AIMS Mathematics, 8(9): 21089–21105.
DOI: 10.3934/math.20231074
Received: 19 May 2023
Revised: 23 June 2023
Accepted: 23 June 2023
Published: 03 July 2023

http://www.aimspress.com/journal/Math

Research article

Designing pair of nonlinear components of a block cipher over quaternion integers

Muhammad Sajjad[1,*], Tariq Shah[1], Huda Alsaud[2] and Maha Alammari[2]

[1] Department of Mathematics, Quaid-I-Azam University, Islamabad 45320, Pakistan
[2] Department of Mathematics, College of Science, King Saud University, P.O. Box 22452 Riyadh 11495, Saudi Arabia

* **Correspondence:** Email: m.sajjad@math.qau.edu.pk; Tel: +923067759056.

Abstract: In the field of cryptography, block ciphers are widely used to provide confidentiality and integrity of data. One of the key components of a block cipher is its nonlinear substitution function. In this paper, we propose a new design methodology for the nonlinear substitution function of a block cipher, based on the use of Quaternion integers (QI). Quaternions are an extension of complex numbers that allow for more complex arithmetic operations, which can enhance the security of the cipher. We demonstrate the effectiveness of our proposed design by implementing it in a block cipher and conducting extensive security analysis. Quaternion integers give pair of substitution boxes (S-boxes) after fixing parameters but other structures give only one S-box after fixing parameters. Our results show that the proposed design provides superior security compared to existing designs, two making on a promising approach for future cryptographic applications.

Keywords: quaternion integers; residue class; block cipher; security analysis
Mathematics Subject Classification: 68P25, 68U15

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].

Substitution boxes, also known as S-boxes, are a key component of modern cryptographic algorithms. Shannon suggested the notion of an S-box in 1949 [2]. S-boxes are used to replace one group of bits with another group of bits to provide confusion and non-linearity in the encryption process. The substitution boxes are designed to make it difficult for attackers to determine the relationship between the input and output of the encryption algorithm. This makes it harder for attackers to crack the encryption, providing increased security for sensitive data. S-boxes have been used in a wide range of cryptographic algorithms, including the Advanced Encryption Standard (AES), the Data Encryption Standard (DES), and the Blowfish encryption algorithm. The design of S-boxes is critical to the security of these algorithms, and much research has been done to create S-boxes that are resistant to attacks. The design of S-boxes typically involves a combination of mathematical analysis, computational complexity, and heuristics to produce a strong S-box that is difficult to break. One of the key properties of S-boxes is their non-linearity. Non-linearity ensures that small changes in the input produce large changes in the output, making it difficult for attackers to determine the relationship between the input and output of the encryption algorithm. This nonlinearity is achieved through careful design of the S-box, often involving complex mathematical functions that ensure that the output is as different as possible from the input. The security of S-boxes has been the subject of much research, with many attacks developed over the years to break them. One of the most famous attacks on S-boxes is the differential cryptanalysis attack, which was developed in the 1990s. This attack involves analyzing the differences between pairs of inputs to the S-box and the corresponding differences in the output. By analyzing these differences, attackers can learn more about the S-box and potentially break the encryption [3–5].

Many scholars employed diverse algebraic and statistical frameworks to confound data and produce S-boxes. In [6], the authors suggested S-boxes over the permutation of the symmetric group. Javeed and Shah utilized a chaotic dynamical system and symmetric group to construct the non-linear component of a block cipher [7]. Meanwhile, the authors of [8] described an S-box constructed using the subgroup of the Galois field. In [9], the authors proposed a dynamic S-box using novel chaotic map. In [10], a new scheme for constructing S-boxes was presented based on the linear fractional transformation and permutation function. The Mobius group and finite field were used to construct an S-box in [11], while [12] proposed an S-box based on a nonlinear chaotic map. Sajjad and Shah designed a pair of nonlinear components of a block cipher over Gaussian integers in [13], and [14] presented fundamental results of cyclic codes and decoding algorithms over octonion integers. Differential cryptanalysis of DES-like cryptosystems was developed by the authors of [15], while Quiroga and Cantón proposed generating dynamical S-boxes for block ciphers using an extended logistic map in [16]. Tang and Liao designed a new method of dynamical S-boxes based on discretized chaotic maps [17]. While Chen and Liao extended this method to obtain S-boxes based on three-dimensional chaotic Baker maps [18]. A novel approach for strong S-Box generation algorithm design based on a chaotic scaled zhongtang system was presented by Çavuşoğlu and Zengin in [19]. Siddiqui and Naseer developed a novel scheme of substitution-box design based on modified Pascal's triangle

and elliptic curve [20]. Farhan and Ali designed a new S-box generation algorithm based on the multistability behavior of a plasma perturbation model [21]. In [22], the authors approached the S-boxes and permutation, substitution-based encryption. The authors constructed block ciphers based on chaotic maps in [23,24].

