGURE 3. Heuristic Evolution-based Optimization Approach.

illustrated through a flowchart given in Figure 2. An example initial 8 × 8 S-box obtained for A = 13, B = 94 is specified in Table 1.

D. HEURISTIC-BASED OPTIMIZATION APPROACH

This step helps in permuting the values of the initial S-box generated using the procedure as presented in previous subsection. The proposed cubic modular transformation (CMT) is dynamic in nature and employs the values of different parameters of CMT through cipher key. Consequently, numerous S-Boxes are produced using this transformation. One can retain an S-box with good cryptographic strength and choose it as an initial S-Box. The heuristic-based

Algorithm 1 Initial S-Box Construction

```
Input parameters:
  n = 8   //  for an n × n S-box
  A       //  A ∈ {1, 3, ......, 2^n - 1 }
  B       //  B ∈ {0, 1, ......, 2^n - 1 }
  S       //  An array of size = 256
  M = 2^n
Output:
  N       // Initial S-box
Initializations:
  V ← 0
  X ← 0
  Y ← 0
while ( V <= 255 ) do
  r  ←  V^3  MOD  ( M + 1 )
  R ←  ( A ∗ r + B )  MOD  ( M )
  S [ V ] ←  Sin (  ( R ∗π ) / ( 2 ∗ ( M − 1 ) )  )       V
← V + 1
endwhile
while ( X <= 255 ) do
  MinVal ← S [ 0 ]
  Pos ← 0
  Y ← 0
  while ( Y <= 255 ) do
    if ( MinVal  >  S [ Y ] ) then
      MinVal ← S [ Y ]
      Pos ← Y
    endif
    Y ← Y + 1
  endwhile
  S [ Pos ] ← 100
  N [ X ] ← Pos
  X ← X + 1
endwhile
return N
```

optimization approach in the proposed scheme plays a vital part to produce robust and strong dynamic S-boxes from the chosen initial S-Box. This phase is the most crucial part of the proposed S-box generation scheme. It is responsible for fetching the strong configuration of S-box which exhibits strong nonlinear cryptographic strength of the final S-box. This approach is presented in Algorithm 2 and depicted in Figure 3. The cipher key involves the values for the variables A, B, and C used in the optimization phase that makes the approach dynamic. A specimen 8 × 8 S-box constructed after the heuristic-based optimization phase is listed in Table 2.

III. SECURITY ASSESSMENT OF PROPOSED S-BOX

A cryptographic S-box generated with the help of a certain method may be strong one to resist attacks or weak one to be the target of attackers. To appraise the forte of S-boxes under consideration, certain conditions or criteria are assessed and these must be fulfilled by an S-box to claim its strength.

Algorithm 2 Final S-Box Erection Using Novel Heuristic-Based Optimization Approach

```
Input parameters:
  A, B, C   // A, B, C ∈ { 0, 1, 2, ......, 2^8 - 1 }
  N         // Initial 8 × 8 S-box
Output:
  S         // Final 8 × 8 S-box
Initializations:
  Z ← 1,   S = N  , T = 256
  N1 ← Nonlinearity ( N ), N2 ← 0.0
while ( Z <= 2^16 − 1 ) do
  R ←  Z^3 MOD 257
  R1 ← (R∗A+B) MOD T, R2 ← (R∗C+B) MOD T
  m ← ( ( ( A + B) / 2 ) ∗ R1+ C ) MOD T
  n  ← ( ( ( C + B) / 2 ) ∗ R2+ A ) MOD T
  Swap ( S [ m ], S [ n ] )
  N2 ← Nonlinearity ( S )
  if ( N2 > N1 ) then
    N1 ← N2
  else
    Swap ( S[ m ], S[ n ] )
  endif
  Z ← Z + 1
endwhile
return S
```

This section examines the strength of the projected S-box depicted in Table 1 by employing standard criteria [52] to evaluate the cryptographic strength of any given S-box. We picked newly explored S-box methods for comparison of the security topographies of our projected S-box with these prevailing S-boxes.

