Hindawi
Security and Communication Networks
Volume 2020, Article ID 8883884, 14 pages
https://doi.org/10.1155/2020/8883884

Research Article

The Effect of the Primitive Irreducible Polynomial on the Quality of Cryptographic Properties of Block Ciphers

Sajjad Shaukat Jamal,[1] **Dawood Shah**,[2] **Abdulaziz Deajim**,[1] **and Tariq Shah**[2]

[1]*Department of Mathematics, College of Science, King Khalid University, P. O. Box 9004, Abha, Saudi Arabia*
[2]*Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan*

Correspondence should be addressed to Sajjad Shaukat Jamal; shussain@kku.edu.sa

Received 23 May 2020; Revised 3 August 2020; Accepted 28 August 2020; Published 24 September 2020

Academic Editor: Tom Chen

Substitution boxes are the only nonlinear component of the symmetric key cryptography and play a key role in the cryptosystem. In block ciphers, the S-boxes create confusion and add valuable strength. The majority of the substitution boxes algorithms focus on bijective Boolean functions and primitive irreducible polynomial that generates the Galois field. For binary field F2, there are exactly 16 primitive irreducible polynomials of degree 8 and it prompts us to construct 16 Galois field extensions of order 256. Conventionally, construction of affine power affine S-box is based on Galois field of order 256, depending on a single degree 8 primitive irreducible polynomial over $\mathbb{Z}_2$. In this manuscript, we study affine power affine S-boxes for all the 16 distinct degree 8 primitive irreducible polynomials over $\mathbb{Z}_2$ to propose 16 different 8×8 substitution boxes. To perform this idea, we introduce 16 affine power affine transformations and, for fixed parameters, we obtained 16 distinct S-boxes. Here, we thoroughly study S-boxes with all possible primitive irreducible polynomials and their algebraic properties. All of these boxes are evaluated with the help of nonlinearity test, strict avalanche criterion, bit independent criterion, and linear and differential approximation probability analyses to measure the algebraic and statistical strength of the proposed substitution boxes. Majority logic criterion results indicate that the proposed substitution boxes are well suited for the techniques of secure communication.

1. Introduction

The exchange of digital data through the Internet has revolutionized the communication parameters over the years. But this rapid communication also provides opportunities to access this digital data illegally. For this reason, the security of this content on the Internet has become a serious challenge for the researchers of different fields. To counter the emerging challenges of security, cryptography and steganography are used to hide the secret information whereas watermarking is used for copyright protection. In this manuscript, we discuss cryptography and relevant aspects of this field. For convenience, cryptography is divided into two types named symmetric key cryptography and asymmetric key cryptography. In symmetric key cryptography, two parties share secret information and keys during encryption and decryption procedures. The private key is shared by both sender and receiver. In addition to this, block ciphers and stream ciphers are two main branches of symmetric key cryptography. In 1949, Shannon gave the idea of block cipher and some examples of block ciphers are Advanced Encryption Standard (AES) [1], Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and many more [2, 3]. In AES, there is availability of three different key sizes such as 128, 192, and 256 bits, whereas in DES, the only available key size is 56 bits. The AES has 10, 12, and 14 rounds for key sizes of 128, 192, and 256 bits, respectively. All these rounds have four basic steps, that is, subbyte, shift row, mix column, and add round key. Subbyte is the step which substitutes the plaintext data with substitution box (S-box). This S-box is the only nonlinear part of block cipher used in different well-known cryptosystems. It is used to create confusion to make plaintext data obscure for any attacker and hence S-box is an integral part of any cryptosystem. S-box is a function which has input and output from the Galois field. The Galois field is a finite field having order 256 and denoted by $GF(2^8)$.

1.1. Related Work. S-box is used to create confusion as observed in AES, International Data Encryption Algorithm (IDEA), DES, and many more cryptosystems [4]. It is an established fact that the strength of block cipher depends on the standard and quality of S-box. Due to the necessary immersion of S-box to generate nonlinearity, intricacy persuades different researchers to design strong S-boxes to enhance the security level of cryptosystems. Among different available methods, the algebraic structure-based construction of S-boxes has much more attention. These S-boxes have strong cryptographic features and are robust against linear and differential cryptanalysis.

In the literature, different structural advancements are viewed to improve the quality of S-boxes. The algebraic complexity of AES S-box has been improved with the extension of this S-box, that is, affine power affine (APA) [5]. Furthermore, the symmetric group S_8 has also been applied to AES S-box to improve the quality and numbers of S-boxes [6]. Similarly, the application of transformation using binary gray codes on AES S-box gives Gray S-box [7]. In [8], S-boxes are constructed by using the projective general linear group (PGL). Moreover, the construction scheme of chaotic S-boxes using DNA sequence and chaotic Chen system is given in [9, 10]. Different analytical, algebraic, and chaos-based techniques for the construction of S-boxes are given in [11–16]. Conventionally, AES uses a polynomial of 8 terms which have all the required properties and improves the security for AES. But the Gray S-box has a 255-term polynomial. Moreover, residue prime, Xyi, and Skipjack S-boxes are frequently used for the encryption and decryption schemes [17, 18].

