Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.039013

ARTICLE

Nonlinear Components of a Block Cipher over Eisenstein Integers

Mohammad Mazyad Hazzazi[1], Muhammad Sajjad[2], Zaid Bassfar[3], Tariq Shah[2,*] and Ashwag Albakri[4]

[1]Department of Mathematics, College of Science, King Khalid University, Abha, 61413, Saudi Arabia

[2]Department of Mathematics, Quaid-I-Azam University, Islamabad, 45320, Pakistan

[3]Department of Information Technology, University of Tabuk, Tabuk, 71491, Saudi Arabia

[4]Department of Computer Science, College of Computer Science & Information Technology, Jazan University, Jazan, 45142, Saudi Arabia

*Corresponding Author: Tariq Shah. Email: stariqshah@qau.edu.pk

Received: 07 January 2023 Accepted: 14 April 2023 Published: 26 December 2023

ABSTRACT

In block ciphers, the nonlinear components, also known as substitution boxes (S-boxes), are used with the purpose to induce confusion in cryptosystems. For the last decade, most of the work on designing S-boxes over the points of elliptic curves, chaotic maps, and Gaussian integers has been published. The main purpose of these studies is to hide data and improve the security levels of crypto algorithms. In this work, we design pair of nonlinear components of a block cipher over the residue class of Eisenstein integers (EI). The fascinating features of this structure provide S-boxes pair at a time by fixing three parameters. However, in the same way, by taking three fixed parameters only one S-box is obtained through a prime field-dependent Elliptic curve (EC), chaotic maps, and Gaussian integers. The newly designed pair of S-boxes are assessed by various tests like nonlinearity, bit independence criterion, strict avalanche criterion, linear approximation probability, and differential approximation probability.

KEYWORDS

Eisenstein integers; residue class of Eisenstein integers; block cipher; S-boxes; analysis of S-boxes

1 Introduction

Cryptography was widely used in military, diplomatic, and government applications until the 1970s. In the 1980s, the telecommunications and financial industries installed hardware cryptographic devices. The mobile phone system was the first cryptographic application in the late 1980s. Nowadays, everyone uses cryptographic applications in their daily lives. Our daily lives commonly depend on the secure transmission of information and data. Online shopping, cell phone messages and calls, ATMs, electronic mail, facsimile, wireless media, and data transfer over the internet all require a system to maintain the secrecy and integrity of private information. Cryptography offers a mechanism for everyone to interact safely in a hostile environment. Sensitive data is significantly aided by cryptography. Communication is encrypted to guarantee that its meaning is hidden, preventing anybody who reads it from understanding something regarding it unless somebody else manages to decrypt it [1].

In cryptography, the S-box is crucial for ensuring secure communication. Shannon suggested the notion of an S-box in 1949 in [2]. S-boxes serve a pivotal role in causing confusion within the data. According to Shannon, concealing the relationship between the key and cipher text is referred to as confusion, while concealing the statistical link between plain text as well as cipher text is referred to as diffusion. In other words, the non-uniformity in the distribution of individual letters inside plain text should be redistributed into the non-uniformity in the distribution of much bigger structures in the encrypted text, which is substantially more difficult to decrypt [3]. The Rijndael algorithm is basically the same as an iterated block cipher but has a few extra features. Before we talk about the Rijndael algorithm, we will talk about an iterated block cipher shown in [4].

Many scholars employed diverse algebraic and statistical frameworks to confound data and produce S-boxes. In [5], the authors suggested S-boxes over the permutation of the symmetric group. In [6], Javeed et al. constructed the non-linear component of block cipher by means of a chaotic dynamical system and symmetric group. In [7], the authors described the S-box based on the subgroup of the Galois field. The author suggested a robust encryption system using a modified Chebyshev map, Advanced Encryption Standard (AES) S-boxes, and a symmetric group of permutations [8].

In [9], the authors proposed a new scheme for the construction of the S-box based on the linear fractional transformation (LFT) and permutation function. In [10], the authors proposed S-box over the Mobius group and finite field. The author proposed S-box on a nonlinear chaotic map in [11]. In [12], Sajjad et al. designed pair of nonlinear components of a block cipher over Gaussian integers. In [13,14], the authors constructed cyclic codes over quaternion integers, these quaternion structures can be helpful for the construction of S-boxes. The authors designed differential cryptanalysis of DES-like cryptosystems in [15]. Cassal-Quiroga et al. generated the dynamical S-boxes for block ciphers via an extended logistic map [16]. Tang et al. designed a new method of dynamical S-boxes based on discretized chaotic maps [17]. Chen et al. extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps [18]. The authors constructed s-boxes using different maps over elliptic curves for image encryption [19]. Cavusoglu et al. [20] constructed S-box based on chaotic scaled zhongtang system. Siddiqui et al. developed a novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve in [21]. Farhan et al. designed a new S-box generation algorithm based on the multistability behavior of a plasma perturbation model [22]. In [23], the authors approached the S-boxes and permutation, substitution, based encryption.

Eisenstein integers are named after German mathematician Ferdinand Eisenstein, who first introduced them in the 1850s while studying the theory of quadratic forms. Like ordinary complex numbers, Eisenstein integers can be added and multiplied together. However, their properties are different. Eisenstein integers have important applications in number theory, coding theory, data security, and algebraic geometry. They also have connections to other areas of mathematics, such as algebraic number theory and modular forms [24].

An S-box generator is appropriate for cryptographic purposes if it can efficiently make highly dynamic S-boxes with good cryptographic properties or tests like nonlinearity, bit independence criterion, strict avalanche criterion, linear approximation probability, and differential approximation probability. The key contributions of our proposed study are given below:

- Propose an algorithm to generate pair of S-boxes by the cyclic group over the residue class of Eisenstein integers.
- Security Analysis.
- The advantages of the proposed algorithm over EI with some of the existing algorithms over EC.