A. BIJECTIVENESS

An S-box must satisfy bijectiveness requirement in a decent way. The bijectivity guarantees that for each unique input value, unique output value is produced and vice versa. Consequently, this input-output association should exhibit 1-to-1 mapping. Our proposed 8 x 8 S-box as presented in Table 1 demonstrates this property as each inimitable input value produces inimitable output value. Each coordinate Boolean function of resultant S-box has total count of 1's (128) equivalent to total count of 0's as proposed in [9], [47].

B. NONLINEARITY

A strong substitution-box essentially has a nonlinear mapping between the ciphertext (output) and the plaintext (input) because a linear mapping makes it easy for an attacker to get original message from the ciphertext. A nonlinear mapping helps in defying the attacks by an invader to deduce the plaintext from the ciphertext and an S-box demonstrating a nonlinear association between its input and output is desired one. Such a nonlinear association (known as nonlinearity)

TABLE 2. Proposed S-Box using Parameters' values A = 13, B = 94, and C = 63.

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

TABLE 3. Nonlinearity Scores of Constituent Boolean Functions.

Boolean Function	S1	S2	S3	S4	S5	S6	S7	S8
NL(Initial S-box)	106	106	106	108	106	106	106	108
NL(Final S-box)	112	110	110	112	110	112	112	112

needs to be higher. A high value of nonlinearity validates that the respective S-box is more resistant against the linear attacks. The nonlinearity value of an S-box with n-bit Boolean function S can be calculated with Eq. (3) [52]:

$$NL\left(S\right)=\left[\frac{2^n}{2}-\frac{1}{2}\left(T_{max}(S)\right)\right] \quad (3)$$

where, $T_{max}(S)$ represents Walsh-Hadamard Transformation for S-box having an n-bit Boolean function S. The Boolean functions that establish our initial and proposed (final) S-boxes and the resultant nonlinearity scores are illustrated in Table 3.

As shown in Table 3, the maximum nonlinearity score of initial S-box (given in Table 1) is 108, the minimum score is 106, and the average score is 106.5. The heuristic-based optimization approach presented in Algorithm 2 capable enough to yield an S-box which is having the maximum nonlinearity score of 112, the minimum score as 110, and a decent average score is 111.3 It clearly indicates a handsome improvisation in the nonlinearity scores of initial S-box through the novel heuristic-based optimization approach. The proposed S-box nonlinearity results are compared with state-of-the-art S-boxes in Table 4. The comparative results are evident that nonlinearity scores of our S-box exceed than the nonlinearity values of recently published S-box studies.

TABLE 4. Comparison of Nonlinearities of different S-boxes.

S-Box Method	Nonlinearity		
	Min	Max	Mean
[17]	108	110	109.3
[31]	106	110	108
[34]	104	110	107.5
[35]	104	108	106.8
[53]	106	110	108.5
[54]	104	108	105.0
[55]	104	110	106.3
[56]	106	108	106.5
[57]	106	112	109.5
[58]	104	108	106.3
[59	104	110	106.9
[60]	106	108	106.5
[61]	106	108	107.0
[62]	110	112	111.8
[63]	110	112	111.5
[64]	110	112	110.3
[65]	110	112	111.5
Proposed	110	112	111.3

C. STRICT AVALANCHE CRITERION (SAC)

Websters and Tavares gave a criterion which guarantees that a one-bit change in the input (plaintext or key) must change

TABLE 5. Dependency Matrix of SAC Scores of Proposed S-box.

.4688	.5625	.5000	.5625	.5000	.4688	.4844	.4844
.4531	.4375	.4844	.5625	.5313	.4375	.4844	.4844
.5313	.4531	.4688	.5625	.4531	.4844	.5156	.5469
.5000	.4844	.5156	.5313	.5156	.4844	.5156	.5469
.5156	.4844	.4531	.5469	.4375	.5000	.5000	.5469
.5313	.5469	.4844	.4531	.4688	.4844	.4844	.5156
.5000	.5156	.5781	.5000	.5000	.4844	.4844	.5000
.4844	.5469	.5000	.4844	.5625	.5000	.4844	.4688

TABLE 6. BIC-NL matrix of Proposed S-box.