It is assumed that the model of Boolean functions and primitive irreducible polynomial has an impact on the strength of S-box. In [19], different primitive irreducible polynomials have been used to identify the effect of primitive irreducible polynomial. To investigate this fact, we want to study all the primitive irreducible polynomials to understand whether there is an impact of irreducible polynomial or not. Archetypally in the synthesis of an S-box, the numbers a, b, c, and d in affine transformation belong to Galois field $\mathrm{GF}(2^8)$. As the polynomial ring $\mathbb{Z}_2[x]$ has 16 primitive irreducible polynomials of degree 8, it shows that only 16 opportunities are available for constructing Galois fields $\mathrm{GF}(2^8)$. In this paper, we have constructed 16 different robust 8×8 S-boxes over the elements of these 16 irreducible polynomials. Firstly, we define 16 affine power affine transformations on these different Galois fields which can be given as $z \longrightarrow (az + b)o(cz + d)^{-1}$; here, for a, b, c, d values, we would be able to get 16 distinct S-boxes.

1.2. Motivation. Due to the role of S-boxes in cryptosystems, it is essential to explore all of its aspects. The motivation behind this work is to study all primitive irreducible polynomials and their role in the construction of S-boxes.

(1) The Mobius transformation used in a different construction of S-boxes has certain limitations and restrictions in its structure [7]. For example, the condition on the parameters, i.e., $a\,d - bc \neq 0$ $\forall a, b, c, d \in \mathrm{GF}(2^8)$ squeezes the remaining cases. Hence, there is a need for any other transformation.

(2) There are 16 primitive irreducible polynomials in the principal ideal domain $\mathbb{Z}_2[x]$ whose impact was not studied yet regarding their impression on analyses of S-boxes.

(3) By exploring all primitive irreducible polynomials, we have a better opportunity to obtain the cryptographically strong cryptosystems.

1.3. Our Contribution. In this manuscript, we studied all binary degree 8 primitive irreducible polynomials for the construction of S-boxes. The quality of the proposed work can be seen from the different security analyses and resistance against malicious attacks. This whole study can be summarized as follows:

(1) We constructed S-boxes associated with the 16 binary degree 8 primitive irreducible polynomials.

(2) The APA transformation is used in this work, which is bijective and has no restrictions on the parameters.

(3) To evaluate the strength of the proposed S-boxes, we have performed different analyses along with differential cryptanalysis. The outcomes of these analyses are compared with the well-known S-boxes.

The remaining part of the paper is planned as follows: Section 2 presents the preliminaries and construction scheme of the proposed S-boxes. In Section 3, algebraic and statistical analyses are calculated in detail. Section 4 presents definitions of the balanced Boolean function. Section 5 concludes the paper.

2. Primitive Irreducible Polynomials of Degree 8 and GF (2^8)

2.1. The Galois Fields $GF(2^8)$. We summarize here some well-known facts from the theory of rings and fields. Let R be a commutative ring with identity. A nonempty subset J of R is called an *ideal* of R if J is an additive subgroup of R and $aJ \subseteq J$ for every $a \in R$, where $aJ = \{aj \mid j \in J\}$. If, furthermore, there does not exist a proper ideal of R properly containing J, then we say that J is a *maximal* ideal of R Besides; R is said to be a *field* if each of its nonzero elements has a must inverse in R. If R is a field of prime characteristic p, then R is an extension of the prime field $\mathbb{Z}_p$. A polynomial $f(x) \in \mathbb{Z}_p[x]$ is said to be irreducible if it cannot be factored in $\mathbb{Z}_p[x]$ into two polynomials of strictly smaller degrees. The principal ideal,

$$\langle f(x) \rangle = \{h(x) f(x) \colon h(x) \in \mathbb{Z}_p[x]\}, \tag{1}$$

generated by a monic irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ is a maximal ideal in $\mathbb{Z}_p[x]$. If $f(x)$ is of degree m, then the quotient ring,

$$\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle} = \left\{g(x) + \langle f(x)\rangle \colon g(x) \in \mathbb{Z}_p[x]\right\}, \quad (2)$$

is an extension field of $\mathbb{Z}_p$ of degree m consisting of p^m elements. This field is called a *Galois field* and is denoted by $\mathrm{GF}(p^m)$ and is said to be the field extension of $\mathbb{Z}_p$ defined by the irreducible polynomial $f(x)$. A representative $g(x)$ of each element of $\mathrm{GF}(p^m)$ can be chosen to be of degree strictly less than m. If α is a root of $f(x)$ in an algebraic closure of $\mathbb{Z}_p$, then $\mathrm{GF}(p^m)$ is isomorphic to the field:

$$\mathbb{Z}_p(\alpha) = \left\{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \colon a_i \in \mathbb{Z}_p, \forall i\right\}, \quad (3)$$

and so we can identify the two fields. Furthermore, if α is a generator of the cyclic finite multiplicative group of nonzero elements of $\mathbb{Z}_p(\alpha)$, then we say that $f(x)$ is *primitive*.

The Galois field $\mathrm{GF}(2^8)$ is particularly of specific interest in cryptographic applications, especially in S-boxes constructions. For our cryptographic purposes, we are interested in such a field whose defining irreducible polynomial is "primitive" (of degree 8, of course). It is well known that there are $(\varphi(2^8 - 1)/8) = 16$ such polynomials over $\mathbb{Z}_2$, for example, $p_1(x), \ldots, p_{16}(x) \in \mathbb{Z}_2[x]$, which we list in Table 1. In the following section, we construct 16 S-boxes out of the Galois fields corresponding to the aforementioned sixteen primitive irreducible polynomials.

