Multimedia Tools and Applications (2024) 83:10409–10425
https://doi.org/10.1007/s11042-023-15971-0

A novel approach for designing secure substitution boxes based on Catalan number and elliptic curve

Bilal Arshad[1,2] · Muhammad Ehatisham-ul-Haq[3] · Zamir Hussain[4] · Awais Asghar[5]

Received: 24 May 2022 / Revised: 16 March 2023 / Accepted: 29 May 2023 /
Published online: 22 June 2023

Abstract
While using the internet, sending confidential emails, or dealing with financial information that affects many aspects of our everyday life, security is one of the most important considerations. We can prevent illegal access to our data with the aid of security. Cryptography is one of the methods used for encryption and decryption in this context to safeguard data. The S-box is the most important and the sole nonlinear component of any cryptographic algorithm that adds uncertainty to the data. Based on the combination of the Catalan number and the elliptic curve, the proposed method constitutes a unique algorithm. The strength of S-boxes is then assessed using nonlinearity, strict avalanche criterion, bit independence criterion, linear and differential approximation probabilities. Performance studies show that the proposed S-boxes have exceptional functionality and can give cryptosystems a significant amount of nonlinearity. Furthermore, the comparison shows that the newly proposed S-boxes offer enhanced security features in contrast to other S-boxes that are already in use literature.

Keywords Substitution box (S-box) · Catalan number · Elliptic curve cryptography (ECC) · Image encryption

✉ Bilal Arshad
bilalarshad689@gmail.com

Muhammad Ehatisham-ul-Haq
ehatishamuet@gmail.com

Zamir Hussain
zamir.hussain@uow.edu.pk

Awais Asghar
awais.asghar154@gmail.com

[1] Department of Elementary and Secondary Education, Khyber Pakhtunkhwa, Pakistan

[2] Department of Basic Sciences, University of Engineering and Technology, Taxila, Pakistan

[3] Department of Creative Technologies, Air University, Islamabad, Pakistan

[4] Department of Mathematics, University of Wah, Wah Cantt, Pakistan

[5] Pak-Austria Fachhochschule: Institute of Applied Sciences and Technology, Haripur, Pakistan

1 Introduction

Today's information systems, from email to mobile communications, heavily rely on cryptography. Examples include secure web access to digital currencies. The use of cryptography enhances confidentiality, fairness, accuracy, and accountability. Ensuring that financial transactions are authentic, it can aid in safeguarding electronic commerce from fraud. You can use it to keep your identity a secret or to confirm it. Vandals won't be able to interfere with your website, and your important material won't be read by business rivals. Cryptography will become even more important as trade and communications move to computer networks. It secures communications and data by enforcing a set of regulations that limit access to and processing of data to just those who are supposed to use it.

Although it is today most closely linked to the terms encryption and decryption, cryptography is commonly known as the study of secrets. To safeguard data from data thieves, plain text that is visible is converted into ciphertext, which is hidden. Researchers employ encryption to ensure that material is concealed from anyone for whom it is not intended, including those who are able to view the encrypted data. Understanding ciphertext, which is at the other end of the process, requires decoding. In symmetric block ciphers, the S-box is a key element that is essential to ensuring the security of the system. By establishing an exclusive link between plaintext and ciphertext, the S-box causes data to get muddled [52].

Today, cryptography plays a crucial role in a number of fields. Satellite remote-sensing images have been used in many aspects of people's life due to the rapid growth of remote-sensing technology. It is critical to encrypt remote sensing photos as well as digital and medical photographs since they contain sensitive information such as land profiles and military secrets [28]. For the past 20 years, face verification has been the subject of extensive research. One of the challenges is that there is rising concern about the template database's security and privacy [30]. Author, [9], provides a face verification system with security that creates a distinct, secure cryptographic key from a face template. After processing, the face photos are turned into face templates or codes that can be used for both encryption and decryption operations. With Advanced Encryption Standard, the identity data obtained is encrypted.

