Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.035347
Article

Designing Pair of Nonlinear Components of a Block Cipher over Gaussian Integers

Muhammad Sajjad[1,*], Tariq Shah[1] and Robinson Julian Serna[2]

[1]Department of Mathematics, Quaid-I-Azam University, Islamabad, 45320, Pakistan
[2]Escuela de Matemáticas y Estadística, Universidad Pedagógica y Tecnológica de Colombia, Tunja, 150003, Columbia

*Corresponding Author: Muhammad Sajjad. Email: m.sajjad@math.qau.edu.pk
Received: 17 August 2022; Accepted: 24 October 2022

Abstract: In block ciphers, the nonlinear components, also known as substitution boxes (S-boxes), are used with the purpose of inducing confusion in cryptosystems. For the last decade, most of the work on designing S-boxes over the points of elliptic curves 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 Gaussian integers (GI). The fascinating features of this structure provide S-boxes pair at a time by fixing three parameters. But the prime field dependent on the Elliptic curve (EC) provides one S-box at a time by fixing three parameters a, b, and p. 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: Gaussian integers; residue class of gaussian 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 are commonly dependent 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. In an antagonistic environment, cryptography provides a way for everyone to communicate securely. Cryptography plays a major role in the security of data. Encryption of a message ensures that the meaning is concealed in it so that someone who reads the message cannot understand anything out of it unless people crack the message [1].

In cryptography, the S-box plays a major role in maintaining safe communication. In 1949, Shannon proposed the concept of an S-box. In creating confusion in data, S-boxes play a key role.

According to Shannon, hiding the relationship between the key and cipher text is known as confusion, while hiding the statistical relationship between plain text and cipher text is known as diffusion. In other words, the plain text's non-uniformity in the distribution of individual letters should be redistributed into the cipher text's non-uniformity in the distribution of much larger structures, which is significantly much harder to detect [2].

In literature, for creating confusion very well-known S-boxes are available in data and information, such as data encryption standard (DES), advanced encryption standard (AES), affine power affine, Gray, Skipjack, Xy_i, and Residue Prime Substitution boxes. In 1974, the National Bureau of Standards requested an American company to create a strong cryptosystem that could be used in unclassified U.S. applications. So, DES was developed by IBM and was adopted by NIST (then called the National Bureau of Standards) on January 15, 1977. It soon became the most widely used cryptosystem in the world. However, from the very beginning, DES attracted criticism for not having a sufficiently large key space to make it secure. The size of the key space in DES is 2^{56}. From early on, attempts were made to build a special-purpose machine devoted exclusively to the task of breaking the DES code. In 1998 a massively parallel network computer, called "DES Cracker," was built by Electronic Frontier Foundation EFF that could search 88 billion DES keys per second. It succeeded in finding a DES secret key in 56 h. In 1999, working in conjunction with a worldwide network of 100,000 computers, the DES Cracker could search 245 billion keys per second and succeed in finding a secret DES key in a little more than 22 h. It was thus clear that DES was no longer a secure cryptosystem [3]. Therefore it was necessary to phase out the DES and adopt a more secure encryption standard.

A brief description of the latest cryptosystem is approved for general use by the National Institute of Standards and Technology (NIST). It is called the Advanced Encryption Standard (AES) and was adopted, effective May 26, 2002, as the official Federal Information Processing Standard (FIPS) to be used by all U.S. government organizations to protect sensitive information. It is also expected to be used by other organizations, institutions, and individuals all over the world. The enciphering algorithm in AES was designed by two Belgian cryptographers, Dr. Joan Daeman and Dr. Vincent Rijmen. It was given the name Rijndael (pronounced "rhine dahl"). The basic structure of the Rijndael algorithm is that of an iterated block cipher, but with some additional features. Before considering the Rijndael algorithm, we will move towards an iterated block cipher which is present in [4].

For creating confusion on data, for the construction of S-boxes, many researchers used different schemes with algebraic and statistical structures. The authors proposed S-boxes over the permutation of the symmetric group in [5]. The construction of S-boxes over the action of the quotient of a modular group by using a secure scheme is given in [6]. The construction of the S-box based on the subgroup of the Galois field is given in [7]. The author proposed a strong encryption scheme by using a modified Chebyshev map, 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 author proposed S-box over the Mobius group and finite field. The author proposed S-box on a nonlinear chaotic map in [11]. The authors proposed S-boxes over the second coordinate of EC in [12]. Adnan et al. [13], designed the construction of a non-linear component of block cipher by means of a chaotic dynamical system and symmetric group. In [14], the author constructed cyclic codes over quaternion integers, these quaternion structures can be helpful for the construction of S-boxes.

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 Gaussian integers.
- Security Analysis.
- The advantages of the proposed algorithm over GI with some of the existing algorithms over EC.

This paper is structured as follows: Basic definitions, cyclic group over the residue class of Gaussian 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 Gaussian integers, cyclic group over a residue class of Gaussian integers, and some fundamental results.