This paper is structured as follows: Basic definitions, cyclic group over the residue class of Eisenstein integers, and some fundamental results are elaborated in Section 2. The scheme of the pair of new S-boxes is proposed in Section 3. Analysis of the proposed S-boxes including nonlinearity, bit independence criterion, strict avalanche criterion, linear approximation probability, and differential approximation probability investigated in Section 4. The comparison of the proposed S-boxes with some of the existing S-boxes are given in Section 5. Conclusions and future directions are given in Section 6.

2 Preliminaries

This section provides the key concepts and basic findings that will be used in the study of upcoming sections. First of all, we recall the definition of Eisenstein integers, cyclic group over a residue class of Eisenstein integers, and some fundamental results.

Eisenstein Integers

In [24], Eisenstein integers are a subset of complex numbers with real and vector parts.

1. $\mathbb{Z}[\omega] = \{b_0 + b_1\omega : b_0, b_1 \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the set of integers.
2. Multiplicative identity is 1.
3. ω is the cube root of unity.

Let $h = b_0 + b_1\omega$ be an element of the Eisenstein integer ring, then the conjugate of h is $\overline{h} = b_0 + b_1\omega^2$. Then the norm of h is given by

$$p = N(h) = h\overline{h} = b_0^2 + b_1^2 - b_0b_1$$

An Eisenstein integer has only two parts, one is the scalar part b_0 and the other is the vector part $b_1\omega$.

Addition of Two Eisenstein Integers

Let $h = a_1 + b_1\omega$ and $k = a_2 + b_2\omega$ be two Eisenstein integers then, the sum of two Eisenstein integers is also an Eisenstein integer defined as

$$h + k = (a_1 + b_1\omega) + (a_2 + b_2\omega) = (a_1 + a_2) + \omega\,(b_1 + b_2) = a_3 + \omega b_3$$

Multiplication of Two* Eisenstein *Integers

Let $h = a_1 + b_1\omega$ and $k = a_2 + b_2\omega$ are two Eisenstein integers then, the multiplication of two Eisenstein integers is also an Eisenstein integer defined as

$$hk = (a_1 + b_1\omega)\,(a_2 + b_2\omega) = (a_1a_2 - b_1b_2) + \omega\,(a_1b_2 + a_2b_1 - b_1b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1 - b_1b_2)$$
$$= a_4 + b_4\omega$$

Theorem: In [24], the set of natural numbers for each odd rational prime p, there is a prime $h \in \mathbb{Z}[\omega]$, such that $N(h) = p = h\overline{h}$. In particular, p is not prime in $\mathbb{Z}[\omega]$.

Theorem: In [24], if the norm of an Eisenstein integer $\boldsymbol{N(h)}$ is prime in $\mathbb{Z}$, then the Eisenstein integer $\boldsymbol{h}$ is prime in $\mathbb{Z}[\boldsymbol{\omega}]$.

Definition: In [24], let $\mathbb{Z}[\boldsymbol{\omega}]$ be the set of Eisenstein integers and $\mathbb{Z}[\boldsymbol{\omega}]_{\boldsymbol{h}}$ be the residue class of Eisenstein integers over modulo $\boldsymbol{h}, \boldsymbol{h} = \boldsymbol{a} + \boldsymbol{b\omega}$. Then, the modulo function:

$$s\colon \mathbb{Z}[\omega] = \{c + d\omega\colon c, d \in \mathbb{Z}\} \to \mathbb{Z}[\omega]_h$$

Then, $s(u) = z(modh) = u - \left[\frac{u\bar{h}}{h\bar{h}}\right] h.$

where $z \in \mathbb{Z}[\omega]_h$ and [.] are rounding to the nearest integer. The rounding of an Eisenstein integer can be done by rounding the real part and coefficients of the vector part separately to the closest integer.

Theorem: In [24], let $\boldsymbol{h}$ be an Eisenstein prime, and the number of Eisenstein integers modulo $\boldsymbol{h}$ is the norm of $\boldsymbol{h}$. If $\boldsymbol{\rho} \neq \mathbf{0}$ (mod $\boldsymbol{h}$), then $\boldsymbol{\rho}^{n(h)-1} \equiv \mathbf{1}$(mod $\boldsymbol{h}$).

Remark: The group generated b $< \boldsymbol{\rho} >$ in the above Theorem is named $\boldsymbol{S}$.

3 Redesign of Pair of $n \times n$ S-boxes over Eisenstein Integers

Multiple methods can be employed to cause confusion inside a security system. S-box is one of the most efficient cryptographic algorithms in use today. The S-boxes are generally formed using the EI class or the multiplicative cyclic group. As a result, it is feasible to create a variety of S-boxes across the residue class of EI, which presents a fantastic outlook for the development of secure and consistent cryptosystems. The subsequent procedures are useful for constructing S-boxes over the residue class of EI (Multiplicative cyclic group).

Step 1: Construct a cyclic group S of order $p - 1$ over the residue class of EI.

Step 2: Apply permutation through affine mapping as:

$f(x) = (ax + b)\ (mod\ 2^n)$

where $b \in S$ and a be the unit element of S.

Step 3: Separate real and vector parts of Step 2.

Step 4: Apply modulo 2^n over the separated parts in Step 3.

Step 5: Select the first 2^n non-repeated elements from the elements of Step 4.

Step 6: Get a pair of S-boxes.

The construction of S-boxes by Eisenstein integers provides us with better performance instead of S-boxes by using other structures like as chaotic maps, elliptic curves, finite fields, etc.