The use of medical image encryption has grown significantly in recent years. The diagnosis of a variety of disorders depends heavily on the use of medical imaging techniques such as magnetic resonance imaging (MRI), computed tomography (CT), X-rays, and ultrasound. The internet has seen quick advancements in terms of sharing and exchanging vast volumes of information. To protect patients' sensitive information during the transmission of medical images, these medical data should be communicated through a secure communication channel; otherwise, a false diagnosis could result from the attacker capturing and tampering with the provided medical image. As a result, transmitting medical images while maintaining confidentiality and integrity became quite difficult. In order to safeguard the medical images exchanged via a public network, extra care must be taken. Cryptography, steganography, and watermarking are common methods used in medical image security [29, 37]. Due to the frequent data exchange over the internet, data concealing in video streams have become more common in the modern world. Compared to hiding inside images, hiding the data in video streams offers more security and increased embedding capacity. The amount of information that must be integrated into the video is growing, and this could negatively affect the quality of the video, making it unsuitable for some appliances. High visual quality, enhanced concealing capacity, and video stream size is the key issues with data hiding in videos [56, 60].

The following format is used in this document: The relevant work is under Section 2. The terms S-box, Catalan number, and elliptic curve are defined in Section 3. Section 4

presents the proposed scheme for S-box production. In Section 5, the algebraic analyses of these S-boxes are presented. Section 6 provides a description of the statistical analyses. Lastly, Section 7 provides a summary of this study's findings.

2 Related work

There are several ideas in the literature for making S-boxes. Well-known S-boxes have been described as producing data misinterpretation in the literature [6, 15, 21, 27, 35]. On the basis of various mathematical frameworks, several academics have devised numerous S-box generation techniques. A good S-box was reportedly obtained by employing a coset diagram and a bijective map in [45]. By combining a chaotic tent-sine system and the Mobius transformation, the authors create robust S-boxes [26]. For the creation of S-boxes, the authors [7] proposed a novel method based on symmetric group permutation. In [4], the authors presented a brand-new S-boxes method using a projective general linear group. Using coset diagrams for the action of a quotient of the modular group on the projective line over the finite field, as well as the Fibonacci sequence for the selection of vertices of the coset diagram, the authors proposed an S-box in [51]. In [48], a fresh idea for the S-box was put out, which was based at the idea of coset graphs and symmetric groups. By specifying various total orders in [13], researchers created an effective technique for producing S-boxes based on a class of Mordell elliptic curves (MECs) over prime fields. The authors developed an effective technique for generating a large number of different, mutually uncorrelated, and cryptographically robust, and uncorrelated injective S-boxes based on ordered isomorphic elliptic curves [12]. In [47], a straightforward technique for making S-boxes were studied using the cyclic and symmetric group. Using the composition of the inversion function and the effect of the $S8$ symmetric group on the Galois field, the authors of [40] proposed a novel strategy. Table 1 lists some newly proposed S-boxes, the design approaches used to make them, as well as their cryptographic features, such as nonlinearity and differential approximation probability.

In this research, we propose a new and effective approach for constructing secure S-boxes based on the Catalan number and the elliptic curve. S-boxes have not yet been created using the Elliptic Curve and Catalan numbers. The combination of the Catalan number plus an elliptic curve yields S-boxes. We used algebraic analyses such as nonlinearity, strict avalanche criterion, bit independence criterion, differential and linear approximation probabilities to examine the cryptographic strength of the proposed S-boxes in accordance with the National Institute of Standards and Technology (NIST) standards. In order to encrypt images, we also used the newly proposed S-boxes. We then performed statistical analysis on both plain and encrypted images using the majority logic criterion.

3 Preliminaries

In this part, we will go over the fundamentals of S-box, elliptic curve cryptography, and Catalan number.