Gaussian Integers

By following [[15], Section 2], Gaussian integers are a subset of complex numbers which have integers as real and imaginary parts;

1. $\mathbb{Z}[i] = \{b_0 + b_1 i\colon b_0,\ b_1 \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the set of integers.
2. Multiplicative identity is 1.
3. $i^2 = -1$

Let $h = b_0 + b_1 i$ be an element of the Gaussian integer ring, then the conjugate of h is $\overline{h} = b_0 - b_1 i$. The norm of h is the sum of the squares of the real part and the coefficient of the vector part of h;

$$p = n(h) = h\overline{h} = b_0^2 + b_1^2$$

A Gaussian integer has only two parts, one is the scalar part b_0 and the other is the vector part $b_1 i$.

Addition of two Gaussian Integers

Let $h = a_1 + b_1 i$ and $k = a_2 + b_2 i$ are two Gaussian integers then, the sum of two Gaussian integers is also a Gaussian integer defined as;

$$h + k = (a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + i(b_1 + b_2) = a_3 + b_3$$

Multiplication of two Gaussian Integers

Let $h = a_1 + b_1 i$ and $k = a_2 + b_2 i$ are two Gaussian integers then, the multiplication of two Gaussian integers is also a Gaussian integer defined as;

$$hk = (a_1 + b_1 i)(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1) = (a_1 a_2 - b_1 b_2\ , a_1 b_2 + a_2 b_1) = a_4 + b_4 i$$

Theorem: In [[15], Section 2], the set of natural numbers for each odd rational prime p, there is a prime $h \in \mathbb{Z}[i]$, such that $N(h) = p = h\bar{h}$. In particular, p is not prime in $\mathbb{Z}[i]$.

Theorem: In [[16], Theorem 6.3], if the norm of a Gaussian integer $\boldsymbol{N}(\boldsymbol{h})$ is prime in $\mathbb{Z}$, then the Gaussian integer $\boldsymbol{h}$ is prime in $\mathbb{Z}[i]$.

Definition: In [[17], Section 2], let $\mathbb{Z}[i]$ be the set of Gaussian integers and $\mathbb{Z}[i]_h$ be the residue class of Gaussian integers over modulo $\boldsymbol{h}$, $\boldsymbol{h} = \boldsymbol{a} + \boldsymbol{b}\boldsymbol{V}$. Then, the modulo function

ω: $\mathbb{Z}[i] = \{c + dV : c, d \in \mathbb{Z}\} \rightarrow \mathbb{Z}[i]_h$

Then, $\omega(u) = z \ (mod\ h) = u - \left[\dfrac{u\bar{h}}{h\bar{h}}\right] h.$

Where $z \in \mathbb{Z}[i]_h$ and [.] are rounding to the nearest integer. The rounding of a Gaussian integer can be done by rounding the real part and coefficients of the imaginary part separately to the closest integer.

Theorem: In [[17], Theorem 7.12], let $\boldsymbol{h}$ be a Gaussian prime, and the number of Gaussian 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 $\boldsymbol{h}$).

Theorem: In [[17], Theorem 2], If $\boldsymbol{c}$ and $\boldsymbol{d}$ are two relatively prime integers, then $\mathbb{Z}[\boldsymbol{i}]/\langle \boldsymbol{c} + \boldsymbol{di} \rangle$ is isomorphic to $\mathbb{Z}_{\mathbf{c}^2+\mathbf{d}^2}$.

3 Redesign of Pair of $n \times n$ S-Boxes Over Gaussian Integers

Numerous procedures can be used to generate confusion in a security system. S-box is one of the most efficient techniques in modern cryptosystems. The S-boxes are generally constructed through the class of GI, which is the multiplicative cyclic group. Consequently, there is a good choice to design a variety of S-boxes over the residue class of GI, which provides a marvelous perspective for secure and consistent cryptosystems. The following steps are helpful for the construction of S-boxes over the residue class of GI (Multiplicative cyclic group);

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

Step 2: Separate real and imaginary parts of the cyclic group constructed in Step 1.

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

Step 4: Select the first 2^n non-repeated elements from the elements of Step 3.

Step 5: Apply permutation through affine mapping as

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

where $b \in \mathbb{Z}_{2^n}$ and a be the units element of $\mathbb{Z}_{2^n}$.

Step 6: Get a pair of S-boxes.

3.1 Pair of 4×4 *S-Boxes Over the Residue Class of GI*

Let $h = 1 + 16i$, $p = n(h) = 1^2 + 16^2 = 257$, and $\beta = 2 + 4i = (2, 4)$, then the cyclic group generated by β as follows;

Select the first 16 non-repeated elements from the last two columns of Table 1, then apply the affine permutation mapping, $f(x) = (3x + 5)\ (mod\ 16)$, and get the pair of S-boxes separately in Tables 2 and 3.

Table 1: Cyclic group generated by β

Number	β^i	Real (β^i)	Imaginary (β^i)	(Real (β^i))(mod 256)	(Imaginary (β^i))(mod 256)
1	(2, 4)	2	4	2	4
2	(3, 256)	3	256	3	0
3	(250, 252)	250	252	10	12
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
256	(1, 0)	1	0	1	0

Table 2: 4×4 S-box by the real part of GI

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

Table 3: 4×4 S-box by the imaginary part

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

3.2 Pair of 8×8 *S-Boxes Over the Residue Class of GI*

Let $h = 14 + 61i$, $p = n(h) = 3917$, and $\beta = 1 + 11i = (1, 11)$, then the cyclic group generated by β as follows;

Select the first 256 non-repeated elements from the real part of Table 4. Then apply the affine permutation map $f(x) = (165x + 120)\ (mod\ 256)$, and get the S-box for the real part of GI in Table 5.