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

50% of the output bites [68]. This is famously known as the strict avalanche performance criterion (SAC). Strong encryption schemes should be able to satisfy this avalanche criterion well. The SAC scores of our proposed S-box are shown as the dependency matrix in Table 5. If the value of SAC of an S-Box is near 0.5, it is treated as a robust one. Average value of SAC scores from Table 5 is 0.5 that authenticates the fulfillment of SAC by our proposed S-box in a decent manner. The SAC score of proposed S-box is equated with the SAC scores of the some existing S-boxes in Table 6. Comparative result demonstrates that the proposed S-box SAC value shows an elegant and better fulfillment of SAC property compared to SAC values of these S-boxes.

D. BIT INDEPENDENCE CRITERION (BIC)

Bit independence criterion ensures that due to a one-bit change in the input (plaintext or key), change in the values of any bits from output is independent of each other [68]. An S-box designer attempts to generate an S-box while keeping in mind this criterion. BIC-Nonlinearity (BIC-NL) results of proposed S-box are illustrated in Table 6. Average BIC-NL value computed from Table 6 is 103.8. This score is an indication that output bits depend feebly on each other and hence proposed S-box appeases the BIC in an elegant manner. The BIC for nonlinearity of anticipated S-box is compared with the recently published S-boxes in Table 7. The critical assessment reveals that the BIC-NL value of the proposed S-box shows an elegant uniformity with the BIC-NL values of contemporary S-boxes.

TABLE 7. Comparison of BIC-NL and SAC Scores.

S-Box	BIC-NL	SAC
[17]	108.2	0.506
[31]	105.3	0.497
[34]	103.5	0.498
[35]	103.9	0.507
[53]	103.9	0.500
[54]	103.5	0.506
[55]	103.9	0.503
[56]	104.1	0.501
[57]	106.9	0.507
[58]	103.6	0.501
[59	106.1	0.509
[60]	103.6	0.499
[61]	102.3	0.493
[62]	103.7	0.502
[63]	103.7	0.502
[64]	104.1	0.495
[65]	104.2	0.506
Proposed	103.8	0.503

E. LINEAR PROBABILITY (LP)

A cryptosystem creator tries to muddle plaintext bits in the best possible way to produce such a ciphertext that is more and more meaningless for the invaders and their attempts of cracking the ciphertext are useless. An S-box created carefully assists in achieving this jumble by producing nonlinear mapping between plaintext and ciphertext bits. The cryptographic forte of this mapping known as linear probability (LP) of an explicit 8 x 8 S-box F is calculated by Eq. (4) [69].

$$LP = \underset{p_r, q_r \neq 0}{MAXIMUM} \left| 2^{-n} \left(\# \{ r \in N \mid r.p_r = F(r).q_r \} \right) - \frac{1}{2} \right| \quad (4)$$

whereas,

$$p_r = \text{input mask}, \quad q_r = \text{output mask}$$
$$N = \{0, 1, \ldots, 2^n - 1\}.$$

If a linear relationship exists among the input and output bits of an S-box, linear probability value of that S-box is high, and it is easy for invaders to perform linear cryptanalysis. Linear probability (LP) score of projected S-box depicted in Table 2 comes out as 0.125 which is very low, and it indicates the resistance of proposed S-box towards linear cryptanalysis. LP value of the proposed S-box

TABLE 8. Differential Distribution Matrix of Proposed S-box.

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

is compared with the recently published S-boxes in Table 9. The comparison result provides evidence that our S-box has enough cryptographic strength to confront the Matsui's cryptanalysis.

F. DIFFERENTIAL UNIFORMITY (DU)

Invaders seize ciphertext communicated over the public channels and try to cryptanalyze it. Different attempts are made by finding the alterations in the ciphertext as well as alterations in the input (plaintext). Careful analysis of such alterations assists an invader to reach the full or part of the key or plaintext [70]. An S-box creator attempts to reduce the dissimilarity between such alterations. Such a difference is assessed through differential uniformity (DU) property of S-boxes. Low value of DU helps in the resistance to the differential cryptanalysis. Value of DU of an n x n S-box S is computed using Eq. (5) [71].

$$DU = \underset{\Delta_c \neq 0, \Delta_d}{Max} \left[\# \{ c \in R | S(c) \oplus S(c \oplus \Delta_c) = \Delta_d \} \right] \quad (5)$$

where,

Δ_c, Δ_d = Input and output differentials,

and

$R = \{0, 1, \ldots\ldots, 2^n - 1\}$.