Quaternion integers are an extension of complex numbers that have gained significant attention in various fields of physics and engineering due to their unique properties. They are a type of hypercomplex number that can be used to describe rotations in 3D space and have applications in areas such as computer graphics, robotics, and quantum mechanics. The concept of quaternion integers was introduced by the Irish mathematician William Rowan Hamilton in 1843. He famously impressed the fundamental formula for quaternions onto a stone bridge in Dublin. Since then, quaternion algebra has been extensively studied, and its applications have been explored [25–27]. In [28], Ozen and Guzeltepe constructed cyclic codes over certain finite quaternion integer rings. Shah and Rasool presented codes over quaternion integers [29]. In [30], the authors constructed cyclic codes over quaternion integers and developed a decoding algorithm. These quaternion structures can be helpful for the construction of S-boxes.

This article presents a novel approach for designing a pair of nonlinear components for a block cipher over QI. Quaternions are an extension of complex numbers that allow for more complex arithmetic operations, which can enhance the security of the cipher. We demonstrate the effectiveness of our proposed design by implementing it in a block cipher and conducting extensive security analysis. Quaternion integers give pair of substitution boxes (S-boxes) after fixing parameters but other structures give only one S-box after fixing parameters. Our results show that the proposed design provides superior security compared to existing designs, two making a promising approach for future cryptographic applications.

The rest of this article is organized as follows. Section 2 provides an overview of the background and related work of quaternion integers. Section 3 presents our proposed design for a pair of nonlinear components, including a detailed description of the operations. 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

The important ideas and fundamental conclusions that will be employed in the analysis of subsequent sections are presented in this section. Prior to that, we should review the definition of quaternion integers, their addition and multiplication, their residue class, and other associated findings.

2.1. Quaternion integers

By following [28, Section 2], let $H(\mathbb{R})$ be the Hamilton Quaternion algebra over the real number $\mathbb{R}$ is the non-commutative but associative unital algebra if it satisfies the following conditions.

- $H(\mathbb{R}) = \{b_0 + b_1 i + b_2 j + b_3 k: b_0, b_1, b_2, b_3 \in \mathbb{R}\}$ is free $\mathbb{R}$ module.
- The multiplicative identity is 1.
- $i^2 = j^2 = k^2 = -1 \; and \; jk = -kj = i, ki = -ik = j, ij = -ji = k.$

The Quaternion integer ring $H(\mathbb{Z}) = \{b_0 + b_1 i + b_2 j + b_3 k: for\ all\ b_0, b_1, b_2, b_3 \in \mathbb{Z}\}$

contained in $H(\mathbb{R})$, where $\mathbb{Z}$ is the ring of integers. If $q = b_0 + b_1 i + b_2 j + b_3 k$ is a Quaternion integer, then $\bar{q} = b_0 - b_1 i - b_2 j - b_3 k$ is the Quaternion conjugate of q. Let $N(q) = q\bar{q} = b_0^2 + b_1^2 + b_2^2 + b_3^2$ be the norm of q. A Quaternion integer q has only two parts one is the scalar part (S.P) b_0 and the other is the vector part (V.P) $b_1 i + b_2 j + b_3 k$. In Quaternion integer's commutative property of multiplication does not hold. It is possible only in case of two vector parts of quaternion integers are parallel.

Define $H(K)$ as: $H(K) = \{a + bU : a, b \in \mathbb{Z}\}$, Where U is $(i + j + k)$. Hence $H(K)$ is a subring of the Quaternion integer ring $H(\mathbb{Z})$, and also the commutative property of multiplication holds over $H(K)$.

2.1.1. Sum and product of two quaternion integers

Let $q_1 = c_0 + c_1 i + c_2 j + c_3 k$ and $q_2 = d_0 + d_1 i + d_2 j + d_3 k$ be the two quaternion integers then, their sum $q_1 + q_2$ and product $q_1 q_2$ will be also a quaternion integer as;

$$q_1 + q_2 = (c_0 + c_1 i + c_2 j + c_3 k) + (d_0 + d_1 i + d_2 j + d_3 k)$$

$$= (c_0 + d_0) + (c_1 + d_1)i + (c_2 + d_2)j + (c_3 + d_3)k = e_0 + e_1 i + e_2 j + e_3 = q_3$$

$$q_1 q_2 = (c_0 + c_1 i + c_2 j + c_3 k)(d_0 + d_1 i + d_2 j + d_3 k)$$

$$= (c_0 d_0 + c_0 d_1 i + c_0 d_2 j + c_0 d_3 k + c_1 d_0 i - c_1 d_1 + c_1 d_2 k - c_1 d_3 j + c_2 d_0 j - c_2 d_1 k - c_2 d_2 + c_2 d_3 i + c_3 d_0 k + c_3 d_1 j - c_3 d_2 i - c_3 d_3)$$

$$= (c_0 d_0 - c_1 d_1 - c_2 d_2 - c_3 d_3) + (c_0 d_1 + c_1 d_0 + c_2 d_3 - c_3 d_2)i + (c_0 d_2 + c_2 d_0 + c_3 d_1 - c_1 d_3)j + (c_0 d_3 + c_3 d_0 + c_1 d_2 - c_2 d_1)k = g_0 + g_1 i + g_2 j + g_3 k = q_4$$

Theorem: In [28, Section 2], the set of natural numbers for each odd rational prime p, there is a prime $\delta \in H(\mathbb{Z})$, such that $N(\delta) = p = \delta\bar{\delta}$. In particular, p is not prime in $H(\mathbb{Z})$.
Theorem: In [29, Section 2], let $\delta \in H(\mathbb{Z})$ be prime in $H(\mathbb{Z})$ if and only if $N(\delta)$ be prime in $\mathbb{Z}$.