Table 4: Cyclic group generated by β

Number	β^i	Real (β^i)	Imaginary (β^i)	(Real (β^i))(mod 256)	(Imaginary (β^i))(mod 256)
1	(1, 11)	1	11	1	11
2	(213, 22)	213	22	213	22
3	(267, 58)	267	58	11	58
.	.	.	.	.	.

(Continued)

Table 4: Continued

Number	β^i	Real (β^i)	Imaginary (β^i)	(Real (β^i))(mod 256)	(Imaginary (β^i))(mod 256)
.	.	.	.	.	.
.	.	.	.	.	.
3916	(1, 0)	1	0	1	0

Table 5: $A = 8 \times 8$ S-box for the real part of GI

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

Select the first 256 non-repeated elements from the imaginary part of Table 4. Then apply the affine permutation map $f(x) = (165x + 119)\ (mod\ 256)$, and get S-box for the imaginary part of GI in Table 6.

Table 6: $B = 8 \times 8$ S-box for the imaginary part of GI

59	46	28	222	115	100	45	131	156	214	76	19	243	247	237	69
186	74	37	147	232	78	234	196	163	204	85	172	126	39	253	48
183	118	79	57	188	1	254	201	215	8	15	184	73	144	187	42
239	7	217	33	109	62	138	87	26	230	133	110	5	122	123	209
132	98	90	185	40	242	177	165	65	246	124	52	88	43	241	199
60	129	218	190	161	80	227	108	223	174	203	41	219	197	56	34
191	101	63	235	158	150	251	51	245	99	125	13	141	35	53	151
116	68	159	216	157	72	155	176	0	238	18	181	210	231	212	140
16	178	50	225	17	14	211	96	135	143	38	66	205	162	20	180

(Continued)

Table 6: Continued

27	206	107	128	121	61	240	24	164	192	179	31	102	202	119	142
194	198	75	91	30	182	226	71	22	111	97	255	93	137	55	12
120	58	248	103	4	134	105	95	167	92	32	104	54	153	195	148
224	229	106	233	67	94	168	169	2	193	44	213	130	221	127	250
112	6	170	173	23	89	86	83	152	208	200	154	47	175	207	149
236	10	11	117	244	84	36	114	136	146	77	228	29	3	113	189
25	49	21	249	171	82	70	145	252	220	64	9	81	160	139	166

3.3 Pair of 8×8 *S-Boxes Over the Residue Class of GI*

Let $h = 19 + 50i, p = n(h) = 2861$, and $\beta = 1 + 7i$, then apply a similar process like 3.2 and 3.3, then get a pair of S-boxes over the residue class of GI in Tables 7 and 8.

Table 7: $C = 8 \times 8$ S-box for the real part of GI

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

Table 8: $D = 8 \times 8$ S-box for the imaginary part of GI

80	35	193	46	83	108	212	88	240	105	14	228	49	196	103	38
101	24	213	8	54	90	159	183	60	178	167	69	231	229	19	161
162	171	180	43	220	7	120	154	147	22	18	15	203	106	44	216
242	217	181	152	138	65	53	185	78	151	211	157	117	109	191	205
72	122	89	133	11	234	61	253	143	199	136	146	56	98	30	12
92	112	94	201	135	52	192	137	165	248	150	75	236	223	68	119

(Continued)

Table 8: Continued

96	197	115	177	21	97	13	95	186	221	81	17	62	166	29	190
184	249	73	163	64	194	169	224	59	174	172	93	113	232	41	58
2	164	241	155	254	139	144	127	235	87	244	158	36	227	145	247
129	6	107	218	173	110	111	63	51	28	116	33	208	170	9	128
210	23	67	245	230	26	141	148	188	214	4	131	76	238	66	27
182	149	250	42	77	91	255	121	71	142	82	246	126	226	50	189
243	123	25	153	206	31	132	34	118	79	16	251	204	160	252	202
102	222	156	47	176	124	57	37	134	195	84	140	70	45	99	100
0	48	215	237	239	114	125	55	168	175	39	5	198	187	200	40
32	1	10	74	225	207	104	209	85	3	179	20	219	233	130	86

3.4 Inverse S-Boxes

The S-boxes A, B, C, and D in 3.2, and 3.3 are invertible and bijective. The procedure of inverse S-boxes over the residue class of GI is defined by applying inverse permutation through the following affine mapping $h(x) = (cx + d)\ (mod\ 2^n)$, where c is the multiplicative inverse of a under modulo 2^n and d is the additive inverse of cb under modulo 2^n.

The Inverse S-box of A is defined by the map, $h_1(x) = (45x + 232)\ (mod\ 256)$ in Table 9.