2.2. The Proposed S-Box Construction Method. For each $i = 1, \ldots, 16$, consider the affine power affine map (APA):

$$S = A_1 \circ f \circ A_2 \colon \mathbb{Z}_2(\alpha_i) \longrightarrow \mathbb{Z}_2(\alpha_i), \quad (4)$$

where $A_1(x) = ax + b$ and $A_2(x) = cx + d$ $(a, b, c, d \in \mathbb{Z}_2(\alpha_i))$ are two affine maps with $a, c \neq 0$, and

$$f(x) = \begin{cases} x^{-1}, & \text{if } x \neq 0, \\ 0, & \text{if } x = 0. \end{cases} \quad (5)$$

Among other things, the map S, which is obviously bijective, was introduced by [5] to produce confusion in the scheme. For our S-boxes, we choose $a = 13$, $b = 14$ and $c = 102$ and $d = 210$. Figure 1 demonstrates the flow chart of the construction of the 16 different S-boxes. Moreover, the construction of S-boxes in correspondence to polynomial 1 (P_1) to polynomial 16 (P_{16}) is shown in Figure 1**.** All the S-boxes are given in Tables 2–17, corresponding to P_1 to P_{16}. These tables are before the conclusion section.

In the proposed work, we present an APA S-box corresponding to each $i = 1, \ldots, 16$ where the APA map S gives the 16×16 lookup tables. We, then, show that these S-boxes have strong cryptographic properties certified with the help of analyses such as nonlinearity, strict avalanche criterion (SAC), bit independent criterion (BIC), linear approximation probability (LP), and differential approximation probability (DP) [20].

Table 1: Primitive irreducible polynomials and their corresponding Galois fields.

Primitive polynomials $p_i(x)$& roots α_i	Galois field $\mathrm{GF}(2^8)$
$p_1(x) = x^8 + x^4 + x^3 + x^2 + 1; \alpha_1$	$\mathbb{Z}_2[x]/\langle p_1(x)\rangle$
$p_2(x) = x^8 + x^5 + x^3 + x + 1; \alpha_2$	$\mathbb{Z}_2[x]/\langle p_2(x)\rangle$
$p_3(x) = x^8 + x^5 + x^3 + x^2 + 1; \alpha_3$	$\mathbb{Z}_2[x]/\langle p_3(x)\rangle$
$p_4(x) = x^8 + x^6 + x^3 + x^2 + 1; \alpha_4$	$\mathbb{Z}_2[x]/\langle p_4(x)\rangle$
$p_5(x) = x^8 + x^6 + x^4 + x^3 + x^2 + x + 1; \alpha_5$	$\mathbb{Z}_2[x]/\langle p_5(x)\rangle$
$p_6(x) = x^8 + x^6 + x^5 + x + 1; \alpha_6$	$\mathbb{Z}_2[x]/\langle p_6(x)\rangle$
$p_7(x) = x^8 + x^6 + x^5 + x^2 + 1; \alpha_7$	$\mathbb{Z}_2[x]/\langle p_7(x)\rangle$
$p_8(x) = x^8 + x^6 + x^5 + x^3 + 1; \alpha_8$	$\mathbb{Z}_2[x]/\langle p_8(x)\rangle$
$p_9(x) = x^8 + x^7 + x^3 + x^2 + 1; \alpha_9$	$\mathbb{Z}_2[x]/\langle p_9(x)\rangle$
$p_{10}(x) = x^8 + x^7 + x^5 + x^3 + 1; \alpha_{10}$	$\mathbb{Z}_2[x]/\langle p_{10}(x)\rangle$
$p_{11}(x) = x^8 + x^7 + x^2 + x + 1; \alpha_{11}$	$\mathbb{Z}_2[x]/\langle p_{11}(x)\rangle$
$p_{12}(x) = x^8 + x^7 + x^6 + x + 1; \alpha_{12}$	$\mathbb{Z}_2[x]/\langle p_{12}(x)\rangle$
$p_{13}(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1; \alpha_{13}$	$\mathbb{Z}_2[x]/\langle p_{13}(x)\rangle$
$p_{14}(x) = x^8 + x^7 + x^6 + x^3 + x^2 + x + 1; \alpha_{14}$	$\mathbb{Z}_2[x]/\langle p_{14}(x)\rangle$
$p_{15}(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1; \alpha_{15}$	$\mathbb{Z}_2[x]/\langle p_{15}(x)\rangle$
$p_{16}(x) = x^8 + x^6 + x^5 + x^4 + 1; \alpha_{16}$	$\mathbb{Z}_2[x]/\langle p_{16}(x)\rangle$

3. Security Analysis

In this section, we present some algebraic and statistical analyses of S-box followed [21]. Such analyses indicate the strength of all the proposed S-boxes and give an idea for their application in image encryption and other modes of secure communication.

3.1. Nonlinearity. Nonlinearity analysis of a function f is the minimum hamming distance between the Boolean function $f : f \colon \{0,1\}^n \longrightarrow \{0,1\}$ and its all n-bit affine functions. In the truth table of Boolean function f, the nonlinearity of f represents the degree of dissimilarity between f and all affine function. If the function has high minimum hamming distance, it indicates it has high nonlinearity. It is an established fact that high nonlinearity provides resistance to any kind of linear approximation attacks [22, 23]. The calculated upper bound of nonlinearity is $M = 2^{m-1} - 2^{((m/2)-1)}$ so that, for $m = 8$, the optimal value of nonlinearity is 120. Table 18 shows the nonlinearity of 16 S-boxes corresponding to all primitive irreducible polynomials. From this table, it can be seen that the value of nonlinearity has not been affected due to background irreducible polynomial.