3.1 Substitution box

Claude Shannon first presented the concept of the S-box in 1949 [52]. S-boxes play a vital role in each block cipher cryptography. For each block cipher (S-box), nonlinear

Table 1 Latest S-boxes design techniques with cryptographic properties

References/ Publication Years	Proposed Techniques	Cryptographic Properties	
		Nonlinearity	DP
[10]/ 2022	Mobius Group and Finite Field	107.25	0.0234
[55]/ 2020	The Action of Matrices on Galois Field	112.00	0.0156
[8]/ 2020	Connected Regular Graphs with Adjacency Matrix	112.00	0.0156
[53]/ 2020	Elliptic Curve and Modified Pascal's Triangle	105.00	0.0390
[54]/ 2020	Modular Group with Projective Line Over a Finite Field	112.00	0.0156
[17]/ 2020	Modular Group $PSL(2,\mathbb{Z})$ with Projective Line $PL(F_{257})$ over Galois Field $GF(2^8)$	106.50	0.0391
[38]/ 2020	Chaos-Based Rotational Matrices	112.00	0.0156
[58]/ 2019	Random Number Generators Over Mordell Elliptic Curves	112.00	0.016
[59]/ 2018	Action of Projective General Linear Group with Units of Finite Local Ring	107.25	0.0469
[19]/ 2018	Elliptic Curves	100.00	0.0391
[46]/ 2017	Coset Diagram and a Bijective Map	106.75	0.0468

components are essential for secure communication. Confusion is an important characteristic, which is only done by S-box in enciphering digital information. S-box is commonly used in block ciphers to hide the connection between the key and the ciphertext, Shannon's property of confusion. A multivalued Boolean function S known as a substitution box maps n-inputs to m-outputs.

$$S : Z_2^n \longrightarrow Z_2^m$$

Typically, S-Box takes a certain amount of input bits n and turns them into a certain amount of output bits m, and then returns the result.

3.2 Catalan number

In the fields of combinatorics and computer science, Catalan numbers play a vital role and have a considerable impact. In investigating an astoundingly large number of combinatorial problems, they form a sequence of natural numbers. Nowadays, computational geometry, geographic information systems, geodesy, cryptography, and medicine are the application of the engineering fields where Catalan numbers are used. In computational geometry problems, they are typically employed in geometric modelling. They aid in the creation of keys used in cryptography to transmit data securely.

Catalan numbers are a group of natural numbers that appear in a wide range of counting problems, the majority of which involve recursively-produced objects. They were named after Belgian mathematician "Eugene Charles Catalan (1814–1894)" [44]. Using binomial coefficients, the *nth* Catalan number is derived as,

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{(n+1)!n!} = \prod_{k=2}^{n}\frac{n+k}{k}; \quad \text{for } n \geq 0$$

3.3 Elliptic curve cryptography

For the first time in 1985, Neal Koblitz [34] and Victor Miller [39] independently proposed Elliptic Curve (EC) cryptography algorithms. A non-singular cubic curve in two variables $f(x,y)=0$, with a rational point is an EC over a field K. The field K is widely used to represent complex numbers, reals, rationals, and algebraic extensions of rationals, as well as a finite field [5].

A prime field F_p with p elements, where p is a prime number. There is exactly one prime field F_p for each prime p number. The elliptic curve on field F_p is defined as the following for any two integers of F_p, let's assume a and b,

$$E_{a,b}(F_p) = \left\{(x,y) \in F_p^2 | \left(y^2 = x^3 + ax + b\right) (\text{mod } p), \;\; a,b,x,y \in F_p \right\} \cup \{O\}$$

Given that $4a^3+27b^2 \neq 0$ and O represent the infinite point. The discriminant of the elliptic curve is $4a^3+27b^2$ [19].

4 Proposed scheme

We'll look at a simple way for creation of S-boxes in this part. The creation of S-boxes is based on the Catalan number and the elliptic curve's composition.

Figure 1 depicts the two halves of the suggested approach for the creation of an S-box, the first of which comprises four crucial phases. An EC is defined in the first phase. Modulo 256 is then applied on EC. The first S-box is then obtained by using $a=789$, $b=713$, and $p=25851$. Three crucial phases make up the second section: first, we defined a Catalan number, and then we obtained the second S-box by applying the formula $k=8$, $n=1:300$. We obtain the final S-boxes by composing these S-boxes.