Table 9: $E =$ Inverse S-box of A

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

The inverse S-box of B is defined by the map, $h_2(x) = (45x + 21)\ (mod\ 256)$ in Table 10.

The inverse S-box of C for the real part of GI is given in Table 11.

The inverse S-box of D for the imaginary parts of GI is given in Table 12.

Table 10: $F =$ Inverse S-box of B

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

Table 11: $G =$ Inverse S-box of C

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

Table 12: H = Inverse S-box of D

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

4 Analysis of S-Boxes

In this section, we will present some useful analyses of the proposed S-box like as; Nonlinearity, bit independence criterion, strict avalanche criterion, linear approximation probability, and differential approximation probability.

4.1 Nonlinearity (NL)

The NL of a Boolean function can be defined as the distance between the function and the set of all affine functions. In other words, we can say that; Non-linearity is the number of bits that must be changed in the truth table of a Boolean function to reach the closest affine function. The upper bound of NL for the S-box is $\boldsymbol{N(f) = 2^{n-1} - 2^{\frac{n}{2}-1}}$ [18]. The optimal value of the NL of the S-box is 120. The NL results of the proposed $\mathbf{8 \times 8}$ S-boxes $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, and $\boldsymbol{D}$ are given in Table 13.

Table 13: Nonlinearity of 8 × 8 proposed S-boxes

Primes	Proposed S-boxes	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	Average
3917	A	108	108	108	108	108	108	106	106	107.50
	B	108	108	104	106	104	106	108	108	106.50
2861	C	108	106	104	108	108	108	106	106	106.75
	D	108	106	106	106	108	108	106	106	106.75

The maximum nonlinearity of all proposed S-boxes A, B, C, and D is 108. The minimum nonlinearity of proposed S-boxes A, B, C, and D are 106, 104, 104, and 106. The average nonlinearity of proposed S-boxes A, B, C, and D are 107.5, 106.5, 106.75, and 106.75.

4.2 Bit Independence Criterion (BIC)

The output BIC was also first introduced by Webster and Tavares, which is explained in [18], which is another desirable property for any cryptographic design. It means that all the avalanche variables should be pair-wise independent for a given set of avalanche vectors generated by the complementing of a single plaintext bit. The average value of BIC is $\frac{1}{2}$. The BIC analysis with the pair of proposed S-boxes ***A***, and ***B*** are given in Tables 14 and 15. The BIC of the proposed S-boxes generated by GI is up to the standard in the sense of encryption strength.

Table 14: BIC of proposed S-box A

…..	0.50390625	0.5	0.50390625	0.515625	0.50390625	0.498046875	0.4765625
0.50390625	…..	0.513671875	0.49609375	0.484375	0.50390625	0.51171875	0.48828125
0.5	0.513671875	…..	0.501953125	0.521484375	0.49609375	0.509765625	0.490234375
0.50390625	0.49609375	0.501953125	…..	0.4921875	0.5078125	0.48828125	0.515625
0.515625	0.484375	0.521484375	0.4921875	…..	0.52734375	0.490234375	0.513671875
0.50390625	0.50390625	0.49609375	0.5078125	0.52734375	…..	0.53515625	0.49609375
0.498046875	0.51171875	0.509765625	0.48828125	0.490234375	0.53515625	…..	0.505859375
0.4765625	0.48828125	0.490234375	0.515625	0.513671875	0.49609375	0.505859375	…..

Table 15: BIC of proposed S-box B

…..	0.53125	0.521484375	0.513671875	0.52734375	0.50390625	0.486328125	0.505859375
0.53125	…..	0.515625	0.5	0.494140625	0.513671875	0.4765625	0.51171875]
0.521484375	0.515625	…..	0.505859375	0.46484375	0.494140625	0.50390625	0.482421875
0.513671875	0.5	0.505859375	…..	0.501953125	0.5	0.5078125	0.4921875
0.52734375	0.494140625	0.46484375	0.501953125	…..	0.478515625	0.494140625	0.505859375
0.50390625	0.513671875	0.494140625	0.5	0.478515625	…..	0.5	0.486328125
0.486328125	0.4765625	0.50390625	0.5078125	0.494140625	0.5	…..	0.51953125
0.505859375	0.51171875	0.482421875	0.4921875	0.505859375	0.486328125	0.51953125	…..

The maximum (Max), average (Ave), and minimum (Min) BIC values of proposed S-boxes (A, B, C, and D) are (0.625, 0.609, 0.609, and 0.578), (0.047, 0.47, 0.47, and 0.47), and (0.375, 0.375, 0.375, and 0.391). The DAP comparison of proposed S-boxes with S-boxes on EC from the literature are given in the comparison section.

4.3 Linear Approximation Probability (LAP)

LAP is the maximum value of the imbalance of an event. The parity of the input bits selected by the mask $\boldsymbol{\Gamma u}$ is equal to the parity of the output bits selected by the mask $\boldsymbol{\Gamma v}$. According to Matsui's original definition, linear approximation probability (or probability of bias) of a given s-box is defined in [18];

$$LP = \max_{\Gamma u,\, \Gamma v = 0} \left| \frac{\#\{u\colon u.\Gamma u = S(u)\,.\,\Gamma v}{2^n} - \frac{1}{2} \right|$$

where, Γu and Γv are input and output masks, respectively; X is the set of all possible inputs and 2^n is the number of its elements. We have calculated the linear approximation probability of proposed S-boxes. We will compare it with some well-known S-boxes in Comparison Table 22. The maximum values of LAP of proposed S-boxes are given in Table 16, which are not so bad against linear attacks.