3.1 Pair of 4 × 4 S-boxes over the Residue Class of EI

Let $h = 2 + 9\omega$, $p = n(h) = 2^2 + 9^2 - 18 = 67$, and $\beta = 2 + 3\omega = (2, 3)$, then the cyclic group generated by β is given in Table 1.

Table 1: Cyclic group generated by $\boldsymbol{\beta}$

i	β^i	i	β^i	i	β^i
1	(2, 3)	23	(1, 65)	45	(64, 66)
2	(2, 1)	24	(66, 65)	46	(66, 1)
3	(66, 63)	25	(64, 1)	47	(4, 3)
4	(3, 3)	26	(0, 64)	48	(64, 0)
5	(4, 4)	27	(2, 5)	49	(5, 7)
6	(3, 6)	28	(5, 6)	50	(3, 1)
7	(2, 66)	29	(64, 65)	51	(1, 3)

(Continued)

Table 1 (continued)

i	β^i	i	β^i	i	β^i
8	(65, 0)	30	(2, 2)	52	(0, 65)
9	(63, 61)	31	(63, 62)	53	(64, 62)
10	(63, 65)	32	(2, 4)	54	(2, 65)
11	(0, 66)	33	(66, 0)	55	(1, 1)
12	(3, 1)	34	(65, 64)	56	(66, 2)
13	(1, 66)	35	(65, 66)	57	(1, 2)
14	(63, 64)	36	(1, 4)	58	(3, 66)
15	(3, 0)	37	(64, 64)	59	(0, 3)
16	(62, 60)	38	(63, 63)	60	(65, 62)
17	(64, 63)	39	(64, 61)	61	(62, 61)
18	(66, 64)	40	(65, 1)	62	(3, 2)
19	(0, 2)	41	(2, 0)	63	(65, 65)
20	(3, 5)	42	(4, 6)	64	(4, 5)
21	(65, 2)	43	(4, 2)	65	(65, 63)
22	(66, 66)	44	(0, 1)	66	(1, 0)

Apply the affine permutation mapping, $f(x) = ((63 + 61\omega)x + (63 + 62\omega))(mod\ 16)$, separate real and vector parts, and select the first 16 non-repeating entries for real and vector parts, which are given in Tables 2 and 3.

Table 2: 4×4 S-box by the scalar part of EI

15	3	1	6
12	9	10	14
11	5	8	7
2	4	0	13

Table 3: 4×4 S-box by the vector part of EI

13	0	12	4
11	9	2	8
14	6	3	5
15	1	10	7

3.2 Pair of 8 × 8 S-boxes over the Residue Class of EI

Example 1: Let $h = 81 + 71\omega$, $p = n(h) = 81^2 + 71^2 - (81)(71) = 5851$, and $\beta = 2 + 3\omega = (2, 3)$, then apply the same procedure of 3.1, we get pair of S-boxes by affine mapping $f(x) = ((59 + 29\omega)x + (14 + 8\omega))\ (mod 256)$ given in Tables 4 and 5.

Table 4: 8×8 S-box by the scalar part of EI $= \boldsymbol{S}_1$

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

Table 5: 8×8 S-box by the vector part of EI $= \boldsymbol{S}_2$

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

Example 2: Let $h = 81 + 71\omega$, $p = n(h) = 81^2 + 71^2 - (81)(71) = 5851$, and $\beta = 2 + 3\omega = (2, 3)$, then apply the same procedure of 3.1, we get pair of S-boxes by affine mapping $f(x)\ ((59 + 29\omega)x + (7 + 5836\omega))\ (mod 256)$ given in Tables 6 and 7.

Table 6: 8×8 S-box by the vector part of EI $= \boldsymbol{S_3}$

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

Table 7: 8×8 S-box by the vector part of EI $= \boldsymbol{S_4}$

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

4 Analysis of S-boxes

There are the following tests to analyze the properties of S-boxes.

4.1 Non-Linearity

The nonlinearity of the S-box refers to the property of the substitution box used in cryptographic algorithms, which is designed to introduce nonlinearity into the encryption process. In particular, the S-box is used in block ciphers to perform the substitution of plaintext bits with cipher text bits, and its nonlinearity is important for the security of the cipher. The nonlinearity of the S-box is usually measured using a metric called the "nonlinearity coefficient" or "nonlinearity index". This metric quantifies the degree of nonlinearity introduced by the S-box and is based on the Walsh-Hadamard transform of the S-box. A high nonlinearity coefficient indicates that the S-box is highly nonlinear, which is desirable for cryptographic purposes. Nonlinear S-boxes make it more difficult for an attacker to find patterns or correlations between the plaintext and cipher text, which can be used to break the cipher [25]. To achieve high nonlinearity, S-boxes are often constructed using mathematical functions that are highly nonlinear, such as power functions or finite field operations. The upper bound of nonlinearity is $N(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$, for S-box. The optimal value of non-linearity is 120. The nonlinearity of the proposed S-boxes is given in Table 8.

Table 8: Non-linearity of proposed S-boxes

S_1	108.0	108.0	108.0	108.0	102.0	108.0	108.0	106.0
S_2	108.0	106.0	108.0	108.0	108.0	106.0	104.0	106.0
S_3	108.0	108.0	108.0	108.0	102.0	108.0	108.0	106.0
S_4	108.0	106.0	108.0	108.0	108.0	106.0	104.0	106.0

The average non-linearity of proposed S-boxes is 107, 106.75, 107.0, and 106.75.