2.1.2. Residue class of quaternion integers

In [30, Section 2], let $H(K)_\delta$ be the residue class of $H(K)$ modulo δ, where $\delta = a + bU$. Then, the modulo function

$$\varphi : H(K) = \{a + bU : a, b \in \mathbb{Z}\} \to H(K)_\delta$$

$$\varphi(q) = z\ (mod\ \delta) = q - \left[\frac{q\bar{\delta}}{p}\right]\delta$$

Where $z \in H(K)_\delta$. The previous equation involves rounding the number of [.] to the nearest integer. To accomplish QI rounding, it is necessary to round the coefficient of the vector part (C.V.P) and scalar part (S.P) independently to the nearest integer.
Theorem: In [30, Section 2], let δ be a quaternion prime, and the number of quaternion integers modulo δ is the norm of δ. If $\alpha \neq 0(mod\ \delta)$, then $\alpha^{p-1} \equiv 1(mod\ \delta)$.
Remark: The group generated by $< \alpha >$ in the above Theorem is named G^*.

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

Multiple methods can be employed to cause confusion inside a security system. The S-box is a nonlinear component of a cryptographic algorithm. The S-boxes are generally formed by the QI class or the multiplicative cyclic group. As a result, it is feasible to create a variety of S-boxes across the residue class of QI, 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 QI as;

Step 1: Construct a cyclic group G^* of order $p-1$ over the residue class of QI.

Step 2: Apply permutation through affine mapping as $g(x) = (sx + t)(mod\ 2^n)$

Where $t \in G^*$ and s be the unit element of G^*.

Step 3: Separate real parts (R.P) and coefficients of the vector parts (C.V.P) of Step 2.

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

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

Step 6: Select the first 2^n non-repeated elements from the S.P and also select the first 2^n non-repeated elements from the C.V.P of Step 3.

Step 7: Get pair of nonlinear components of a block cipher.

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

3.1. Pair of 4×4 S-boxes over the residue class of quaternion integers

Let $\delta = 16 + i + j + k = (16,1,1,1)$, $p = N(\delta) = 16^2 + 1^2 + 1^2 + 1^2 = 259$, and $\beta = 5 + i + j + k = (5,1,1,1)$, then the cyclic group generated by β shown in Table 1.

Table 1. Cyclic group generated by β.

i	β^i	S.P	C.V.P (β^i)	(S.P (β^i))(mod 16)	(C.V.P(β^i))(mod 16)
1	$(5,1,1,1)$	5	1	5	1
2	$(9,-7,-7,-7)$	9	-7	9	9
3	$(6,8,8,8)$	6	8	6	8
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
258	$(1,0,0,0)$	1	0	1	0

Select the first 16 non-repeated elements from the last two columns of Table 1, then apply the affine permutation mapping, $f(x) = (4x + 1)(mod\ 16)$, and get the pair of S-boxes separately in Table 2 and 3.

Table 2. 4×4 S-box by the S.P of QI.

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

Table 3. 4×4 S-box by the C.V.P of QI.

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

3.2. Pair of 8×8 *S-boxes over the residue class of quaternion integers*

Let $\delta = 68 + 31i + 31j + 31k = (68, 31, 31, 31), p = N(\delta) = 7507,$ and $\beta = 1 + 17i + 17j + 17k = (1,17,17,17)$, then the cyclic group generated by β shown in Table 4;

Table 4. Cyclic group generated by β over QI.

i	β^i	$S.P(\beta^i)$	$C.V.P(\beta^i)$	(S.P(β^i))(mod 256)	(C.V.P(β^i))(mod 256)
1	$(1, 17, 17, 17)$	1	17	1	17
2	$(-48,14,14,1\ 4)$	-48	14	208	14
3	$(11, -3, -3, -3)$	11	-3	11	253
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
3916	(1,0,0,0)	1	0	1	0

Select the first 256 non-repeated elements from the real part of Table 4. Then apply the affine permutation map $g(x) = (121x + 166)(mod\ 256)$, and get the S- box from the scalar part of QI in Table 5.

Table 5. $A = 8 \times 8$ S-box by the S.P of QI.

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

Select the first 256 non-repeated elements from the imaginary part of Table 4. Then apply the affine permutation map $g(x) = (37x + 120)(mod\ 256),$ and get the S-box for the C.V.P of QI in Table 6.

Table 6. $B = 8 \times 8$ S-box by the C. V. P of QI.

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

3.3. Inverse S-boxes

The S-boxes A, and B in 3.1.2 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 $h(x) = (ux + v)(mod\ 2^n)$, where u is the multiplicative inverse of s under modulo 2^n and v is the additive inverse of ut under modulo 2^n.

The Inverse S-box of A is defined by the map, $h_1(x) = (201x + 143)(mod\ 256)$ in Table 7.

Table 7. $\boldsymbol{C}$ = 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, $h_2(x) = (173x + 24)(mod\ 256)$ in Table 8.

Table 8. $\boldsymbol{D}$ = 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

4. Analysis of S-boxes

The analysis of S-boxes is a crucial part of cryptanalysis, ensuring the security of encrypted data. Nonlinearity, output distribution, and resistance to attacks are all important aspects of S-box design, and their analysis requires mathematical and statistical tools to measure their effectiveness [31-40]. There is the following analysis.