Table 16: LAP of proposed S-boxes

Primes	Proposed S-boxes	LAP values
3917	*A*	0.1328125
	B	0.140625
2861	*C*	0.1328125
	D	0.1328125

4.4 *Differential Approximation Probability (DAP)*

The nonlinear transformation S-box should ideally have differential uniformity. An input differential $\boldsymbol{\Delta u_i}$ should uniquely map to an output differential $\boldsymbol{\Delta v_i}$, thereby ensuring a uniform mapping probability for each $\boldsymbol{i}$. The differential approximation probability DAP of a given S-box is a measure of differential uniformity and is defined as

$$DP^s(\Delta u \rightarrow \Delta v) = \left[\frac{\#\{u \in X\colon S(u) \oplus S(u \oplus \Delta u) = \Delta v\}}{2^m} \right]$$

The DAP results of proposed S-boxes A and B are given in Tables 17 and 18.

Table 17: DAP of proposed S-box A

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0.023	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	0.016	0.023
0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.016	0.023	0.023	0.023
0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.031	0.023	0.031
0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.031	0.023
0.031	0.023	0.031	0.023	0.031	0.023	0.023	0.023	0.031	0.031	0.023	0.039	0.023	0.023	0.023	0.023
0.031	0.023	0.023	0.031	0.023	0.023	0.023	0.031	0.016	0.047	0.031	0.023	0.023	0.023	0.023	0.023
0.023	0.023	0.023	0.031	0.031	0.039	0.023	0.031	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023
0.031	0.039	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.031	0.031	0.023
0.023	0.039	0.023	0.023	0.023	0.023	0.023	0.031	0.016	0.023	0.023	0.023	0.023	0.023	0.023	0.023
0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.031	0.039	0.023	0.023
0.031	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.031	0.031	0.016
0.023	0.023	0.023	0.039	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.023	0.016	0.023	0.023
0.023	0.031	0.023	0.016	0.023	0.031	0.023	0.031	0.023	0.031	0.023	0.031	0.023	0.023	0.031	0.031
0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.039	0.023	0.023	0.031	0.023

(Continued)

Table 17: Continued

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0.023	0.031	0.031	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
0.023	0.031	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.023	0.023	0.031	0

Table 18: DAP of proposed S-box B

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0.031	0.031	0.023	0.039	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.031	0.023
0.031	0.023	0.031	0.023	0.023	0.023	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	0.023	0.023	0.023	0.031	0.031	0.031	0.023	0.039	0.023	0.031	0.031	0.023	0.031
0.023	0.023	0.031	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023
0.039	0.023	0.016	0.023	0.031	0.023	0.023	0.023	0.023	0.031	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	0.023	0.023	0.031	0.023	0.031	0.023	0.023	0.031	0.023
0.023	0.023	0.031	0.023	0.023	0.031	0.031	0.023	0.031	0.039	0.023	0.023	0.023	0.031	0.031	0.031
0.023	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	0.031	0.031
0.039	0.023	0.031	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.023
0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.031	0.023
0.039	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.039	0.023	0.031	0.031	0.031	0.031
0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.039	0.023	0.023	0.031	0.031	0.023	0.031	0.031
0.031	0.023	0.023	0.023	0.031	0.031	0.039	0.023	0.023	0.031	0.031	0.016	0.023	0.023	0.023	0.031
0.023	0.023	0.039	0.031	0.016	0.031	0.023	0.023	0.031	0.023	0.039	0.031	0.031	0.023	0.023	0.031
0.031	0.023	0.023	0.047	0.031	0.023	0.039	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	0.023	0.023	0.023	0.039	0.023	0.031	0.023	0.031	0.023	0.023	0.023	0

The Max. DAP values of proposed S-boxes A, B, C, and D are 0.047, 0.47, 0.47, and 0.47. The DAP comparison of proposed S-boxes with S-boxes on EC from the literature are given in the comparison section.

4.5 *Strict Avalanche Criterion (SAC)*

An S-box satisfies SAC if a single bit changes on the input results in a change on half of the output bits. Note that when S-box is used to build an S-P network, then a single change on the input of the network causes an avalanche of changes. The SAC results of the proposed S-boxes $\boldsymbol{A}$ and $\boldsymbol{B}$ are given in Tables 19 and 20. We have come to a close that the value of the proposed S-boxes is approximately equal to $\frac{1}{2}$. So, we conclude that we can make use of proposed S-boxes in block cipher for secure communication.

The Max SAC values of proposed S-boxes A, B, C, and D are 0.594, 0.594, 0.594, and 0.594. The minimum SAC values of the proposed S-boxes A, B, C, and D are 0.406, 0.406, 0.406, and 0.422. The average SAC values of the proposed S-boxes A, B, C, and D are 0.5, 0.5, 0.5, and 0.508. Hence, we conclude that the proposed S-boxes satisfied the SAC close to the optimal possible value.