3.2. Strict Avalanche Criteria. In [24], Webster and Tavares introduced the strict avalanche criteria (SAC) on the concepts of completeness and avalanche. If a single input bit changes, the output bits change with almost 0.5 probability. It helps to show that the resulting output vector is highly random, and no single pattern can be predictable by minor variation in the input vector [25]. By seeing the performance indexes of S-boxes, the proposed S-boxes successfully satisfy SAC. Table 19 depicts the value of SAC for all the proposed 16 S-boxes. It shows that the maximum value of SAC is 0.562500 for the first 9 S-boxes including 11^{th}, 14^{th}, and 16^{th} S-boxes. Similarly,

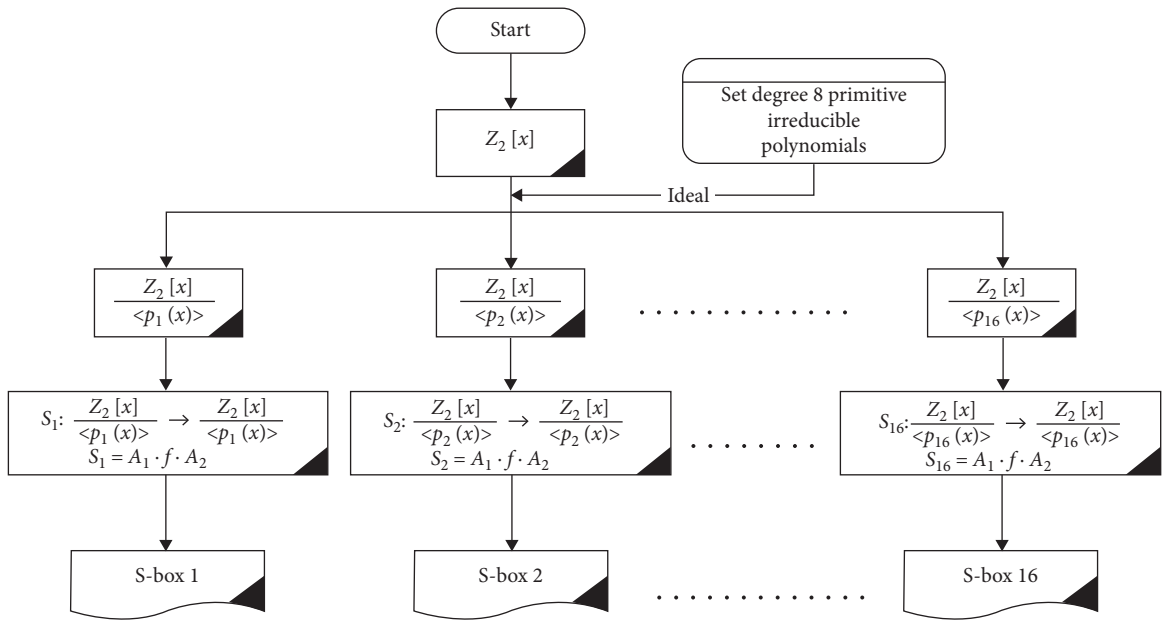

Figure 1: Flow chart for the construction of the proposed S-boxes and S-boxes corresponding to P_1 and P_{16}.

Table 2: S-box corresponding to P2.

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

Table 3: S-box corresponding to P2.

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

Table 4: S-box corresponding to P3.

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

Table 5: S-box corresponding to P4.

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

Table 6: S-box corresponding to P5.

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

Table 7: S-box corresponding to P6.

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

Table 8: S-box corresponding to P7.

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

Table 9: S-box corresponding to P8.

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

Table 10: S-box corresponding to P9.

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

Table 11: S-box corresponding to P10.

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

Table 12: S-box corresponding to P11.

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

Table 13: S-box corresponding to P12.

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

Table 14: S-box corresponding to P13.

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

Table 15: S-box corresponding to P14.

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

Table 16: S-box corresponding to P15.

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

Table 17: S-box corresponding to P15.

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

Table 18: Nonlinearity of the proposed S-box.

S-boxes	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	Average
S-box 1	112	112	112	112	112	112	112	112	112
S-box 2	112	112	112	112	112	112	112	112	112
S-box 3	112	112	112	112	112	112	112	112	112
S-box 4	112	112	112	112	112	112	112	112	112
S-box 5	112	112	112	112	112	112	112	112	112
S-box 6	112	112	112	112	112	112	112	112	112
S-box 7	112	112	112	112	112	112	112	112	112
S-box 8	112	112	112	112	112	112	112	112	112
S-box 9	112	112	112	112	112	112	112	112	112
S-box 10	112	112	112	112	112	112	112	112	112
S-box 11	112	112	112	112	112	112	112	112	112
S-box 12	112	112	112	112	112	112	112	112	112
S-box 13	112	112	112	112	112	112	112	112	112
S-box 14	112	112	112	112	112	112	112	112	112
S-box 15	112	112	112	112	112	112	112	112	112
S-box 16	112	112	112	112	112	112	112	112	112

Table 19: Strict avalanche criterion.

S-box	Max	Min	Average	Square deviation
S-box 1	0.562500	0.437500	0.496094	0.0172495
S-box 2	0.546875	0.453125	0.495117	0.0128725
S-box 3	0.562500	0.453125	0.494141	0.0152856
S-box 4	0.562500	0.453125	0.50708	0.0118748
S-box 5	0.546875	0.453125	0.503174	0.0153901
S-box 6	0.562500	0.453125	0.501709	0.016637
S-box 7	0.562500	0.453125	0.502441	0.0170951
S-box 8	0.562500	0.453125	0.503906	0.0165152
S-box 9	0.562500	0.453125	0.485596	0.0153978
S-box 10	0.546875	0.453125	0.509766	0.0123912
S-box 11	0.562500	0.4375	0.50415	0.0191487
S-box 12	0.5625	0.453125	0.501221	0.016475
S-box 13	0.546875	0.4375	0.500977	0.0127235
S-box 14	0.5625	0.453125	0.508301	0.0158654
S-box 15	0.546875	0.437500	0.498779	0.0143727
S-box 16	0.5625	0.437500	0.496582	0.0143171

Table 20: Bit independent criterion.