The proposed algorithm consists of the essential phases outlined below:

Step 1: Define a Catalan number as,

$$C_n = \prod_{k=2}^{n} \frac{n+k}{k}; \quad for\ n \geq 0$$

We generate an algorithm using this equation for $k=8$ and $n=1:300$ to obtain an S-box, but this S-box doesn't have good cryptographic properties and for secure communication,

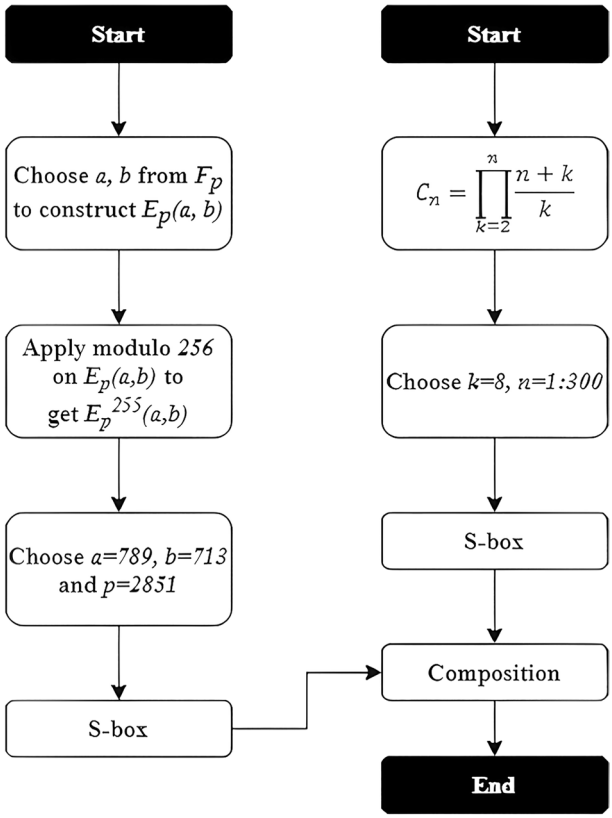

Fig. 1 Proposed methodology for S-box design

Table 2 The final S-box-1 creation by the offered algorithm

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

this S-box is not regarded as being particularly powerful. To improve the cryptographic features of this S-box, we go to the next step.

Step 2: a and b are two distinct elements to be chosen from F_p, where p is a huge prime number. The large value of p is used to produce an elliptic curve with at least 256 unique members. Create the EC $E_p(a,b)$ by using the equation,

$$y^2 = \left(x^3 + ax + b\right) mod p$$

Step 3: Now, apply modulo 256 on $E_p(a,b)$ to get $E_p^{255}(a,b)$. This action is used to limit the values of $E_p(a,b)$ in the range 0–255.
Step 4: Finally, by the selection of $a=789$, $b=713$, and $p=2851$, S-box is generated.
Step 5: The final S-boxes were created by the composition of the Catalan number and the elliptic curve S-boxes. This composition gives us the desired S-boxes which were presented in Tables 2 and 3.

5 Results, analysis, comparison

At this point, to study the attributes of proposed S-boxes, we utilized the algebraic tests such as NL, SAC, BIC, DAP, and LAP. Furthermore, we also compare our proposed S-boxes to various existing S-boxes in the literature, as shown in Tables 5, 9, and 11.

5.1 Nonlinearity

A distance between the function itself and the set of all affine functions can be used to describe nonlinearity for a Boolean function. Nonlinearity refers to the number of bits that must be

Table 3 The final S-box-2 creation by the offered algorithm

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

transferred to a Boolean function's truth table in order to achieve the nearby affine function. For the S-box over the Galois field $GF(2^n)$, the nonlinearity is $N(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$. Because the S-box in the advanced encryption standard is in $GF(2^8)$, the highest nonlinearity value is 120. Table 4 shows that the proposed S-box-1 has nonlinearity scores of 106, 106, 102, 106, 106, 108, and 104, with the least nonlinearity being 102, maximum nonlinearity being 108 and average nonlinearity score being 105.50. Proposed S-box-2 has nonlinearity scores of 104, 106, 108, 102, 104, 106, 108, and 96, with the least nonlinearity being 96, maximum nonlinearity being 108 and average nonlinearity score being 104.24 respectively.