Table 19: SAC of proposed S-box A

0.53125	0.453125	0.5	0.421875	0.484375	0.59375	0.484375	0.5625
0.53125	0.53125	0.484375	0.484375	0.53125	0.53125	0.4375	0.484375
0.515625	0.484375	0.515625	0.484375	0.515625	0.546875	0.515625	0.46875
0.5	0.5625	0.484375	0.515625	0.53125	0.484375	0.515625	0.484375
0.5	0.5625	0.515625	0.53125	0.5625	0.484375	0.515625	0.453125
0.484375	0.46875	0.484375	0.46875	0.515625	0.5625	0.5	0.546875
0.40625	0.46875	0.453125	0.5	0.546875	0.53125	0.546875	0.515625
0.453125	0.515625	0.5625	0.484375	0.578125	0.5	0.546875	0.484375

Table 20: SAC of proposed S-box B

0.46875	0.5	0.515625	0.5	0.5	0.515625	0.53125	0.53125
0.453125	0.53125	0.53125	0.5	0.46875	0.46875	0.53125	0.5625
0.515625	0.46875	0.4375	0.53125	0.5625	0.453125	0.5	0.515625
0.515625	0.515625	0.59375	0.40625	0.484375	0.4375	0.578125	0.5625
0.53125	0.5	0.421875	0.53125	0.515625	0.484375	0.5	0.484375
0.515625	0.5	0.484375	0.46875	0.53125	0.4375	0.515625	0.453125
0.484375	0.546875	0.5	0.53125	0.4375	0.453125	0.515625	0.4375
0.5	0.53125	0.5	0.453125	0.515625	0.5625	0.453125	0.40625

5 Comparison

The former tests are applied on well-known S-boxes over EC presented in [19,20] to compare with the proposed S-boxes A, B, C, and D over GI. The analysis of EC and GI for the same primes with different parameters is presented in Table 21, and Figs. 1–5.

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

$S-boxes$	$Primes$	$Type$	NL	LAP	DAP	$SAC\ Max$	$SAC\ Ave$	$SAC\ Min$	$BIC Max$	$BIC\ Ave$	$BIC Min$
A	3917	GI	107.5	0.133	0.047	0.594	0.5	0.406	0.625	0.5	0.375
B	3917	GI	106.5	0.141	0.047	0.594	0.5	0.406	0.609	0.492	0.375
C	2861	GI	106.75	0.133	0.047	0.594	0.5	0.406	0.609	0.492	0.375
D	2861	GI	106.75	0.133	0.047	0.594	0.508	0.422	0.578	0.4845	0.391
[19]	3917	EC	104.0	0.148	0.047	0.610	0.516	0.422	0.543	0.503	0.463
[20]	2861	EC	104.0	0.148	0.039	0.625	0.508	0.391	0.531	0.501	0.471