	BIC-SAC			BIC		
S-box	Min	Average	Square deviation	Max	Average	Square deviation
S-box 1	0.47461	0.50119	0.01132	112	112	0
S-box 2	0.49219	0.50600	0.00845	112	112	0
S-box 3	0.48047	0.50202	0.01015	112	112	0
S-box 4	0.47852	0.50656	0.01201	112	112	0
S-box 5	0.48438	0.50105	0.00924	112	112	0
S-box 6	0.47656	0.49819	0.00784	112	112	0
S-box 7	0.48633	0.50593	0.00925	112	112	0
S-box 8	0.48828	0.50251	0.00835	112	112	0
S-box 9	0.48828	0.50258	0.00644	112	112	0
S-box 10	0.48438	0.50739	0.00981	112	112	0
S-box 11	0.47656	0.49784	0.00950	112	112	0
S-box 12	0.47070	0.49679	0.01026	112	112	0
S-box 13	0.48242	0.50021	0.01085	112	112	0
S-box 14	0.49023	0.50718	0.00901	112	112	0
S-box 15	0.48438	0.50265	0.00883	112	112	0
S-box 16	0.48633	0.50544	0.00861	112	112	0

Table 21: Linear and differential approximation probability analysis.

S-box	Linear approximation probability		Differential approximation probability	
	Max count	LP	Max value	DP
S-box 1	144	0.0625	4	0.015625
S-box 1	144	0.0625	4	0.015625
S-box 2	144	0.0625	4	0.015625
S-box 3	144	0.0625	4	0.015625
S-box 4	144	0.0625	4	0.015625
S-box 5	144	0.0625	4	0.015625
S-box 6	144	0.0625	4	0.015625
S-box 7	145	0.0664	4	0.015625
S-box 8	144	0.0625	4	0.015625
S-box 9	144	0.0625	4	0.015625
S-box 10	144	0.0625	4	0.015625
S-box 11	144	0.0625	4	0.015625
S-box 12	144	0.0625	4	0.015625
S-box 13	144	0.0625	4	0.015625
S-box 14	144	0.0625	4	0.015625
S-box 15	144	0.0625	4	0.015625
S-box 16	144	0.0625	4	0.015625

Table 22: Comparison of the performance indexes of the proposed S-boxes with some standard S-boxes.

8×8 S-boxes	Nonlinearity	SAC	BIC	BIC-SAC	DP	LP
AES S-box	112	0.5058	112	0.504	0.0156	0.062
APA S-box	112	0.4987	112	0.499	0.0156	0.062
Gray S-box	112	0.5058	112	0.502	0.0156	0.062
Skipjack S-box	105.7	0.4980	104.1	0.499	0.0468	0.109
Xyi S-box	105	0.5048	103.7	0.503	0.0468	0.156
Residue prime	99.5	0.5012	101.7	0.502	0.2810	0.132
Reference [27]	106	0.4978	103.92	—	—	—
Reference [28]		0.505	—	—	—	—
Reference [29]	104	0.5241	103	0.50181	0.1625	0.0486
S-box 1	112	0.496094	112	0.50119	0.015625	0.0625
S-box 2	112	0.495117	112	0.50600	0.015625	0.0625
S-box 3	112	0.494141	112	0.50202	0.015625	0.0625
S-box 4	112	0.50708	112	0.50656	0.015625	0.0625
S-box 5	112	0.503174	112	0.50105	0.015625	0.0625
S-box 6	112	0.501709	112	0.49819	0.015625	0.0625
S-box 7	112	0.502441	112	0.50593	0.015625	0.0625
S-box 8	112	0.503906	112	0.50251	0.015625	0.0664
S-box 9	112	0.485596	112	0.50258	0.015625	0.0625
S-box 10	112	0.509766	112	0.50739	0.015625	0.0625
S-box 11	112	0.50415	112	0.49784	0.015625	0.0625
S-box 12	112	0.501221	112	0.49679	0.015625	0.0625
S-box 13	112	0.500977	112	0.50021	0.015625	0.0625
S-box 14	112	0.508301	112	0.50718	0.015625	0.0625
S-box 15	112	0.498779	112	0.50265	0.015625	0.0625
S-box 16	112	0.496582	112	0.50544	0.015625	0.0625

Table 23: MLC analyses for the proposed S-boxes.

S-boxes	Entropy	Correlation	Contrast	Energy	Homogeneity
S-box 1	7.2763	0.1032	8.8505	0.0175	0.4499
S-box 2	7.2763	0.1246	9.1517	0.0174	0.4530
S-box 3	7.2763	0.0895	9.5748	0.0175	0.4532
S-box 4	7.2763	0.1486	8.9132	0.0184	0.4579
S-box 5	7.2763	0.1277	9.2077	0.0195	0.4714
S-box 6	7.2763	0.1326	9.8130	0.0178	0.4532
S-box 7	7.2642	0.0904	10.0599	0.0177	0.4438
S-box 8	7.2763	0.1256	9.6635	0.0182	0.4509
S-box 9	7.2763	0.1099	8.9653	0.0179	0.4609
S-box 10	7.2763	0.0747	9.7106	0.0177	0.4453
S-box 11	7.2763	0.0927	9.7905	0.0182	0.4529
S-box 12	7.2763	0.0879	9.8720	0.0182	0.4531
S-box 13	7.2763	0.0868	8.5569	0.0188	0.4606
S-box 14	7.2763	0.0862	8.6308	0.0179	0.4510
S-box 15	7.2763	0.1245	9.3829	0.0184	0.4522
S-box 16	7.2763	0.0843	9.5898	0.0179	0.4533

the minimum value of SAC is 0.453125 for the first 10 S-boxes including 12^{th} and 14^{th} S-boxes. The average value of SAC lies in the interval [0.4856, 0.509766].