Table 5 compares the nonlinearity scores of the newly proposed S-boxes to those of previously published S-boxes, which are available in the literature. Table 5 shows that the average nonlinearity rating of the newly proposed S-boxes, with the exception of a few S-boxes, is greater than the mean nonlinearity rating of the majority of various existing S-boxes in literature and generally on par with other strong S-boxes.

5.2 Strict avalanche criterion

The SAC is reliant on modifying the input and output bits. An S-box fulfills SAC, when a single bit on the input changes and half of the output bits change as well. When using S-box to create a Substitution Permutation (S-P) network, a single exchange in the network's input cause an avalanche of adjustments. Table 6 indicates the outcomes of applying the strict avalanche criterion.

Table 4 Nonlinearity of proposed S-boxes

Proposed S-boxes	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Min. Value	Max. Value	Avg. Value
Proposed S-box-1	106	106	106	102	106	106	108	104	102	108	105.50
Proposed S-box-2	104	106	108	102	104	106	108	96	96	108	104.24

Table 5 Nonlinearity scores for different S-boxes

S-boxes/Year	Type of S-boxes	Nonlinearities		
		Min	Max	Mean
Proposed S-box-1	Proposed S-boxes	102	108	**105.50**
Proposed S-box-2		96	108	**104.25**
[13]/2019	Elliptic Curve S-boxes	106	108	106.5
[12]/2018		106	110	107.0
[47]/2020		102	108	104.0
[19]/2018		100	108	105.0
[18]/2019		101	107	104.0
[20]/2021		106	108	106.25
[24]/2021		106	110	106.5
[33]/2023		88	106	99.06
[42]/2010	Chaotic S-boxes	100	106	103.2
[32]/2012		98	108	103.0
[31]/2013		100	108	104.5
[36]/2015		104	108	105.80
[43]/2013		103	109	105.1
[41]/2020		102	108	105.25
[3]/2022		100	106	103.75
[2]/2015	Other S-boxes	106	110	107.0
[45]/2017		104	108	106.75
[14]/2020		96	108	102.25
[49]/2021		98	106	103.7
[62]/2020		102	108	105.0
[22]/2020		98	108	104.0
[50]/2020		106	110	108
[23]/2020		96	110	104
[25]/2022		104	108	106.75
[11]/2022		108	104	106
[61]/2020		104	110	107.5
[1]/2023		102	110	107.00

5.3 Bit Independence criterion

A cryptographic structure essentially carries the output bits independence criterion. This was first mentioned by Detombe and Tavares [16]. It requires all the avalanche variables pairwise however independent of a given set of avalanche vectors. The complementing of a single plaintext bit generates these vectors. Table 7 shows the outcomes of the BIC analysis of the proposed S-box-1, whereas Table 8 shows the BIC results for SAC. The score for BIC is 103.

The average SAC scores of our proposed S-boxes are 0.500 and 0.515 respectively, indicating that the proposed S-boxes effectively justify SAC. Furthermore, the average BIC score is 103 and 103.5, indicating that our proposed S-box-1 meets BIC analyses. Table 9 shows a comparison of the proposed S-boxes' SAC and BIC scores with the SAC and BIC scores of S-boxes published in the literature, demonstrating that our S-boxes outperform various other S-boxes.