4.1. Nonlinearity

Nonlinearity (NL) is a fundamental property of many natural and artificial systems, and it describes the behavior of a system that is not proportional to its inputs. In other words, small changes in inputs may lead to significant changes in outputs, and the relationship between input and output is not a straight line. Nonlinearity is observed in a wide range of phenomena, such as fluid dynamics, electrical circuits, and signal processing. Nonlinear systems can exhibit complex behavior, including chaotic dynamics, oscillations, and bifurcations, and they are often more difficult to analyze and control than linear systems. Nonlinearity is a critical concept in many fields, including physics, engineering, economics, and biology, and it plays a crucial role in understanding the behavior of complex systems and designing effective control strategies. The upper bound of NL for the S-box is $N(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ [26]. The optimal value of the NL of the S-box is 120. The NL results of the proposed 8×8 S- boxes A, and B are given in Table 9.

Table 9. 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
7507	A	108	108	106	108	106	106	108	106	107.00
	B	108	108	106	108	106	106	108	106	107.00

The proposed S-boxes A and B exhibit a maximum nonlinearity of 108, as well as a minimum nonlinearity of 106. Additionally, the average nonlinearity of both S-boxes A and B is calculated to be 107.00.

4.2. Bit independent criterion

The bit-independent criterion (BIC) is a measure used in cryptanalysis to evaluate the security of substitution boxes, or S-boxes, used in block ciphers. The criterion is designed to assess the strength of an S-box against differential cryptanalysis, which is a type of attack used by cryptanalysts to recover the key used in encryption. The bit-independent criterion measures the ability of an S-box to satisfy certain properties that make it resistant to differential cryptanalysis. Specifically, the criterion evaluates whether the S-box is balanced, has high nonlinearity, and is immune to linear attacks. A balanced S-box ensures that for any input, there is an equal number of output bits with a value of 1 and 0. High nonlinearity ensures that small changes in input bits result in significant changes in output bits, making it difficult for attackers to deduce the key used in encryption. Finally, immunity to linear attacks ensures that the S-box cannot be easily broken using linear equations. To evaluate an S-box using the bit-independent criterion, a differential characteristic is chosen, and the expected value of the characteristic is computed. Next, the number of pairs of inputs that satisfy the differential characteristic is counted, and the difference between this value and the expected value is measured. If this difference is close to zero, the S-box is said to satisfy the bit-independent criterion [26]. 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 10 and 11. The BIC of the proposed S-boxes generated by QI is up to the standard in the sense of encryption strength.

Table 10. BIC of S-box A.

0.0	0.484375	0.5	0.49609375	0.521484375	0.501953125	0.5	0.490234375
0.484375	0.0	0.51953125	0.48828125	0.51953125	0.505859375	0.509765625	0.4921875
0.5	0.51953125	0.0	0.501953125	0.521484375	0.50390625	0.533203125	0.494140625
0.49609375	0.48828125	0.501953125	0.0	0.494140625	0.505859375	0.50390625	0.494140625
0.521484375	0.51953125	0.521484375	0.494140625	0.0	0.53125	0.513671875	0.50390625
0.501953125	0.505859375	0.50390625	0.505859375	0.53125	0.0	0.51953125	0.5
0.5	0.509765625	0.533203125	0.50390625	0.513671875	0.51953125	0.0	0.501953125
0.490234375	0.4921875	0.494140625	0.494140625	0.50390625	0.5	0.501953125	0.0

Table 11. BIC of S-box B.

0.0	0.484375	0.5	0.49609375	0.521484375	0.501953125	0.5	0.490234375
0.484375	0.0	0.51953125	0.48828125	0.51953125	0.505859375	0.509765625	0.4921875
0.5	0.51953125	0.0	0.501953125	0.521484375	0.50390625	0.533203125	0.494140625
0.49609375	0.48828125	0.501953125	0.0	0.494140625	0.505859375	0.50390625	0.494140625
0.521484375	0.51953125	0.521484375	0.494140625	0.0	0.53125	0.513671875	0.50390625
0.501953125	0.505859375	0.50390625	0.505859375	0.53125	0.0	0.51953125	0.5
0.5	0.509765625	0.533203125	0.50390625	0.513671875	0.51953125	0.0	0.501953125
0.490234375	0.4921875	0.494140625	0.494140625	0.50390625	0.5	0.501953125	0.0

The proposed S-boxes (A, B) have been evaluated using the bit-independent criterion (BIC), which measures the S-box's resistance to differential cryptanalysis. The BIC values of the S-boxes have been calculated as follows: the maximum BIC value for both S-boxes A and B is 0.6094, while the minimum BIC value for both is 0.375. The average BIC value for both S-boxes A and B is 0.5054.