3.3. Bit Independent Criterion. Another algebraic criterion (BIC) is used to evaluate the strength of S-box, which is presented by Detombe and Tavares in [26]. In Table 14, the outcomes of BIC to SAC and BIC for the proposed S-boxes are given. The minimum BIC to SAC value is 0.47070 for 12^{th} S-box and the highest minimum value is 0.49219 for 2^{nd} S-box. The average BIC to SAC lies between 0.49679 and 0.50739. Similarly, the square deviation values for all the proposed S-boxes are given in Table 20. The maximum and average value of BIC is 112 for all S-boxes. It is depicted that the proposed S-boxes give the nearest best value of BIC analyses.

3.4. Linear Approximation Probability. Matsui defines the extreme value of the imbalance of an event as the linear approximation probability. It is notable that the parity of the input bits that is, the mask G_l, is equal to the parity of the output bits, i.e., the mask G_m. The linear approximation probability of a given S-box is defined in the following equation:

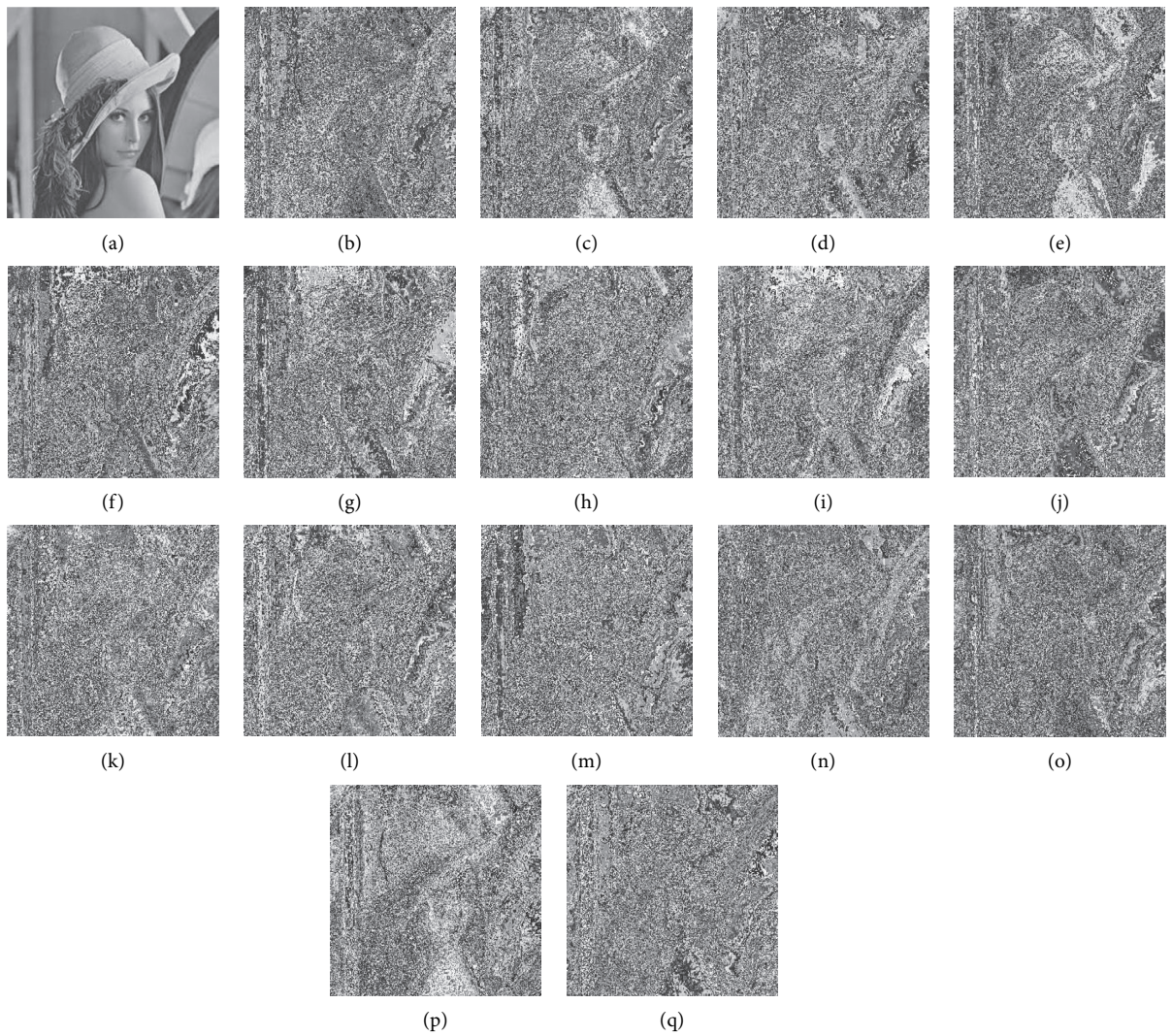

FIGURE 2: Original Lena image and the encrypted images using all 16 primitive irreducible polynomials S-boxes. (a) Lena image, (b) S-box 1, (c) S-box 2, (d) S-box 3, (e) S-box 4, (f) S-box 5, (g) S-box 6, (h) S-box 7, (i) S-box 8, (j) S-box 9, (k) S-box 10, (l) S-box 11, (m) S-box 12, (n) S-box 13, (o) S-box 14, (p) S-box 15, and (q) S-box 16.

$$\mathrm{LP} = \max_{G_l, G_m \neq 0} \left| \frac{\#\{l \in X \mid l \cdot G_l = S(l) \cdot G_m\}}{2^n} - \frac{1}{2} \right|, \tag{6}$$

where G_l and G_m are input and output masks, respectively, and the set "X" represents the set of all possible inputs; 2^n is the number of elements of X. The value of linear approximation indicates the strength of S-box against various linear attacks. In Table 21, the maximum count and the LP value for all proposed S-boxes is 144 and 0.0625. These values of LP of the proposed S-boxes are appropriate against linear attacks.