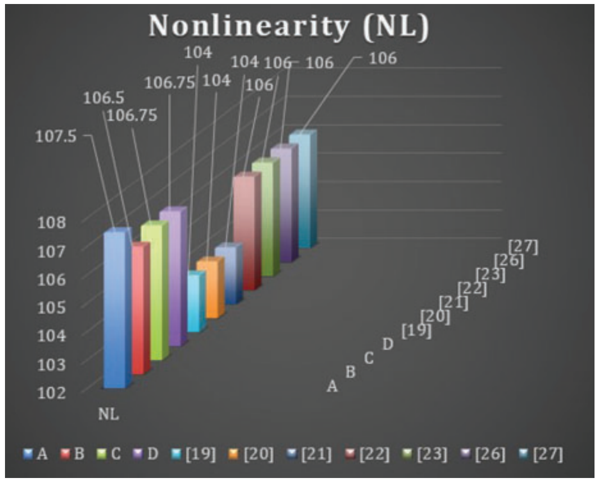

Figure 1: Nonlinearity

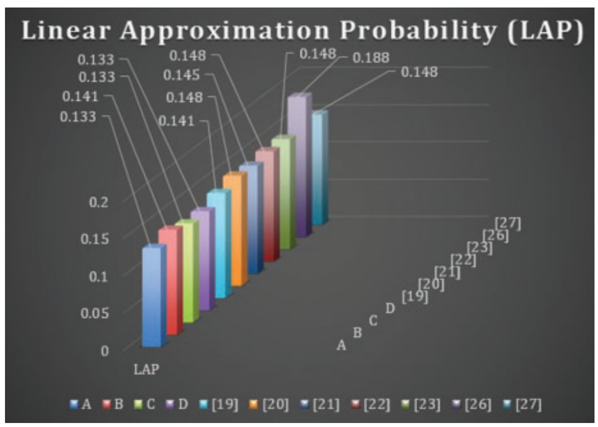

Figure 2: Linear approximation probability

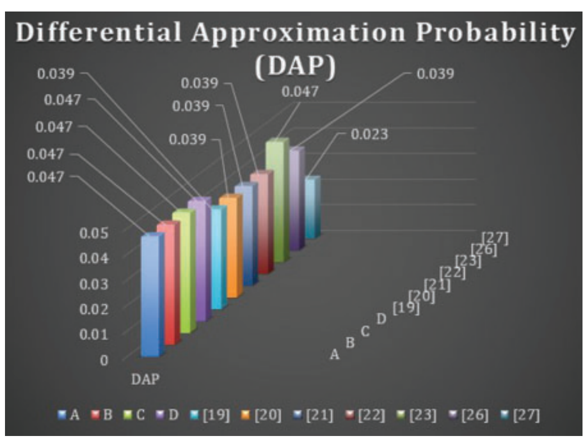

Figure 3: Differential approximation probability

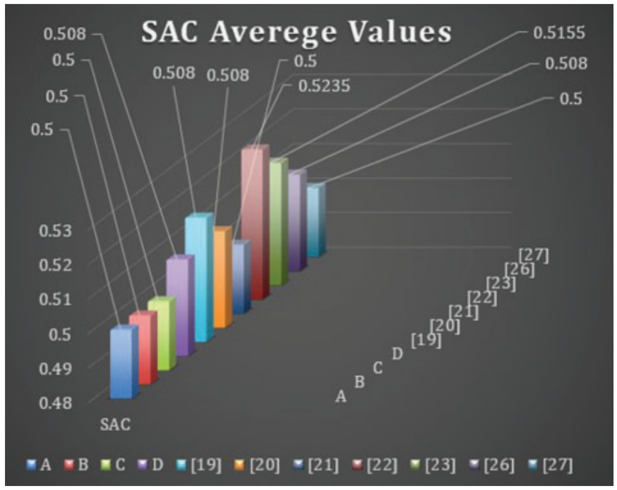

Figure 4: SAC average values

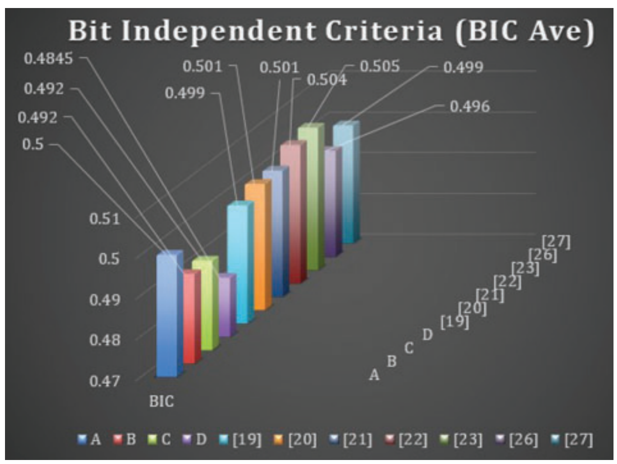

Figure 5: Bit independent criteria

Similarly, the comparison of S-boxes over EC presented in [19–27] with the proposed S-boxes A, B, C, and D over GI by some tests of S-boxes. The analysis of EC and GI for different primes with different parameters is presented in Table 22, and Figs. 1–5.

Table 22: Proposed S-boxes comparison with EC S-boxes for different primes

$S-boxes$	$Primes$	$Type$	NL	LAP	DAP	$SAC\ Max$	$SAC\ Ave$	$SAC\ Min$	$BICMax$	$BIC\ Ave$	$BICMin$
A	3917	GI	107.50	0.133	0.047	0.594	0.5	0.406	0.625	0.5	0.375
B	3917	GI	106.50	0.141	0.047	0.594	0.5	0.406	0.609	0.492	0.375
C	2861	GI	106.75	0.133	0.047	0.594	0.5	0.406	0.609	0.492	0.375
D	2861	GI	106.75	0.133	0.047	0.594	0.508	0.422	0.578	0.4845	0.391
[19]	9551	EC	104.00	0.141	0.039	0.610	0.508	0.406	0.525	0.499	0.473
[21]	2851	EC	104.00	0.145	0.039	0.610	0.5	0.390	0.531	0.501	0.471

(Continued)

Table 22: Continued

$S-boxes$	$Primes$	$Type$	NL	LAP	DAP	$SAC\ Max$	$SAC\ Ave$	$SAC\ Min$	$BIC Max$	$BIC\ Ave$	$BIC Min$
[22]	3299	EC	106.00	0.148	0.039	0.641	0.5235	0.406	0.537	0.504	0.471
[23]	4177	EC	106.00	0.148	0.047	0.625	0.5155	0.406	0.539	0.505	0.471
[26]	3917	EC	106.00	0.188	0.039	0.610	0.508	0.406	0.527	0.496	0.465
[27]	1607	EC	106.00	0.148	0.023	0.609	0.5	0.391	0.525	0.499	0.473