Table 6 Results of SAC

0.500	0.484	0.484	0.484	0.515	0.531	0.437	0.546
0.453	0.500	0.531	0.453	0.406	0.531	0.437	0.531
0.468	0.484	0.546	0.453	0.453	0.562	0.562	0.546
0.531	0.468	0.531	0.453	0.468	0.500	0.546	0.562
0.453	0.593	0.546	0.500	0.500	0.484	0.453	0.468
0.515	0.500	0.500	0.484	0.515	0.515	0.500	0.515
0.515	0.531	0.468	0.437	0.500	0.515	0.484	0.578
0.578	0.546	0.437	0.546	0.421	0.484	0.390	0.546

5.4 Differential approximation probability

The important property of the non-linear transformation of an S-box is differential uniformity, which makes it unique. The input differential D_{x_i} maps the output differential D_{y_i}, ensuring uniform mapping probability for each. The probability of a given S-box being a measure for differential uniformity can be written as,

$$DP^s(\Delta x \longrightarrow \Delta y) = \left[\frac{\#\{x \in Xj | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^m}\right]$$

The highest DAP value for the proposed S-box-1 is 0.0390 according to Table 10.

5.5 Linear approximation probability

To investigate an event of imbalance, the linear approximation probability approach is used. This quantity is used for estimating the maximum output imbalance value in an event, where x and y are the two masks that are applied to the uniformity of input bits and output bits, respectively. The probability of bias for a particular S-box is also known as the linear approximation probability and is defined as,

$$LP = \max_{\tau x, \tau y} \left| \frac{\#\{x | x.\tau x = S(x).\tau y\}}{2^n} - \frac{1}{2} \right|$$

Where set X consists all possible inputs and 2^n gives the number of elements in it. The LAP of the proposed S-box-1 is 0.1328.

Table 7 Bit independence criterion of proposed S-box-1

0	100	104	100	102	100	104	104
100	0	106	106	106	102	102	100
104	106	0	106	100	104	98	98
100	106	106	0	106	104	106	106
102	106	100	106	0	106	104	100
100	102	104	104	106	0	104	102
104	102	98	106	104	104	0	104
104	100	98	106	100	102	104	0

Table 8 Bit independence criterion results for strict avalanche criterion

0	0.488	0.503	0.470	0.535	0.521	0.488	0.492
0.488	0	0.500	0.519	0.480	0.494	0.513	0.498
0.503	0.500	0	0.517	0.513	0.498	0.501	0.503
0.470	0.519	0.517	0	0.486	0.513	0.500	0.521
0.535	0.480	0.513	0.486	0	0.505	0.498	0.484
0.521	0.494	0.498	0.513	0.505	0	0.482	0.494
0.488	0.513	0.501	0.500	0.498	0.482	0	0.478
0.492	0.498	0.503	0.521	0.484	0.494	0.478	0

The LAP and DAP scores of our proposed S-boxes are compared to the LAP and DAP scores of S-boxes found in the literature in Table 11. From Table 11, it can be seen that our proposed S-boxes' DAP values are 0.0390 and 0.0468. In addition, the LAP values of our work are 0.1328 and 0.125. These tests demonstrate that our proposed S-boxes can thwart both linear and differential cryptanalysis.

Table 9 Performance valuation of SAC and BIC scores

S-boxes/Year	Type of S-boxes	BIC	SAC
Proposed S-box-1	Proposed S-boxes	**103.0**	**0.5000**
Proposed S-box-2		**103.5**	**0.5156**
[13]/2019	Elliptic Curve S-boxes	104.14	0.5046
[12]/2018		103.85	0.4968
[47]/2020		103.14	0.5007
[19]/2018		104.14	0.5007
[18]/2019		103.21	0.500
[20]/2021		102.37	0.5086
[24]/2021		103.93	0.5009
[33]/2023		96.62	0.6047
[42]/2010	Chaotic S-boxes	103.7	0.5048
[32]/2012		104.07	0.5012
[31]/2013		103.6	0.4978
[36]/2015		104.5	0.4976
[43]/2013		103.6	0.5061
[41]/2020		102.6	0.5037
[3]/2022		108.0	0.5000
[2]/2015	Other S-boxes	104.2	0.5014
[45]/2017		103.64	0.5031
[14]/2020		103.5	0.5059
[49]/2021		103.8	0.496
[62]/2020		102.9	0.503
[22]/2020		98.0	0.593
[50]/2020		105.28	0.497
[23]/2020		103.00	0.493
[25]/2022		103.78	0.609
[11]/2022		106.0	0.5002
[61]/2020		103.5	0.4980
[1]/2023		103.00	0.5044