3.5. Differential Approximation Probability. The degree of differential uniformity is known as differential approximation probability (DP^s) of S-box. Mathematically, it can be given as

$$\mathrm{DP}^s(\Delta l \longrightarrow \Delta m) = \left[\frac{\#\{l \in X \mid S(l) \pm S(l \pm \Delta l) = \Delta m\}}{2^m} \right]. \tag{7}$$

Briefly, it can be explained as follows: an input differential Δl_i must be mapped to an output differential Δm_i uniquely for each i. Here, X represents all the possible input values and the number of its elements is given by 2^m. Table 21 depicts the results of DP, which include the maximum and DP value.

Moreover, Table 22 represents the values of proposed S-boxes along with AES, Skipjack, Xyi, APA, Gray, and residue prime S-boxes.

3.6. Statistical Analyses. To evaluate the visual strength of the substitution with the help of the proposed S-boxes, various statistical analyses are made on the host

and substituted images. In this proposed work, statistical analyses like homogeneity, entropy, contrast, energy, and correlation are used to evaluate the substitution ability of the 16 proposed S-boxes. These analyses are given as

$$\text{correlation} = \sum_{k,l} \frac{(k-\mu k)(l-\mu l)}{\sigma_k \sigma_l} p(k,l), \tag{8}$$

$$\text{contrast} = \sum_{k,l} |k-l|^2 p(k,l), \tag{9}$$

$$\text{entropy} = -\sum_{k,l} \text{pr}(p(k,l)) \log \Pr(p(k,l)), \tag{10}$$

$$\text{homogeneity} = \sum_{k,l} \frac{p(k,l)}{1+|k-l|}, \tag{11}$$

$$\text{energy} = -\sum_{k,l} p(k,l)^2, \tag{12}$$

where k, l give the row and column locations of an image. The pixel value at k^{th} row and l^{th} column is represented by $p(k, l)$ and $\Pr(p(k,l))$ is the probability of the image pixel. In equation (8), μ and σ are mean and standard deviation, respectively.

Correlation analysis helps to find the similarity between the host and substituted image. The correlation analysis provides the range which indicates the perfect, negative, and positive correlation. This is $[-1, 1]$ interval for correlation and value of 1 indicates the perfect correlation.

The randomness of the digital image can be calculated with the help of entropy. The higher value of entropy from the interval $[0, 8]$ represents the higher amount of randomness in a digital image. For any viewer, it is only possible with the help of contrast analysis to intensely recognize the objects in the texture of an image. With the help of contrast analyses, one can observe the maximum distinction in image pixels. The range of the contrast can be given by $[(\text{size}(\text{Image}) - 1)^2]$. For constant image, the value of contrast is zero. The goal of finding close distribution between the matrix and its diagonal is obtained in homogeneity analysis. The matrix used in this analysis is named gray level cooccurrence matrix (GLCM) and the range of homogeneity lies between 0 and 1. The range for energy analysis also lies in the interval [0, 1]. The results of Table 23 are obtained by applying these analyses on the original and encrypted images. For all the proposed 16 S-boxes, we calculated the values of the statistical analyses.

A 256×256 JPEG image of Lena is considered for MLC analysis. Figure 2 shows the results of image encryption with 16 proposed S-boxes.

4. Balanced Boolean Function

4.1. Balance Property. The imbalance of a Boolean function weak system against linear cryptanalysis highlights the importance of balance property. The balance property indicates that the higher the magnitude of a function's imbalance, the more the chances of a high probability linear approximation. A Boolean function $f: \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$ is balanced. If the cardinality or Hamming weight of these two functions, that is, $\{x: f(x) = 0\}$ and $\{x: f(x) = 1\}$ is the same, then it is named the balance function.

4.2. Balance Property of the Proposed S-Box. All the Boolean functions $f_i, i = 1, 2, 3, \ldots, 8$ involved in proposed S-boxes are balanced just like the Boolean functions of AES, S_8, AES and other well-known S-boxes. The nonlinearity of the proposed S-boxes is equal to 112.

5. Conclusion

In this paper, a scheme for the synthesis of 8×8 S-boxes over 16 isomorphic Galois fields is presented. Here, we fixed all the parameters of affine power affine transformation, that is, a, b, c, d for 16 S-boxes. We have 16 primitive irreducible polynomials of degree 8 and they prompt us to construct 16 Galois field extensions of order 256. By using elements of the Galois field, corresponding to each different pair of the parameters, one can construct different S-boxes. These S-boxes obtained as a result of APA transformation which is bijective, pass nonlinearity test, and out bit independent criterion (BIC) which demonstrates that the existing S-boxes have high confusion producing capability. The evaluation of constructed S-boxes is done with some algebraic and statistical analyses. The results of these analyses highlight the characteristics of all the proposed S-boxes and later these S-boxes are equated with some of the existing S-boxes. In addition to this, we also ensured that all these constructed S-boxes are balanced that guarantee the strength of our S-boxes. Hence, we have concluded that a large class of S-boxes can be obtained by varying parameters of affine power affine transformations. These S-boxes can be used for secure communication.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

There are no conflicts of interest among the authors.