4.2 Bit Independent Criterion (BIC)

The bit independence criterion of an S-box is a measure of its resistance to linear and differential cryptanalysis attacks. Specifically, it refers to the property that no linear relationship exists between any two output bits of the S-box and any two input bits of the S-box. In other words, the bit independence criterion of an S-box ensures that changing one input bit or one output bit of the S-box will not affect the other output bits or input bits, respectively, in a linear way [26]. This property makes it more difficult for an attacker to analyze the S-box using linear or differential cryptanalysis. To achieve high bit independence, S-box designers often use mathematical structures, such as finite fields and Boolean functions, to construct the S-box lookup table. They also perform extensive testing and analysis to ensure that the S-box meets the required bit independence criteria and other cryptographic properties. The results of the BIC are given in Tables 9–12.

Table 9: Bit independent criterion of S_1

0.0	0.498046875	0.49609375	0.517578125	0.501953125	0.5078125	0.509765625	0.4765625
0.498046875	0.0	0.4921875	0.509765625	0.48828125	0.513671875	0.5	0.5078125
0.49609375	0.4921875	0.0	0.5234375	0.5234375	0.515625	0.513671875	0.50390625
0.517578125	0.509765625	0.5234375	0.0	0.498046875	0.490234375	0.49609375	0.5234375
0.501953125	0.48828125	0.5234375	0.498046875	0.0	0.51953125	0.494140625	0.53515625
0.5078125	0.513671875	0.515625	0.490234375	0.51953125	0.0	0.529296875	0.513671875
0.509765625	0.5	0.513671875	0.49609375	0.494140625	0.529296875	0.0	0.5078125
0.4765625	0.5078125	0.50390625	0.5234375	0.53515625	0.513671875	0.5078125	0.0

Table 10: Bit independent criterion of S_2

0.0	0.49609375	0.53125	0.529296875	0.484375	0.5234375	0.4921875	0.4921875
0.49609375	0.0	0.505859375	0.509765625	0.494140625	0.490234375	0.486328125	0.513671875
0.53125	0.505859375	0.0	0.4921875	0.5	0.5078125	0.48828125	0.494140625
0.529296875	0.509765625	0.4921875	0.0	0.498046875	0.517578125	0.501953125	0.486328125
0.484375	0.494140625	0.5	0.498046875	0.0	0.5	0.48046875	0.509765625
0.5234375	0.490234375	0.5078125	0.517578125	0.5	0.0	0.521484375	0.498046875
0.4921875	0.486328125	0.48828125	0.501953125	0.48046875	0.521484375	0.0	0.498046875
0.4921875	0.513671875	0.494140625	0.486328125	0.509765625	0.498046875	0.498046875	0.0

Table 11: Bit independent criterion of S_3

0.0	0.498046875	0.49609375	0.517578125	0.501953125	0.5078125	0.509765625	0.4765625
0.498046875	0.0	0.4921875	0.509765625	0.48828125	0.513671875	0.5	0.5078125
0.49609375	0.4921875	0.0	0.5234375	0.5234375	0.515625	0.513671875	0.50390625
0.517578125	0.509765625	0.5234375	0.0	0.498046875	0.490234375	0.49609375	0.5234375
0.501953125	0.48828125	0.5234375	0.498046875	0.0	0.51953125	0.494140625	0.53515625
0.5078125	0.513671875	0.515625	0.490234375	0.51953125	0.0	0.529296875	0.513671875
0.509765625	0.5	0.513671875	0.49609375	0.494140625	0.529296875	0.0	0.5078125
0.4765625	0.5078125	0.50390625	0.5234375	0.53515625	0.513671875	0.5078125	0.0

Table 12: Bit independent criterion of S_4

0.0	0.49609375	0.53125	0.529296875	0.484375	0.5234375	0.4921875	0.4921875
0.49609375	0.0	0.505859375	0.509765625	0.494140625	0.490234375	0.486328125	0.513671875
0.53125	0.505859375	0.0	0.4921875	0.5	0.5078125	0.48828125	0.494140625
0.529296875	0.509765625	0.4921875	0.0	0.498046875	0.517578125	0.501953125	0.486328125
0.484375	0.494140625	0.5	0.498046875	0.0	0.5	0.48046875	0.509765625
0.5234375	0.490234375	0.5078125	0.517578125	0.5	0.0	0.521484375	0.498046875
0.4921875	0.486328125	0.48828125	0.501953125	0.48046875	0.521484375	0.0	0.498046875
0.4921875	0.513671875	0.494140625	0.486328125	0.509765625	0.498046875	0.498046875	0.0

Hence S_1, S_2, S_3 and S_4 satisfied the bit-independent criterion close to the best possible value.

4.3 Linear Approximation Probability (LP)

The linear approximation probability for a substitution box (S-box) is a measure of the probability that a linear approximation of the S-box will hold. In other words, it is a measure of the correlation

between a set of input bits and a set of output bits of the S-box [27]. The linear approximation probability of an S-box is defined as $Pr[a \cdot x = b \cdot S(x)]$, where a and b are two-bit vectors of the same length as the input and output of the S-box, respectively, x is an input to the S-box, and S(x) is the output of the S-box. The symbol $\cdot$ denotes the bitwise inner product of the two-bit vectors. The linear approximation probability is a value between 0 and 1. A value of 0 means that there is no linear approximation of the S-box, while a value of 1 means that the linear approximation holds with certainty. We have calculated the linear approximation probability of the S-boxes S_1, S_2, S_3 and S_4. The maximum value of LP is 0.1484375, 0.1328125, 0.1484375, and 0.1328125.