4.3. Linear approximation probability

Linear approximation probability (LAP) is a measure used in cryptanalysis to evaluate the security of substitution boxes, or S-boxes, used in block ciphers. The measure evaluates the probability of a linear approximation of an S-box being satisfied, where the linear approximation is a linear equation that approximates the behavior of the S-box. Linear approximation probability is based on the idea that a good S-box should not be easily modeled using linear equations. If an S-box can be modeled using a linear equation, it is vulnerable to linear attacks, where an attacker can use the linear equation to recover the key used in encryption. To evaluate the linear approximation probability of an S-box, a linear approximation is chosen, and the expected value of the linear approximation is computed. Next, the number of pairs of inputs that satisfy the linear approximation is counted, and the difference between this value and the expected value is measured. If this difference is close to zero, the S-box is said to have a low linear approximation probability and is considered to be resistant to linear attacks. The linear approximation probability of an S-box is closely related to its nonlinearity, which is another measure used to evaluate the security of S-boxes. A high nonlinearity implies a low linear approximation probability, and vice versa. However, nonlinearity measures the S-box's resistance to all types of attacks, while linear approximation probability focuses specifically on linear attacks [26]. The maximum values of LAP of proposed S-boxes are given in Table 12, which are not so bad against linear attacks.

Table 12. LAP of S-boxes over QI.

Primes	Proposed S-boxes	LAP values
3917	A	0.1328125
	B	0.1328125

4.4. Differential approximation probability

The proposed S-boxes have been evaluated using differential approximation probability (DAP), which is a measure used in cryptanalysis to evaluate the security of substitution boxes (S-boxes) against differential attacks. The DAP value of an S-box measures the probability of a differential approximation of the S-box being satisfied. In the case of the proposed S-boxes, the DAP values were computed by selecting a differential approximation and counting the number of input-output pairs that satisfy the differential approximation. This count was then divided by the total number of possible input-output pairs, giving the DAP value. The DAP values of the proposed S-boxes were compared with those of existing S-boxes from the literature. The results showed that the proposed S-boxes have a lower DAP value than some existing S-boxes, indicating that they are more resistant to differential attacks. The DAP results of proposed S-boxes A and B are given in Tables 13 and 14.

Table 13. DAP of S-box A.

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

Table 14. DAP of S-box B.

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

The maximum DAP values of the proposed S-boxes A and B are 0.039. The comparison of the DAP values of the proposed S-boxes with the S-boxes on different structures from the literature is presented in the comparison section.

4.5. Strict avalanche criterion

The strict avalanche criterion (SAC) is an important concept in the field of cryptography and information theory. It is a mathematical property that measures the sensitivity of a cryptographic function to small changes in the input. In other words, it determines how much the output of the function changes when a single bit of the input is flipped. The SAC is a fundamental requirement for the security of cryptographic algorithms. A function that satisfies the SAC is said to be an "avalanche effect" because the output of the function changes drastically (like an avalanche) when the input is changed even slightly. This means that an attacker cannot predict the output of the function even if they know a small part of the input. The SAC is typically measured using a metric called the "avalanche distance," which is the proportion of output bits that change when a single input bit is flipped. A function that satisfies the SAC should have an avalanche distance of at least 50% (i.e., half of the output bits should change when a single input bit is flipped). This ensures that the function is highly sensitive to input changes and provides a high level of security. There are several techniques for evaluating the SAC of a cryptographic function, including statistical testing and algebraic analysis. These techniques are used to ensure that the function meets the strict avalanche criterion and is secure against attacks. The SAC results of the proposed S-boxes A and B are given in Tables 15 and 16. 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.

Table 15. SAC of S-box A.

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

Table 16. SAC of S-box B.

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

The proposed S-boxes A and B have maximum Strict Avalanche Criterion (SAC) values of 0.594 each, and minimum SAC values of 0.406 each. On average, the SAC values of S-boxes A and B are 0.504 each. These results indicate that the proposed S-boxes are very close to achieving the optimal possible SAC value. Therefore, we can conclude that the SAC of the proposed S-boxes meets the required criteria.

5. Comparison

The former tests are performed on well-known S-boxes over EC, chaotic maps, etc presented in [18–24] in order to compare them with the proposed S-boxes A and B over QI. Table 17 shows the results of the EC, CM, and QI 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 other structures have one S-box at a time by fixing three parameters $a, b,$ and p. Table 17 and Figure 1 show the nonlinearity of the proposed S-box. The proposed S-box LAP results are lower than those presented in [18–24] and Figure 2. As a result, the proposed S-boxes generate more data confusion and are more resistant to linear attack than [18-24]. The proposed S-boxes' SAC and BIC results are comparable to those of other S-boxes used in Table 17 and Figure 2. As a result, the S-box generated by the proposed technique and the S-boxes shown in Table 17 cause equal magnitude diffusion in the data. The proposed DAP is comparable to the DAP of S-boxes in [18–24] and Figure 2. Thus, when compared to the others, the proposed technique generates an S-box with high resistance to differential cryptanalysis.