The results of differential uniformity are presented in Table 8 through the differential distribution matrix. The maximum score of this matrix is 10 which the DU of the proposed S-box and respective score of DP (differential probability) is 0.039. The obtained low scores of differential uniformity and differential probability specify that anticipated S-box has the latent to defy differential cryptanalysis. The projected S-box DP sore is equated with DP values of some recently investigated S-boxes in Table 9. The comparative analysis provides evidence that the DP of proposed S-box is gracefully consistent with the values of DP of other S-boxes and thus possesses enough cryptographic strength to rebel the differential cryptanalytic efforts practiced by the invaders to break the ciphers involving S-boxes.

G. FIXED POINTS ANALYSIS (FPA)

If an n x n S-box S is designed in such a way that S (u) = u for some u's where $0 \leq u \leq 2^n - 1$, S has some fixed points (FP). Such an S-box presents severe weakness to the invaders of the ciphertext. Attackers try to find one or more FP's in an S-box employed in a cipher to exploit the feebleness presented by such S-boxes. Hence, careful S-box designers generate substitution boxes that don't own such fixed points [64]. The comparative analysis of some recent S-boxes and the proposed S-box with respect to the FP's is given in Table 9. The proposed S-box does not contain any FP and thus gratifies FPA condition gracefully. Table 9 reveals that some recent S-boxes contain fixed points and use of such S-boxes may provide weaker protection to the ciphertext.

H. EFFECTIVENESS OF NOVEL HEURISTIC-BASED OPTMIZATION APPROACH

To validate the effectiveness of the novel heuristic-based nonlinearity performance optimization approach, Table 10 is maintained to illustrate the average NL values of few initial S-boxes generated using Algorithm 1. These initial S-boxes are processed using proposed Algorithm 2 to improvise the NL scores. The results are shown in Table 10. It is evident that the novel heuristic-based optimization approach, presented in Algorithm 2 and Figure 3, effectively improvises the NL scores of the respective initial S-boxes as seen in Table 10. The effectiveness of the

TABLE 9. Recital Comparison of DP, LP and Fixed Points of Different S-Boxes.

S-Box Method	LP	DP	FPs
[17]	0.094	0.031	0
[31]	0.125	0.063	2
[34]	0.141	0.039	0
[35]	0.141	0.054	0
[53]	0.133	0.039	1
[54]	0.133	0.039	2
[55]	0.133	0.039	1
[56]	0.133	0.039	0
[57]	0.133	0.031	0
[58]	0.133	0.039	0
[59	0.125	0.031	2
[60]	0.125	0.039	0
[61]	0.141	0.047	1
[62]	0.125	0.039	0
[63]	0.125	0.039	0
[64]	0.125	0.039	1
[65]	0.125	0.039	0
Proposed	0.125	0.039	0

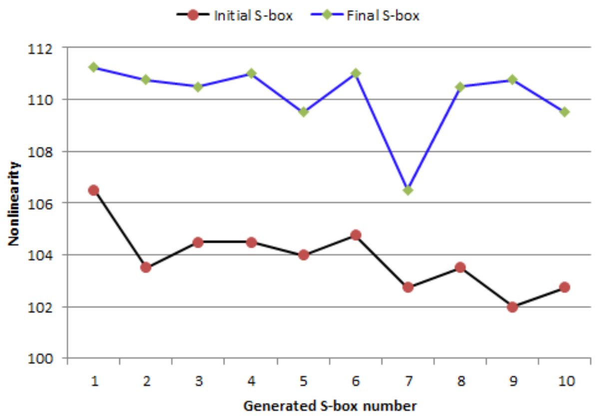

FIGURE 4. Nonlinearity improvisation with heuristic-based optimization approach.

suggested heuristic-based optimization approach is also described through the plot shown in Figure 4. It is visually evident that nonlinearity scores of initial S-boxes get improvised up to a remarkable extent which justifies the consistency of the complete proposed S-box construction scheme.