4.4 Differential Approximation Probability (DAP)

The differential approximation probability for a substitution box (S-box) is a measure of the probability that a differential approximation of the S-box will hold. In other words, it is a measure of the correlation between a set of input differences and a set of output differences of the S-box. The differential approximation probability of an S-box is defined as $Pr[\Delta x \rightarrow \Delta y = \Delta u \rightarrow \Delta v]$, where Δx and Δy are two input differences of the S-box, Δu, and Δv are the corresponding output differences, and $\rightarrow$ denotes the S-box operation. The differential approximation probability is a value between 0 and 1. A value of 0 means that there is no differential approximation of the S-box, while a value of 1 means that the differential approximation holds with certainty. The DAP results of the proposed work are given in Tables 13–16.

Table 13: Differential approximation probability of $\boldsymbol{S_1}$

0.023	0.031	0.016	0.023	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.031	0.031	0.031
0.023	0.023	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.031
0.031	0.023	0.023	0.016	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.031
0.023	0.031	0.023	0.023	0.023	0.031	0.031	0.039	0.023	0.023	0.023	0.031	0.031	0.023	0.039	0.023
0.031	0.031	0.031	0.023	0.023	0.023	0.031	0.023	0.031	0.031	0.031	0.023	0.031	0.023	0.031	0.031
0.023	0.023	0.039	0.031	0.023	0.023	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.023
0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.031	0.031	0.023	0.031	0.031	0.031	0.023	0.023	0.031
0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.023	0.023
0.023	0.039	0.031	0.023	0.031	0.031	0.023	0.039	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023
0.031	0.023	0.023	0.023	0.047	0.016	0.023	0.023	0.039	0.031	0.031	0.031	0.031	0.031	0.023	0.039
0.023	0.023	0.023	0.031	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0.031	0.023	0.031	0.016
0.023	0.031	0.031	0.039	0.031	0.031	0.031	0.031	0.023	0.023	0.031	0.023	0.023	0.023	0.031	0.031
0.023	0.023	0.031	0.023	0.023	0.039	0.023	0.023	0.023	0.031	0.031	0.031	0.023	0.023	0.023	0.023
0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.039	0.023	0.031	0.023	0.031
0.023	0.031	0.023	0.031	0.031	0.031	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.023	0.016
0.023	0.023	0.031	0.031	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0

Table 14 Differential approximation probability of S_2

0.023	0.023	0.016	0.023	0.023	0.023	0.023	0.031	0.023	0.039	0.031	0.023	0.023	0.023	0.023	0.031
0.031	0.023	0.031	0.031	0.031	0.023	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.031
0.031	0.023	0.031	0.023	0.023	0.023	0.031	0.031	0.023	0.031	0.023	0.023	0.039	0.023	0.023	0.023
0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.023	0.031
0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.031	0.031	0.023	0.031	0.023	0.023	0.031
0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023
0.023	0.023	0.031	0.031	0.031	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031
0.023	0.031	0.023	0.023	0.039	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.031	0.023	0.031	0.031
0.023	0.023	0.023	0.031	0.031	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.031
0.023	0.023	0.023	0.023	0.023	0.023	0.039	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023
0.031	0.016	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.023
0.031	0.023	0.031	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.031	0.031	0.023
0.023	0.023	0.023	0.039	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023
0.031	0.023	0.031	0.023	0.023	0.023	0.031	0.039	0.023	0.023	0.031	0.023	0.023	0.039	0.031	0.023
0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.023	0.031	0.031	0.023	0.023	0.031	0.031	0.023	0.023
0.016	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0

Table 15: Differential approximation probability of S_3

0.023	0.031	0.016	0.023	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.031	0.031	0.031
0.023	0.023	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.031
0.031	0.023	0.023	0.016	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.031
0.023	0.031	0.023	0.023	0.023	0.031	0.031	0.039	0.023	0.023	0.023	0.031	0.031	0.023	0.039	0.023
0.031	0.031	0.031	0.023	0.023	0.023	0.031	0.023	0.031	0.031	0.031	0.023	0.031	0.023	0.031	0.031
0.023	0.023	0.039	0.031	0.023	0.023	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.023
0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.031	0.031	0.023	0.031	0.031	0.031	0.023	0.023	0.031
0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.023	0.023
0.023	0.039	0.031	0.023	0.031	0.031	0.023	0.039	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023
0.031	0.023	0.023	0.023	0.047	0.016	0.023	0.023	0.039	0.031	0.031	0.031	0.031	0.031	0.023	0.039
0.023	0.023	0.023	0.031	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0.031	0.023	0.031	0.016
0.023	0.031	0.031	0.039	0.031	0.031	0.031	0.031	0.023	0.023	0.031	0.023	0.023	0.023	0.031	0.031
0.023	0.023	0.031	0.023	0.023	0.039	0.023	0.023	0.023	0.031	0.031	0.031	0.023	0.023	0.023	0.023
0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.039	0.023	0.031	0.023	0.031
0.023	0.031	0.023	0.031	0.031	0.031	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.023	0.016
0.023	0.023	0.031	0.031	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0

Table 16 Differential approximation probability of S_4

0.023	0.023	0.016	0.023	0.023	0.023	0.023	0.031	0.023	0.039	0.031	0.023	0.023	0.023	0.023	0.031
0.031	0.023	0.031	0.031	0.031	0.023	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.031
0.031	0.023	0.031	0.023	0.023	0.023	0.031	0.031	0.023	0.031	0.023	0.023	0.039	0.023	0.023	0.023

(Continued)

Table 16 (continued)

0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.023	0.031
0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.031	0.031	0.023	0.031	0.023	0.023	0.031
0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023
0.023	0.023	0.031	0.031	0.031	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031
0.023	0.031	0.023	0.023	0.039	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.031	0.023	0.031	0.031
0.023	0.023	0.023	0.031	0.031	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.031
0.023	0.023	0.023	0.023	0.023	0.023	0.039	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023
0.031	0.016	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.023
0.031	0.023	0.031	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.031	0.031	0.023
0.023	0.023	0.023	0.039	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023
0.031	0.023	0.031	0.023	0.023	0.023	0.031	0.039	0.023	0.023	0.031	0.023	0.023	0.039	0.031	0.023
0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.023	0.031	0.031	0.023	0.023	0.031	0.031	0.023	0.023
0.016	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0

The maximum value of differential approximation probability for both S-boxes S_1, S_2, S_3, and S_2 is 0.046875, 0.0390625, 0.046875, and 0.0390625.