It is observed that the value of nonlinearity of the proposed S-boxes is better than with EC S-boxes. The fascinating features of the proposed technique by using affine mapping provide S-boxes pair at a time by fixing three parameters a, b, and p. But the prime field dependent on the EC by different techniques provides one S-box at a time by fixing three parameters a, b, and p. The nonlinearity of the proposed S-boxes is given in Table 22, and Figs. 1–5. The LAP results of the proposed S-boxes are less than the S-boxes presented in [19–27] This fact reveals that the proposed S-boxes create high confusion in the data and higher resistance against linear attack [24] as compared to [19–27]. The SAC and BIC results of proposed S-boxes are comparable with other S-boxes used in Tables 21, 22, and Figs. 1–5. Thus, the S-box generated by the proposed technique and S-boxes presented in Tables 21, 22, and Figs. 1–5 create diffusion in the data of equal magnitude. The DAP of proposed S-boxes is comparable to the DAP of S-boxes in [19–27]. Thus, the proposed technique generates S-box with high resistance against differential cryptanalysis [25] as compared to the others. The analysis results of newly generated paired S-boxes by the cyclic group of GI are listed in Tables 21, 22, and Figs. 1–5. It is evident from Tables 21, 22, and Figs. 1–5 that the performance of paired S-boxes by the cyclic group over GI is comparable with the S-boxes over EC.

6 Conclusion and Future Directions

A novel S-box construction technique is presented in this article. The fascinating features of the proposed technique by using affine mapping provide S-boxes pair at a time by fixing three parameters a, b, and p. But the prime field dependent on the EC by different techniques provides one S-box at a time by fixing three parameters a, b, and p. For the generation of cryptographically strong proposed S-boxes prime p which is greater than or equal to 257 and a, b belongs to the cyclic group over the residue class of Gaussian integers. Several tests are applied to the newly proposed S-boxes and analyze their cryptographic strength. Furthermore, the cryptographic properties of proposed S-boxes are compared with some of the existing prevailing S-boxes over EC. Experimental results showed that the proposed algorithm is capable of generating paired S-boxes with high resistance against linear and differential attacks.

The proposed S-boxes over the residue class of GI can be extended to the S-boxes over the residue class of quaternion and octonion integers. Furthermore, we can use these structures in watermarking and image encryption.

Funding Statement: The third author is supported by Minciencias Convocatoria 891.

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, no. 2, 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] I. Shahzad, Q. Mushtaq and A. Razaq, "Construction of new S-box using action of quotient of the modular group for multimedia security," *Security and Communication Networks*, vol. 19, no. 1, pp. 1–13, 2019.

[7] T. Shah and A. Qureshi, "S-box on subgroup of galois field," *Cryptography*, vol. 3, no. 2, pp. 1–9, 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] I. Hussain, T. Shah, M. A. Gondal and H. Mahmood, "A novel image encryption algorithm based on chaotic maps and GF (28) exponent transformation," *Nonlinear Dynamics*, vol. 72, no. 1, pp. 399–406, 2013.

[12] U. Hayat, N. A. Azam and M. Asif, "A method of generating 8×8 substitution boxes based on elliptic curves," *Wireless Personal Communications*, vol. 101, no. 1, pp. 439–451, 2018.

[13] A. Javeed, T. Shah and A. Ullah, "Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group," *Wireless Personal Communications*, vol. 112, no. 1, pp. 467–480, 2020.

[14] 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.

[15] G. Davidoff, P. Sarnak and A. Valette, "Elementary number theory, group theory, and ramanujan graphs," *Cambridge University Press*, vol. 55, no. 1, pp. 45–80, 2003.

[16] K. Conrad, "The Gaussian integers," *Preprint, Paper Edition*, vol. 10, no. 2, pp. 1–13, 2018.

[17] K. Huber, "Codes over Gaussian integers," *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 207–216, 1994.

[18] M. I. Haider, A. Ali, D. Shah and T. Shah, "Block cipher's nonlinear component design by elliptic curves: An image encryption application," *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 4693–4718, 2021.

[19] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, no. 1, pp. 391–402, 2019.

[20] G. Dresden and W. M. Dymàčcek, "Finding factors of factor rings over the Gaussian integers," *The American Mathematical Monthly*, vol. 112, no. 7, pp. 602–611, 2005.

[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, 2021.

[22] N. A. Azam, U. Hayat and I. Ullah, "Efficient construction of a substitution box based on a mordell elliptic curve over a finite field," *Frontiers of Information Technology & Electronic Engineering*, vol. 20, no. 10, pp. 1378–1389, 2019.

[23] U. Hayat, N. A. Azam, H. R. G. Ruiz, S. Naz and L. Batool, “A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings,” *Arabian Journal for Science and Engineering*, vol. 46, no. 9, pp. 8887–8899, 2021.
[24] B. Collard and F. X. Standaert., “Experimenting linear cryptanalysis,” in *Advanced Linear Cryptanalysis of Block and Stream Ciphers*, 1st ed., vol. 1. Du Levant 3, B-1348, Louvain-la-Neuve, Belgium: IOS Press, pp. 1–28, 2011.
[25] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.
[26] N. A. Azam, U. Hayat and I. Ullah, “An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization,” *Security and Communication Networks*, vol. 80, no. 3, pp. 220–229, 2018.
[27] I. Ullah, U. Hayat and M. D. Bustamante, “Image encryption using elliptic curves and rossby/drift wave triads,” *Entropy*, vol. 22, no. 4, pp. 454–473, 2020.