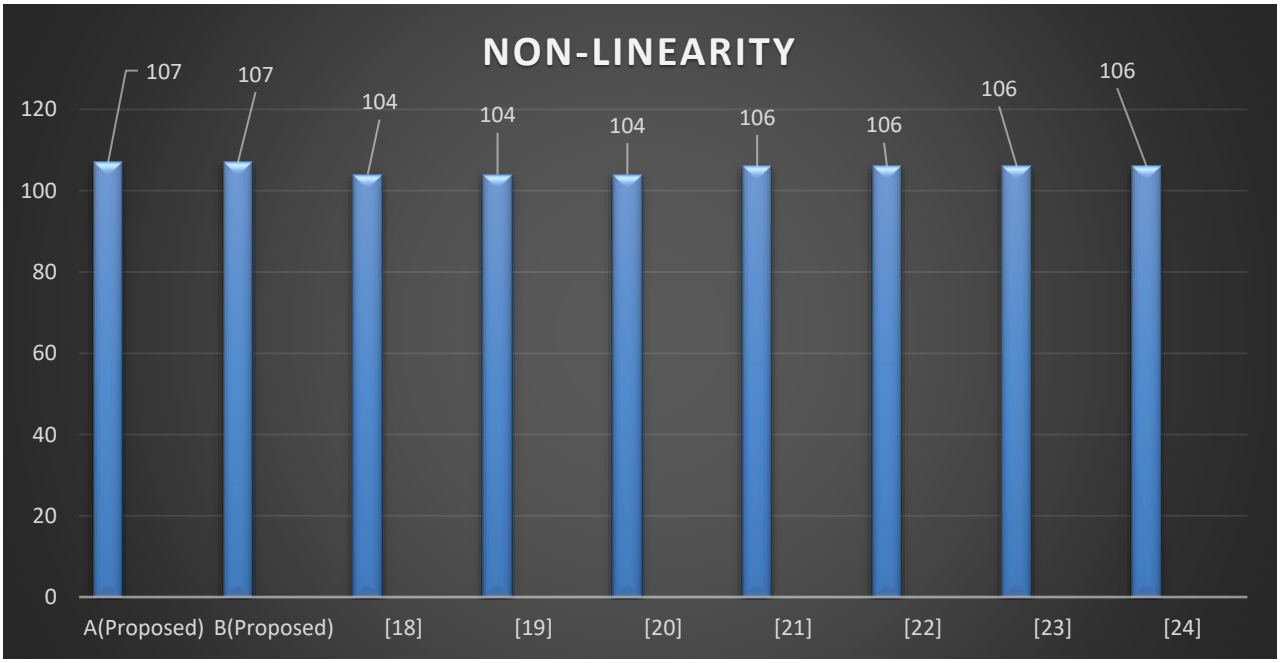

Figure 1. Comparison of NL of proposed work with existing techniques works.

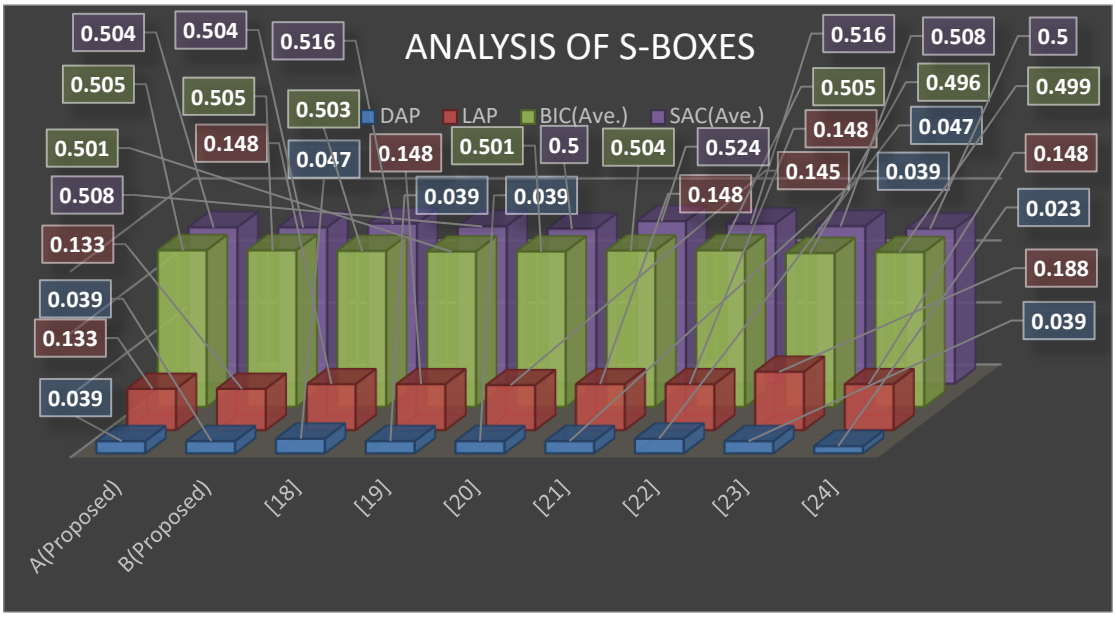

Figure 2. Comparison of BIC, SAC, and LAP of proposed work with existing techniques works.

Table 17. Proposed S-boxes comparison with existing techniques S-boxes.