TABLE 10. NL improvisation of some initial S-boxes using Proposed heuristic-based Optimization Approach.

Values of Parameters			Average NL Score		Difference
A	B	C	Initial S-box	Final S-box	
13	94	63	106.5	111.25	4.8
17	108	131	103.5	110.75	7.3
137	208	51	104.5	110.5	6.0
217	38	171	104.5	111.0	6.5
231	182	91	104.0	109.5	5.5
187	20	249	104.75	111.0	6.2
51	212	179	102.75	106.5	3.7
147	82	239	103.5	110.5	7.0
89	146	169	102.0	110.75	8.8
25	248	213	102.75	109.5	6.7

I. EFFICIENCY ANALYSIS

Several techniques exist to generate 8 × 8 S-boxes having high nonlinearity higher or equal to 110. The main advantage of our proposed scheme is the capability to construct large number of such dynamic and highly nonlinear S-boxes in an efficient way. To observe the efficiency of the projected S-box scheme, we implemented it in Visual C# and executed on a system having an Intel Core i7 CPU (2.2 GHz) and 4GB RAM. The computational efficiency of our projected technique was analyzed for set of S-boxes (i.e. both initial and final ones). The performance erection of S-box has been performed using novel heuristic-based optimization approach to extemporize nonlinearity of initial S-box. Table 11 demonstrates a comparative analysis of computational efficiency in terms of generation time of S-box constructions along with time incurred in recently published articles [62], [63], [72], [73], [75], [76] which have applied some heuristic approaches. Table 11 demonstrates that the computational time of generating our proposed S-box is handsomely inspirational as compared to those of [62], [63], [72], [73], [75], [76] while NL scores of these approaches are nearly equal and quite high.

Although several researchers projected novel techniques to generate S-boxes with nonlinearity scores ∼ 112, such techniques are deficient of one or more security standards like presence of fixed points [30], [70]–[73], non-bijectiveness [74], static heuristic approach [75], high DU value and complicated generation procedure [76], application of static irreducible polynomial [72], [75], etc.

To evaluate the computational efficiency and gain offered by the proposed heuristic approach when an initial S-Box with a certain nonlinearity value is given to it, different

TABLE 11. Generation Time (seconds) of Proposed and Other S-box Techniques.

S-Box Technique	NL	Iterations	Time
[62]	111.8	~ 10^4	307
[63]	111.5	~ 10^4	305
[72]	112	~ 10^3	213
[73]	112	~ $10^{3.93}$	293
[75]	112	~ $10^{4.27}$	367
[76]	112	~ $10^{4.73}$	403
Proposed	111.3	~ 10^3	289

TABLE 12. Time and Number of Iterations for Final S-box with NL >=110.

Initial S-Box Nonlinearity	Number of S-Boxes	Avg. No. of Iterations	Avg. Time (Seconds)
>=100 and <102	3375	~ $10^{3.92}$	303
>=102 and <104	5073	~ $10^{3.85}$	287
>=104 and <106	5907	~ $10^{3.95}$	307
>=106 and <108	2913	~ $10^{3.41}$	291
>=108 and <110	2495	~ $10^{2.95}$	273

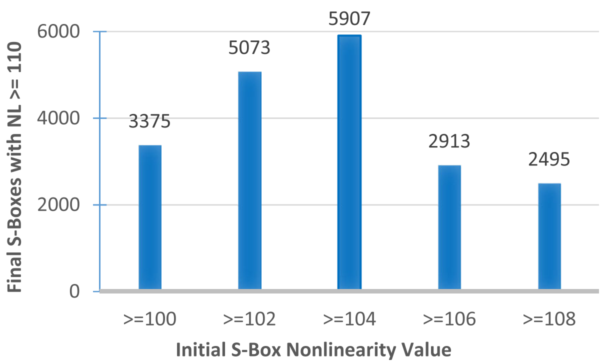

FIGURE 5. Initial S-Box NL and Number of Final S-Boxes with NL >= 110.