4.5 Strict Avalanche Criterion (SAC)

The Strict Avalanche Criterion (SAC) is a measure of the cryptographic strength of a substitution box (S-box). The SAC measures how much a change in one input bit affects the output bits on average, and is defined as follows: For every pair of input bits i and j, and for every pair of output bits k and l, the difference between the output bits when i and j are flipped is denoted by $\Delta_{\{i,j\}}^{\{k,l\}}$. The SAC requires that the average over all pairs of input and output bits of the total number of output bit differences that occur when a single input bit is flipped is at least 1/2:

$$\sum \{i,j=1\}^{\{n\}} \sum \{k,l=1\}^{\{m\}} abs\left(Pr\left[\Delta_{\{i,j\}}^{\{k,l\}}=1\right]-\frac{1}{2}\right) \leq \varepsilon$$

where n is the number of input bits, m is the number of output bits, and ε is a small positive constant, typically set to 0.01 or smaller. The results in Tables 17–20 show that the value of the strict avalanche criterion of S-boxes based on the residue of a prime number is ~1/2.

Table 17: Strict avalanche criterion of S_1

0.53125	0.453125	0.5	0.421875	0.421875	0.546875	0.5	0.5
0.53125	0.53125	0.484375	0.484375	0.421875	0.5	0.4375	0.484375
0.515625	0.484375	0.515625	0.484375	0.53125	0.515625	0.5	0.515625
0.5	0.5625	0.484375	0.515625	0.546875	0.484375	0.484375	0.484375
0.5	0.5625	0.515625	0.53125	0.421875	0.5	0.546875	0.5
0.484375	0.46875	0.484375	0.46875	0.5	0.578125	0.578125	0.515625
0.40625	0.46875	0.453125	0.5	0.484375	0.515625	0.546875	0.4375
0.453125	0.515625	0.5625	0.484375	0.515625	0.5	0.453125	0.46875

Table 18: Strict avalanche criterion of S_2

0.421875	0.515625	0.484375	0.53125	0.515625	0.46875	0.53125	0.484375
0.484375	0.375	0.53125	0.484375	0.515625	0.4375	0.515625	0.5
0.578125	0.53125	0.53125	0.515625	0.5	0.578125	0.5625	0.484375
0.515625	0.484375	0.453125	0.53125	0.53125	0.484375	0.546875	0.484375
0.5	0.546875	0.46875	0.5	0.46875	0.5625	0.578125	0.5
0.53125	0.5	0.453125	0.4375	0.5	0.484375	0.453125	0.453125
0.546875	0.515625	0.46875	0.484375	0.46875	0.546875	0.453125	0.5
0.53125	0.46875	0.53125	0.515625	0.484375	0.515625	0.5625	0.46875

Table 19: Strict avalanche criterion of S_3

0.53125	0.453125	0.5	0.421875	0.421875	0.546875	0.5	0.5
0.53125	0.53125	0.484375	0.484375	0.421875	0.5	0.4375	0.484375
0.515625	0.484375	0.515625	0.484375	0.53125	0.515625	0.5	0.515625
0.5	0.5625	0.484375	0.515625	0.546875	0.484375	0.484375	0.484375
0.5	0.5625	0.515625	0.53125	0.421875	0.5	0.546875	0.5
0.484375	0.46875	0.484375	0.46875	0.5	0.578125	0.578125	0.515625
0.40625	0.46875	0.453125	0.5	0.484375	0.515625	0.546875	0.4375
0.453125	0.515625	0.5625	0.484375	0.515625	0.5	0.453125	0.46875

Table 20: Strict avalanche criterion of S_4

0.421875	0.515625	0.484375	0.53125	0.515625	0.46875	0.53125	0.484375
0.484375	0.375	0.53125	0.484375	0.515625	0.4375	0.515625	0.5
0.578125	0.53125	0.53125	0.515625	0.5	0.578125	0.5625	0.484375
0.515625	0.484375	0.453125	0.53125	0.53125	0.484375	0.546875	0.484375
0.5	0.546875	0.46875	0.5	0.46875	0.5625	0.578125	0.5
0.53125	0.5	0.453125	0.4375	0.5	0.484375	0.453125	0.453125
0.546875	0.515625	0.46875	0.484375	0.46875	0.546875	0.453125	0.5
0.53125	0.46875	0.53125	0.515625	0.484375	0.515625	0.5625	0.46875

5 Comparison

The former tests are performed on well-known S-boxes over EC, chaotic maps, and finite fields presented in [19–23,26,27] in order to compare them to the proposed S-boxes S_1, S_2, S_3, and S_4 over EI. Table 21 shows the results of the EC, chaotic maps (CM), and EI analyses for the various parameters. It is discovered that the proposed S-boxes have a higher nonlinearity value than EC, CM, and other S-boxes. The intriguing features of the proposed technique provide S-boxes pair at a time by fixing three parameters a, b, and p. However, the prime field, which is dependent on the EC via various techniques, provides one S-box at a time by fixing three parameters a, b, and p. Table 21 and Fig. 1 show the

nonlinearity of the proposed S-box. The proposed S-box LAP results are lower than those presented in [19–23,26,27] and Fig. 2. As a result, the proposed S-boxes generate more data confusion and are more resistant to linear attack [17] than [19–23,26,27]. The proposed S-boxes' SAC and BIC results are comparable to those of other S-boxes used in Table 21 and Fig. 2. As a result, the S-box generated by the proposed technique and the S-boxes shown in Table 21 cause equal magnitude diffusion in the data. The proposed DAP is comparable to the DAP of S-boxes in [19–23,26,27] and Fig. 2. Thus, when compared to the others, the proposed technique generates an S-box with high resistance to differential cryptanalysis [18]. Table 21 shows the analysis results of newly generated paired S-boxes by the EI cyclic group. Table 21 shows that the performance of paired S-boxes by the cyclic group over EI is comparable to that of S-boxes over EC.