$S-boxes$	$Type$	NL	LAP	DAP	$SAC\ Max$	$SAC\ Ave$	$SAC\ Min$	$BIC\ Max$	$BIC\ Ave$	$BIC\ Min$
A(Proposed)	QI	107.0	0.133	0.039	0.594	0.504	0.406	0.609	0.505	0.375
B(Proposed)	QI	107.0	0.133	0.039	0.594	0.504	0.406	0.609	0.505	0.375
[18]	EC	104.00	0.148	0.047	0.610	0.516	0.422	0.543	0.503	0.463
[19]	CM	104.00	0.148	0.039	0.625	0.508	0.391	0.531	0.501	0.471
[20]	EC	104.00	0.145	0.039	0.610	0.5	0.390	0.531	0.501	0.471
[21]	CM	106.00	0.148	0.039	0.641	0.5235	0.406	0.537	0.504	0.471
[22]	CM	106.00	0.148	0.047	0.625	0.5155	0.406	0.539	0.505	0.471
[23]	CM	106.00	0.188	0.039	0.610	0.508	0.406	0.527	0.496	0.465
[24]	CM	106.00	0.148	0.023	0.609	0.5	0.391	0.525	0.499	0.473

6. Conclusions and future directions

The proposed design methodology for the nonlinear substitution function of a block cipher based on quaternion integers has shown promising results in terms of enhancing the security of cryptographic applications. The use of quaternions in the design allows for more complex arithmetic operations, improving the cipher's confusion and diffusion properties. The implementation of the proposed design in a block cipher and extensive security analysis confirms its superiority over existing designs.

Future research directions could involve investigating the impact of varying parameters of the proposed design, such as the number of rounds and key size, on the cipher's security. Additionally, exploring the potential of combining the proposed design with other cryptographic techniques, such as key exchange or digital signatures, could lead to the development of more secure and versatile cryptographic systems.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

Researchers supporting project number (RSP 2023R472), King Saud University, Riyadh, Saudi Arabia.

Conflict of interest

The authors declared that they had no conflict of interest.

References

1. K. Jacobs, A survey of modern mathematical cryptology.Ruohonen, *Mathematical Cryp.*, **1** (2011), 1–13. https://trace.tennessee.edu/utk_chanhonoproj/1406
2. C. E Shannon, Communication theory of secrecy systems, *Bell Syst. Tech. J.*, **28** (1949), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x
3. E. Biham, A. Shamir, Differential cryptanalysis of the data encryption standard, *Springer Sci. B. Med.*, **1** (1993), 1–13. https://doi.org/10.1007/978-1-4613-9314-6
4. J. Daemen, V. Rijmen, The advanced encryption standard process, The Advanced Encryption Standard Process, In: *The Design of Rijndael: AES.*, **1** (2002), 1–8. https://doi.org/10.1007/978-3-662-04722-4
5. N. Ferguson, B. Schneier, T. Kohno, Cryptography engineering: Design principles and practical applications, *J. Wiley Sons*, **1** (2011), 1–27. http://www.wiley.com/go/permissions
6. A. Anees, Y. P. P. Chen, Designing secure substitution boxes based on permutation of the symmetric group, *NCA*, **2** (2020), 7045–7056. https://doi.org/10.1007/s00521-019-04207-8
7. A. Javeed, T. Shah, A. Ullah, Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group, *Wireless Pers Commun.*, **112** (2020), 467–480. https://doi.org/10.1007/s11277-020-07052-4
8. T. Shah, A. Qureshi, S-Box on subgroup of galois field, *Cryptography*, **13** (2019), 1–9. https://doi.org/10.3390/cryptography3020013
9. A. H. Zahid, M. J. Arshad, M. Ahmad, N. F. Soliman, W. El-Shafai, Dynamic S-Box generation using novel chaotic map with nonlinearity tweaking, *CMC-Comput. Mater. Con.*, **75** (2023), 3011–3026. https://doi.org/10.32604/cmc.2023.037516
10. L. C. N. Chew, E. S. Ismail, S-box construction based on linear fractional transformation and permutation function, *Symmetry*, **12** (2020), 826–842. https://doi.org/10.3390/sym12050826
11. B. Arshad, N. Siddiqui, Z. Hussain, M. E. U. Haq, A novel scheme for designing secure substitution boxes (S-boxes) based on Mobius group and finite field, *Wireless Pers Commun.*, **135** (2022), 3527–3548. https://doi.org/10.1007/s11277-022-09524-1