Acknowledgments

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through research groups program under Grant no. R.G.P. 1/234/41.

References

[1] J. Daemen and V. Rijmen, "The design of Rijndael: AES,"in The Advanced Encryption Standard, Springer, Berlin, Germany,2002.

[2] R. Zimmermann, A. Curiger, H. Bonnenberg, H. Kaeslin, N. Felber, and W. Fichtner, "A 177 Mb/s VLSI implementation of the international data encryption algorithm,"

IEEE Journal of Solid-State Circuits, vol. 29, no. 3, pp. 303–307, 1994.

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

[4] National Bureau of Standards, *Data Encryption Standard*, Vol. 46, FIPS Publication, U.S. Department of Commerce, Washington, DC, USA, 1977.

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

[6] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, "Construction of S8 Liu J S-boxes and their applications," *Computers & Mathematics with Applications*, vol. 64, no. 8, pp. 2450–2458, 2012.

[7] M. T. Tran, D. K. Bui, and A. D. Duong, "Gray S-box for advanced encryption standard,"in Proceedings of the 2008 International Conference on Computational Intelligence and Security, vol. 1, IEEE, Suzhou, China, December 2008.

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

[9] M. Khan, T. Shah, H. Mahmood, M. A. Gondal, and I. Hussain, "A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems," *Nonlinear Dynamics*, vol. 70, no. 3, pp. 2303–2311, 2012.

[10] M. Khan and T. Shah, "An efficient construction of substitution box with fractional chaotic system," *Signal, Image and Video Processing*, vol. 9, no. 6, pp. 1335–1338, 2015.

[11] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, "A projective general linear group based algorithm for the construction of substitution box for block ciphers," *Neural Computing and Applications*, vol. 22, no. 6, pp. 1085–1093, 2013.

[12] Y. Tian and Z. Lu, "Novel permutation-diffusion image encryption algorithm with chaotic dynamic S-box and DNA sequence operation," *AIP Advances*, vol. 7, no. 8, Article ID 085008, 2017.

[13] M. Khan, F. Masood, A. Alghafis, M. Amin, and S. I. Batool Naqvi, "A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion," *PLoS One*, vol. 14, no. 12, Article ID e0225031, 2019.

[14] M. Khan and T. Shah, "A novel cryptosystem based on general linear group," *3D Research*, vol. 6, no. 1, 2015.

[15] D. Shah, T. Shah, and S. S. Jamal, "A novel efficient image encryption algorithm based on affine transformation combine with linear fractional transformation," *Multidimensional Systems and Signal Processing*, vol. 31, no. 3, pp. 885–905, 2020.

[16] Y. Naseer, D. Shah, and T. Shah, "A novel approach to improve multimedia security utilizing 3D mixed chaotic map," *Microprocessors and Microsystems*, vol. 65, pp. 1–6, 2019.

[17] K. E. A. Skipjack, "Algorithm," *Specifications Version*, vol. 2, no. 29, pp. 1–23, 1998.

[18] E. S. Abuelyman and A.-A. Sultan Alsehibani, "An optimized implementation of the S-box using residue of prime numbers," *International Journal of Computer Science and Network Security*, vol. 8, no. 4, pp. 304–309, 2008.

[19] S. Mahmood et al., "To study the effect of the generating polynomial on the quality of nonlinear components in block ciphers." *Security and Communication Networks*, vol. 2018, Article ID 5823230, 8 pages, 2018.

[20] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—Eurocrypt'93*, pp. 386–397, Springer Berlin Heidelberg, Heidelberg, Germany, 1993.

[21] Y. Wang, Q. Xie, Y. Wu, and B. Du, "A software for S-box performance analysis and test," in *Proceedings of the 2009 International Conference on Electronic Commerce and Business Intelligence*, pp. 125–128, IEEE, Beijing, China, June 2009.

[22] M. A. Gondal, A. Raheem, and I. Hussain, "A scheme for obtaining secure S-boxes based on chaotic Baker's map," *3D Research*, vol. 5, no. 3, pp. 5–17, 2014.

[23] A. Belazi, R. Rhouma, and S. Belghith, "A novel approach to construct S-box based on Rossler system," in *Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 611–615, Dubrovnik, Croatia, August 2015.

[24] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology—Crypto'85 Proceedings*, pp. 523–534, Springer Berlin Heidelberg, Heidelberg, Germany, 1985.

[25] F. Sattar and M. Mufti, "Spectral characterization and analysis of avalanche in cryptographic substitution boxes using walsh-hadamard transformations," *International Journal of Computer Applications*, vol. 28, no. 6, 2011.

[26] J. Detombe and S. Tavares, "On the design of S-boxes," *Advances in Cryptology: Proceedings of CRYPTO_92*, Springer Berlin Heidelberg, Heidelberg, Germany, Lecture Notes in Computer Science, 1992.

[27] 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.

[28] A. Farhan, R. Subhi, H. Rashed Yassein, and N. Al-Saidi, "A new approach to generate multi S-boxes based on RNA computing," *International Journal of Innovative Computing, Information and Control: IJICIC*, vol. 16, no. 1, pp. 331–348, 2020.

[29] D. Shah and T. Shah, "Binary galois field extensions dependent multimedia data security scheme," *Microprocessors and Microsystems*, vol. 77, Article ID 103181, 2020.