Table 21: Proposed S-boxes comparison with EC S-boxes for different primes

S-boxes	*Type*	*NL*	*LAP*	*DAP*	*SAC Max*	*SAC Ave*	*SAC Min*	*BIC Max*	*BIC Ave*	*BIC Min*
S_1 *(Proposed)*	*EI*	107.00	0.148	0.047	0.578	0.497	0.406	0.625	0.507	0.375
S_2 *(Proposed)*	*EI*	106.75	0.133	0.039	0.578	0.502	0.375	0.625	0.502	0.391
S_3 *(Proposed)*	*EI*	107.00	0.148	0.047	0.578	0.497	0.406	0.625	0.507	0.375
S_4 *(Proposed)*	*EI*	106.75	0.133	0.039	0.578	0.502	0.375	0.625	0.502	0.391
[19]	*EC*	104.00	0.148	0.047	0.610	0.516	0.422	0.543	0.503	0.463
[20]	*CM*	104.00	0.148	0.039	0.625	0.508	0.391	0.531	0.501	0.471
[21]	*EC*	104.00	0.145	0.039	0.610	0.5	0.390	0.531	0.501	0.471
[22]	*CM*	106.00	0.148	0.039	0.641	0.5235	0.406	0.537	0.504	0.471
[23]	*CM*	106.00	0.148	0.047	0.625	0.5155	0.406	0.539	0.505	0.471
[26]	*CM*	106.00	0.188	0.039	0.610	0.508	0.406	0.527	0.496	0.465
[27]	*CM*	106.00	0.148	0.023	0.609	0.5	0.391	0.525	0.499	0.473

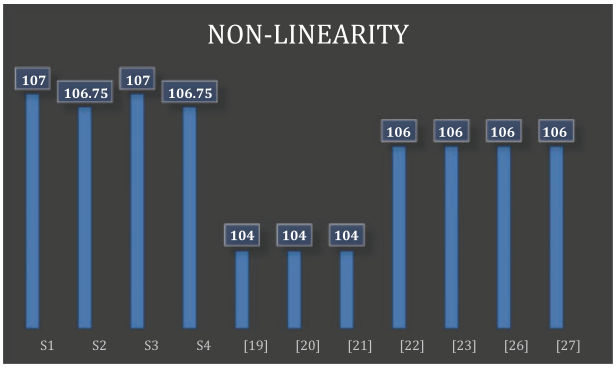

Figure 1: Comparison of NL of proposed work with existing works

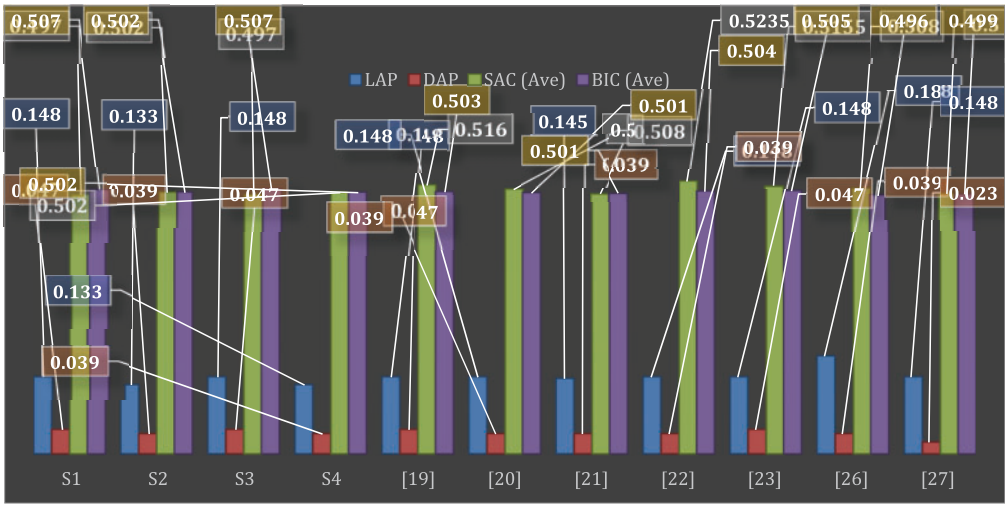

Figure 2: Comparison of BIC, SAC and LAP of proposed work with existing works

6 Conclusion and Future Directions

We propose a novel construction of substitution boxes by using affine mapping and fixing three parameters a, b, and p. By fixing the three parameters, the prime field dependent on the EC, chaotic maps, and Gaussian integers provide one S-box at a time. Here, the Prime p must be greater than or equal to 257 and belong to the cyclic group over the residue class of Eisenstein integers in order to produce cryptographically robust S-boxes. The newly proposed S-boxes are tested by using different available algebraic and statistical tests. Additionally, the proposed S-boxes cryptographic characteristics are contrasted with some of the currently used S-boxes over EC, Gaussian integers, and chaotic maps. The results indicate that the proposed algorithm can generate paired S-boxes with high resistance to linear and differential attacks.