20,000 initial S-boxes were generated using Algorithm 1. Nonlinearity values of each initial and final S-Box were noted along with the time (seconds) and the number of iterations taken. Although the nonlinearity of each initial S-Box was improvised by the application of the proposed heuristic evolution approach, we considered only those cases where the nonlinearity value gained by the final S-Box was $>= 110$. Table 12 demonstrates the average time (seconds) and average number of iterations taken for such S-Boxes. Out of 20,000 initial S-Boxes, only 237 S-Boxes (1.19%) could not generate final S-Box with NL $>= 110$.

It can be seen from Table 12 that an initial S-Box with high NL generally takes less time and number of iterations to produce final S-Box with high NL value. Figure 5 shows the relationship between the initial S-Box NL values and the number of final S-Boxes having NL $>= 110$.

Our projected technique for S-box construction employs modest, innovative, and dynamic cubic modular transformation (CMT) which is the first one of its nature, uses cubic trigonometric transform, and a novel dynamic heuristic-based optimization approach. As compared to the weak points present in many techniques in literature, proposed technique offers a freedom to erect dynamic S-boxes with high cryptographic forte and causes an attacker's efforts more ineffective.

IV. CONCLUSION

Several existing techniques generate S-boxes that lack different security standards like presence of fixed points, non-bijectiveness, low score of differential uniformity, etc. Other methods use static transformations, fixed irreducible polynomials, and static heuristic approaches. This research article projected a simple and innovative scheme for the creation of highly nonlinear S-boxes with a novel cubic modular transformation along with the trigonometric Sine function. A pioneering heuristic-based optimization approach, which is dynamic in nature, is suggested that improvises the nonlinearity of the initial S-box. The proposed scheme uses input parameters of integer type in transformation and optimization phases that possesses the potential to spawn a large count of sturdy S-boxes when a minute variation is applied in the parameters' values. Cipher key is used to employ values to the input parameters for the creation of dynamic S-boxes. A specimen S-box is spawned, and its recital has been achieved through standard criteria of S-box evaluation along with the comparative analysis with many existing S-boxes.

ACKNOWLEDGMENT

This research was funded by the Deanship of Scientific Research at Princess Nourah Bint Abdulrahman University through the Fast-track Research Funding Program.

REFERENCES

[1] C. Paar, J. Pelzl, and B. Preneel, *Understanding Cryptography*, 1st ed. Berlin, Germany: Springer, 2010.

[2] A. Kadhim and S. Khalaf, "New approach for security chatting in real time," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 4, no. 3, pp. 30–36, 2015.

[3] M. Ahmad, E. Al Solami, X.-Y. Wang, M. N. Doja, M. M. S. Beg, and A. 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, 2018.

[4] M. M. Lauridsen, C. Rechberger, and L. R. Knudsen, "Design and analysis of symmetric primitive," Tech. Univ. Denmark, Lyngby, Denmark, Tech. Rep. 382, 2016.