12. I. Hussain, T. Shah, M. A. Gondal, H. Mahmood, A novel image encryption algorithm based on chaotic maps and GF (2^8) exponent transformation, *Nonlinear Dyn.*, **72** (2013), 399–406. https://doi.org/10.1007/s11071-012-0723-5
13. M. Sajjad, T. Shah, R. J. Serna, Designing pair of nonlinear components of a block cipher over Gaussian integers, *CMC-Comput. Mater. Con.*, **75** *(*2023), 5287–5305. https://doi.org/10.32604/cmc.2023.035347
14. M. Sajjad, T. Shah, R. J. Serna, A. Z. E. Suarez, O. S. Delgado, Fundamental results of cyclic codes over octonion integers and their decoding algorithm, *Computation*, **10** (2022), 1–12. https://doi.org/10.3390/computation10120219
15. E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptol.*, **4** (1991), 3–72. https://doi.org/10.1007/BF00630563
16. B. B. C. Quiroga, E. C. Cantón, Generation of dynamical S-boxes for block ciphers via extended logistic map, *Math. Probl. Eng.*, **3** (2020), 1–12. https://doi.org/10.1155/2020/2702653
17. G. Tang, X. Liao, A method for designing dynamical S-boxes based on discretized chaotic map, *Chaos Soliton. Fract.*, **23** (2005), 1901–1909. https://doi.org/10.1016/j.chaos.2004.07.033
18. G. Chen, Y. Chen, X. Liao, An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps, *Chaos Soliton. Fract.*, **31** (2007), 571–579. https://doi.org/10.1016/j.chaos.2005.10.022
19. U. Çavuşoğlu, A. Zengin, I. Pehlivan, S. Kaçar, A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system, *Nonlinear Dynam.*, **87** (2021), 1081–1094. https://doi.org/10.1007/s11071-016-3099-0
20. N. Siddiqui, A. Naseer, M. E. U. Haq, A novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve, *Wireless Pers. Commun.*, **116** (2021), 3015–3030. https://doi.org/10.1007/s11277-020-07832-y
21. A. K. Farhan, R. S. Ali, H. Natiq, N. M. Al-Saidi, A new S-box generation algorithm based on multistability behavior of a plasma perturbation model, *IEEE Access*, **7** (2021), 124914–124924. https://doi.org/10.1109/ACCESS.2019.2938513
22. A. Belazi, M. Khan, A. A. A. E. Latif, S. Belghith, Efficient cryptosystem approach: S-boxes and permutation, substitution, based encryption, *Nonlinear Dynam.*, **87** (2017), 337–361. https://doi.org/10.1007/s11071-016-3046-0
23. G. Jakimoski, L. Kocarev, Chaos and cryptography: block encryption ciphers based on chaotic maps, *IEEE T. Circuits-I*, **48** (2001), 163–169. https://doi.org/10.1109/81.904880
24. M. Khan, T. Shah, H. Mahmood, M. A. Gondal, I. Hussain, A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems, *Nonlinear Dynam.*, **70** (2012), 2303–2311. https://doi.org/10.1007/s11071-012-0621-x
25. W. R. Hamilton, On a new species of imaginary quantities, connected with the theory of quaternions, *P. Roy. Irish Aca. C.*, **2** (1840), 424–434. https://www.jstor.org/stable/20520177
26. C. A Deavours, The quaternion calculus, *Am. Math. Mon.*, **80** (1973), 995–1008. https://www.jstor.org/stable/2318774
27. J. B. Kuipers, Quaternions and rotation sequences: A primer with applications to orbits, aerospace, and virtual reality, In: *Princeton University Press*, **1** (1999), 127–143. https://doi.org/10.1017/S0001924000065039
28. M. Özen, M. Güzeltepe, Cyclic codes over some finite quaternion integer rings, *J. Franklin I*, **348** (2011), 1312–1317. https://doi.org/10.1016/j.jfranklin.2010.02.008

29. T. Shah, S. S. Rasool, On codes over quaternion integers, *Appl. Algebr. Eng. Comm.*, **24** (2013), 477–496. https://doi.org/10.1007/s00200-013-0203-2
30. M. Sajjad, T. Shah, M. M. Hazzazi, A. R. Alharbi, I. Hussain, Quaternion integers based higher length cyclic codes and their decoding algorithm, *CMC*, **73** (2022), 1177–1194. https://doi.org/10.32604/cmc.2022.025245
31. S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, C. Wang, et al., Asynchronous updating Boolean network encryption algorithm, *IEEE T. Circuits*, **62** (2022), 1–12. https://doi.org/10.1109/TCSVT.2023.3237136
32. S. Gao, R. Wu, X. Wang, J. Wang, Q. Li, C. Wang, et al., A 3D model encryption scheme based on a cascaded chaotic system, *Signal Process.*, **202** (2023), 1–13. https://doi.org/10.1016/j.sigpro.2022.108745
33. S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, X. Tang, EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory, *Inf. Sci.*, **621** (2023), 766–781. https://doi.org/10.1016/j.ins.2022.11.121
34. R. Wu, S. Gao, X. Wang, S. Liu, Q. Li, U. Erkan, et al., AEA-NCS: An audio encryption algorithm based on a nested chaotic system, *Chaos Soliton. Fract.*, **165** (2023), 1–10. https://doi.org/10.1016/j.chaos.2022.112770
35. Y. Chen, C. Tang, R. Ye, Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion, *Signal Process*, **167** (2020), 1–12. https://doi.org/10.1016/j.sigpro.2019.107286
36. X. Wang, H. Sun, A chaotic image encryption algorithm based on improved Joseph traversal and cyclic shift function, *Opt. Laser Technol.*, **122** (2020), 1–12. https://doi.org/10.1016/j.optlastec.2019.105854
37. J. Chen, L. Chen, Y. Zhou, Cryptanalysis of a DNA-based image encryption scheme, *Inf. Sci.*, **520** (2020), 130–141. https://doi.org/10.1016/j.ins.2020.02.024
38. H. Zhu, J. Ge, W. Qi, X. Zhang, X. Lu, Dynamic analysis and image encryption application of a sinusoidal-polynomial composite chaotic system, *Math. Comput. Simulat.*, **198** (2022), 188–210. https://doi.org/10.1016/j.matcom.2022.02.029
39. Y. Xian, X. Wang, X. Yan, Q. Li, X. Wang, Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion, *Opt. Laser Eng.*, **134** (2020), 1–13. https://doi.org/10.1016/j.optlaseng.2020.106202
40. C. Li, Y. Zhang, E. Y. Xie, When an attacker meets a cipher-image: A year in review, *J. Inf. Secur. Appl.*, **48** (2019), 1–9. https://doi.org/10.1016/j.jisa.2019.102361