The proposed S-boxes over the residue class of EI integers may extend to the S-boxes over the residue class of quaternion and octonion integers. These structures may also use for watermarking and image encryption.

Acknowledgement: The authors would like to thank the anonymous reviewers for their valuable comments. This work was financially supported by the Deanship of Scientific Research at King Khalid University in Saudi Arabia.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University, for funding this work through the General Research Groups Program under Grant No. R.G.P.2/109/43.

Author Contributions: Study conception and design: M. S., and T. S.; data collection: M. S., and M. M. H.; analysis and interpretation of results: M. S., T. S., M. M. H., Z. B., and A. A.; draft manuscript preparation: M. S., and M. M. H. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Ruohonen, "Mathematical cryptology," *Lecture Notes*, vol. 1, no. 1, pp. 1–138, 2010.

[2] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] M. M. Hoobi, "Strong triple data encryption standard algorithm using nth degree truncated polynomial ring unit," *Journal of Science*, vol. 3, no. 3, pp. 1760–1771, 2017.

[4] A. Fathy, I. F. Tarrad, H. F. A. Hamed and A. I. Awad, "Advanced encryption standard algorithm, issues and implementation aspects," in *Int. Conf. on Advanced Machine Learning Technologies and Applications*, Berlin, Heidelberg, Springer, vol. 12, pp. 516–523, 2012.

[5] A. Anees and Y. P. P. Chen, "Designing secure substitution boxes based on permutation of symmetric group," *Neural Computing and Applications*, vol. 2, no. 11, pp. 7045–7056, 2020.

[6] 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.

[7] H. A. Ahmed, M. F. Zolkipli and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," *Neural Computing and Applications*, vol. 31, pp. 7201–7210, 2019.

[8] I. Hussain, A. Anees, A. H. Alkhaldi, M. Aslam, N. Siddiqui *et al.,* "Image encryption based on Chebyshev chaotic map and S8 S-boxes," *Optica Applicata*, vol. 49, no. 2, pp. 317–330, 2019.

[9] L. C. N. Chew and E. S. Ismail, "S-box construction based on linear fractional transformation and permutation function," *Symmetry*, vol. 12, no. 5, pp. 826–842, 2020.

[10] B. Arshad, N. Siddiqui, Z. Hussain and M. E. U. Haq, "A novel scheme for designing secure substitution boxes (S-boxes) based on Mobius group and finite field," *Wireless Personal Communications*, vol. 135, no. 124, pp. 3527–3548, 2022.

[11] A. H. Zahid and M. J. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, pp. 1–10, 2019.

[12] M. Sajjad, T. Shah and R. J. Serna, "Designing pair of nonlinear components of a block cipher over gaussian integers," *Computers, Materials & Continua*, vol. 74, no. 1, pp. 1–20, 2023.

[13] M. Sajjad, T. Shah, M. M. Hazzazi, A. R. Alharbi and I. Hussain, "Quaternion integers based higher length cyclic codes and their decoding algorithm," *Computers, Materials & Continua*, vol. 73, no. 1, pp. 1177–1194, 2022.

[14] M. Özen and M. Güzeltepe, "Cyclic codes over some finite quaternion integer rings," *Journal of the Franklin Institute*, vol. 348, no. 7, pp. 1312–1317, 2011.

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

[16] B. B. Cassal-Quiroga and E. Campos-Cantón, "Generation of dynamical S-boxes for block ciphers via extended logistic map," *Mathematical Problems in Engineering*, vol. 3, pp. 1–12, 2020.

[17] G. Tang and X. Liao, "A method for designing dynamical S-boxes based on discretized chaotic map," *Chaos Solitons and Fractals*, vol. 23, no. 5, pp. 1901–1909, 2005.

[18] G. Chen, Y. Chen and X. Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps," *Chaos Solitons and Fractals*, vol. 31, no. 3, pp. 571–579, 2007.

[19] S. Ibrahim and A. Alharbi, "Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography," *IEEE Access*, vol. 8, pp. 194289–194302, 2020.

[20] U. Çavuşoğlu, A. Zengin, I. Pehlivan and S. Kaçar, "A novel approach for strong S-box generation algorithm design based on chaotic scaled Zhongtang system," *Nonlinear Dynamics*, vol. 87, no. 2, pp. 1081–1094, 2021.

[21] N. Siddiqui, A. Naseer and M. E. U. Haq, "A novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve," *Wireless Personal Communications*, vol. 116, no. 4, pp. 3015–3030, 2019.

[22] A. K. Farhan, R. S. Ali, H. Natiq and N. M. Al-Saidi, "A new S-box generation algorithm based on multistability behavior of a plasma perturbation model," *IEEE Access*, vol. 7, pp. 124914–124924, 2021.
[23] A. Belazi, M. Khan, A. A. A. El-Latif and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation, substitution, based encryption," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 337–361, 2017.
[24] K. Huber, "Codes over eisenstein-jacobi integers," *Contemporary Mathematics*, vol. 168, no. 1, pp. 165, 1994.
[25] C. Baudoin and F. X. Standaert, "Experimenting linear cryptanalysis," in *Advanced Linear Cryptanalysis of Block and Stream Ciphers*. Amsterdam: IOS Press, pp. 1–28, 2011.
[26] G. Jakimoski and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps," *IEEE Transactions on Circuits and Systems: Fundamental Theory and Applications*, vol. 48, no. 2, pp. 163–169, 2001.
[27] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S_8 permutation," *Neural Computing and Applications*, vol. 29, no. 4, pp. 993–999, 2018.