[5] A. Belazi, A. A. Abd 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] A. K. Farhan, R. S. Ali, H. Natiq, and N. M. G. Al-Saidi, "A new S-box generation algorithm based on multistability behavior of a plasma perturbation model," *IEEE Access*, vol. 7, pp. 124914–124924, 2019.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] J. Mohaimen Hassan and F. Alaa Kadhim, "New S-box transformation based on chaotic system for image encryption," in *Proc. 3rd Int. Conf. Eng. Technol. Appl. (IICETA)*, Najaf, Iraq, Sep. 2020, pp. 214–219.
[13] C. M. Ou, "Design of block ciphers by simple chaotic functions," *IEEE Comput. Intell. Mag.*, vol. 3, no. 2, pp. 54–59, May 2008.
[14] D. Lambić, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2407–2413, 2017.
[15] A. A. Abd El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, pp. 92–102, Aug. 2019.
[16] A. A. Alzaidi, M. Ahmad, M. N. Doja, E. A. Solami, and M. M. S. Beg, "A new 1D chaotic map and beta-hill climbing for generating substitution-boxes," *IEEE Access*, vol. 6, pp. 55405–55418, 2018.
[17] 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.
[18] 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.
[19] 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.
[20] C.-H. Chen, L.-J. Sheu, H.-K. Chen, J.-H. Chen, H.-C. Wang, Y.-C. Chao, and Y.-K. Lin, "A new hyper-chaotic system and its synchronization," *Nonlinear Anal., Real World Appl.*, vol. 10, no. 4, pp. 2088–2096, Aug. 2009.
[21] J. Ma and Y. Yang, "Hyperchaos numerical simulation and control in a 4D hyperchaotic system," *Discrete Dyn. Nature Soc.*, vol. 2013, pp. 1–16, Oct. 2013.
[22] 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.
[23] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, 2018.
[24] 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, Dec. 2015.
[25] 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.
[26] H. Shaw, "A cryptographic system based upon the principles of gene expression," *Cryptography*, vol. 1, no. 3, p. 21, Nov. 2017.
[27] 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.
[28] 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.
[29] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with DNA binary strands," *Biosystems*, vol. 57, no. 1, pp. 13–22, Jun. 2000.
[30] 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.
[31] 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, Jun. 2016.
[32] 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.
[33] 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.
[34] 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.
[35] A. H. Zahid and M. J. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, 2019.
[36] A. H. Zahid, M. J. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Entropy*, vol. 21, no. 3, p. 245, May 2019.
[37] 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.
[38] 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.
[39] M. S. Mahmood 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.
[40] 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.
[41] 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.
[42] F. Özkaynak, "On the effect of chaotic system in performance characteristics of chaos based S-box designs," *Phys. A, Stat. Mech. Appl.*, vol. 550, Jul. 2020, Art. no. 124072.
[43] 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, 2017.
[44] 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.
[45] Y. Wang, K.-W. Wong, C. Li, and L. Yang, "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, 2012.
[46] 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.
[47] 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.
[48] 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, 2016.
[49] 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.
[50] 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.*, Dec. 2009, pp. 463–467.
[51] 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.
[52] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. Amsterdam, The Netherlands: Elsevier, 2009.

[53] 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.
[54] 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.
[55] 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.
[56] 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.
[57] 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.
[58] M. 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, pp. 3041–3064, Dec. 2019.
[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] 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.
[61] 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.
[62] A. H. Zahid, A. M. Iliyasu, M. Ahmad, M. M. U. Shaban, M. J. Arshad, H. S. Alhadawi, and A. El-Latif, "A novel construction of dynamic S-box with high nonlinearity using heuristic evolution," *IEEE Access*, vol. 9, pp. 67797–67812, 2021, doi: 10.1109/ACCESS.2021.3077194.
[63] A. H. Zahid, H. Rashid, M. M. U. Shaban, and S. Ahmad, "Dynamic S-box design using a novel square polynomial transformation and permutation," *IEEE Access*, vol. 8, pp. 82390–82401, 2021, doi: 10.1109/ACCESS.2021.3086717.
[64] Y. Wang, Z. Zhang, L. Y. Zhang, J. Feng, J. Gao, and P. Lei, "A genetic algorithm for constructing bijective substitution boxes with high nonlinearity," *Inf. Sci.*, vol. 523, pp. 152–166, Jan. 2020.
[65] A. H. Zahid, L. Tawalbeh, M. Ahmad, A. Alkhayyat, M. T. Hassan, A. Manzoor, and A. K. Farhan, "Efficient dynamic S-box generation using linear trigonometric transformation for security applications," *IEEE Access*, vol. 9, pp. 98460–98475, 2021.
[66] 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, pp. 523–534.
[67] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Adv. Cryptol.*, Lofthus, Norway, 1994, pp. 386–397.
[68] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, 1991.
[69] 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.
[70] K. E. 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, 2018.
[71] 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.
[72] 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, p. 6, 2020.
[73] 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, 2020, Art. no. e0241890.
[74] 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, Apr. 2018, Art. no. 582323.
[75] 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.
[76] 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.

AMJAD HUSSAIN ZAHID received the Ph.D. degree in computer science (information security) from the University of Engineering and Technology, Lahore. He is currently working as an Assistant Professor with the University of Management and Technology (UMT), Lahore, Pakistan. He is also the Program Advisor for BS (IT) Program and a member of many academic bodies. He has been an Active Member of the Higher Education Commission (HEC) National Curriculum Revision Committee (NCRC), Pakistan. 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, blockchain, and so on. He has been 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 the Faculty Board of Studies, Punjab University College of Information Technology (PUCIT) and the Virtual University of Pakistan.

MUSHEER AHMAD received the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively, and the Ph.D. degree in chaos-based cryptography from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India. From 2007 to 2010, he worked with the Department of Computer Engineering, Aligarh Muslim University. Since 2011, he has been working as an Assistant Professor with the Department of Computer Engineering, Jamia Millia Islamia. He has published over 85 research papers in international reputed refereed journals and conference proceedings of the IEEE/Springer/Elsevier. He has more than 1600 citations of his research works with an H-index of 23. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, authentication, machine learning for security, and optimization techniques. He has served as a reviewer and a technical program committee member of many international conferences. He has also served as a referee of some renowned journals, such as *Information Sciences*, *Signal Processing*, *Journal of Information Security and Applications*, IEEE Journal of Selected Areas in Communications, IEEE Transactions on Circuits and Systems for Video Technology, IEEE Transactions on Industrial Informatics, IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE Transactions on Neural Networks and Learning Systems, IEEE Transactions on NanoBioscience, IEEE Multimedia, IEEE Access, *Wireless Personal Communications*, *Neural Computing and Applications*, *International Journal of Bifurcation and Chaos*, *Chaos Solitons & Fractals*, *Physica A*, *Signal Processing: Image Communication*, *Neurocomputing*, *IET Information Security*, *IET Image Processing*, *Security and Communication Networks*, *Optik*, *Optics and Laser Technology*, *Complexity*, *Computers in Biology and Medicine*, *Computational and Applied Mathematics*, *Concurrency and Computation*, and so on.

AHMED ALKHAYYAT received the B.Sc. degree in electrical engineering from AL KUFA University, Najaf, Iraq, in 2007, the M.Sc. degree from the Dehradun Institute of Technology, Dehradun, India, in 2010, and the Ph.D. degree from Cankaya University, Ankara, Turkey, in 2015. He is currently the Dean of International Relationship and Manager of the word ranking in the Islamic University, Najaf, Iraq. His research interests include the IoT in the health-care system, SDN, network coding, cognitive radio, efficient-energy routing algorithms, and efficient-energy MAC protocol in cooperative wireless networks and wireless body area networks, and cross-layer designing for self-organized networks. He contributed in organizing a several IEEE conferences, workshop, and special sessions. He served as a reviewer for several journals and conferences.

MUHAMMAD JUNAID ARSHAD is currently working as an Associate Professor with the University of Engineering and Technology (UET), Lahore. He is also a 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. He has supervised more than 50 BS Research Projects, 60 M.Sc./M. Phil theses, and currently 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 modeling, information security, cloud computing, and so on. He is a member of the IEEE Computer Society and the IEEE Communications Society Korea Information and Communications Society (KICS). He is serving as an editor/reviewer in many reputed International Research Journals. He is an Advisor of the Punjab Public Service Commission and the Federal Public Service Commission.

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, blockchain, and so on.

NAGLAA F. SOLIMAN received the B.Sc., M.Sc., and Ph.D. degrees from the Faculty of Engineering, Zagazig University, Egypt, in 1999, 2004, and 2011, respectively. She has been with the Faculty of Computer Science, Princess Nourah Bint Abdulrahman University, Saudi Arabia, since 2015. She has been a Teaching Staff Member with the Department of Electronics and Communications Engineering, Faculty of Engineering, Zagazig University. Her current research interests include digital image processing, information security, multimedia communications, medical image processing, optical signal processing, big data, and cloud computing.

ABEER D. ALGARNI received the B.Sc. degree (Hons.) in computer science from King Saud University, Riyadh, Saudi Arabia, in 2007, and the M.Sc. and Ph.D. degrees from the School of Engineering and Computer Sciences, Durham University, U.K., in 2010 and 2015, respectively. She has been an Assistant Professor with the College of Computer and Information Sciences, Princess Nourah Bent Abdulrahman University, since 2008. Her current research interests include networking and communication systems, digital image processing, digital communications, and cyber security.