Table 10 Differential approximation probability of the proposed S-box-1

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

6 Image encryption applications

In this stage, we give some statistical studies of the novel and popular S-boxes. The majority logic criterion (MLC) is used to evaluate the efficacy of the proposed S-box in applications of image encryption. The applicability of the S-box in encryption applications is determined by statistical analyses such as energy, contrast, correlation, entropy, and homogeneity. These investigations determined whether the S-box is acceptable for encryption applications or not. In the energy analysis, we calculate the energy of the encrypted images as processed by numerous S-boxes. The number of square elements in the co-occurrence matrix at the gray level is determined by this calculation. When compared to plain images, encrypted images have less energy. The ability to detect objects in an image is measured through contrast analysis. To achieve successful encryption, a high level of contrast is required. Table 10 summarizes the results of the statistical analyses. By researching correlation analysis, we can detect the resemblances between plain pixel patterns and encoded images. There are three different types of correlation analysis. For this reason, the vertical, horizontal, and diagonal forms are used. The correlation between adjacent pixels in the encrypted image should be close to zero. Entropy is a statistical randomness measure that may be used to characterize the texture of an image. The optimum entropy of a perfect random image is 8. The homogeneity test compares the dispersion of variables in the grey-level co-occurrence matrix (GLCM) to the inclination of the GLCM. The GLCM displays measurements as simple blends of pixel splendor values or dark stages.

As illustrated in Table 12, the proposed S-boxes deliver robust image encryption outcomes. The achieved parameters are comparable to those of the AES, Skipjack, APA, and Gray S-boxes. Plan images of Lena and Baboon obtained using the proposed S-box-1 have entropy values of 7.2248 and 7.4087, respectively, and encoded images of Lena and Baboon have entropy values of 7.2245 and 7.4087, which are nearly equal to the optimal value of 8. The image's randomness is amplified by the image's nonlinear substitution of input and output elements, which is measured by its entropy. To establish their linear independence, calculations are made to determine the relationship between the plain and encrypted images.

Table 11 Evaluation of DP and LAP of different S-Boxes

S-boxes/Year	Type of S-boxes	DAP	LAP
Proposed S-box-1	Proposed S-boxes	**0.0390**	**0.1328**
Proposed S-box-2		**0.0468**	**0.125**
[13]/2019	Elliptic Curve S-boxes	0.0391	0.1328
[12]/2018		0.0391	0.1875
[47]/2020		0.0390	0.125
[19]/2018		0.0391	0.0547
[18]/2019		0.0468	0.144
[20]/2021		0.0468	0.1484
[24]/2021		0.0391	0.1172
[33]/2023		0.044322	0.046645
[42]/2010	Chaotic S-boxes	0.0391	0.1328
[32]/2012		0.0468	0.1328
[31]/2013		0.0468	0.1406
[36]/2015		0.0391	0.1250
[43]/2013		0.0391	0.1563
[41]/2020		0.0391	0.1328
[3]/2022		0.03125	0.1028
[2]/2015	Other S-boxes	0.0391	0.1484
[45]/2017		0.0468	0.1484
[14]/2020		0.0468	0.125
[49]/2021		0.0468	0.125
[62]/2020		0.0468	0.1484
[22]/2020		0.25	0.1328
[50]/2020		0.0625	0.125
[23]/2020		0.125	0.125
[25]/2022		0.0391	0.1250
[11]/2022		0.0380	0.1328
[61]/2020		0.0390	0.1406
[1]/2023		0.0312	0.1172

Table 12 shows that when employing the proposed S-box-1, the correlation between plain images and their encrypted versions is 0.1940 and 0.0252, respectively. These statistics reveal a slight linear association between the pixels' input and output values. Because of this, the proposed S-boxes have good cryptographic qualities such as confusion and diffusion. The energy measure values for Lena and Baboon's plain images are 0.1075 and 0.0779, respectively. After using the S-box-1 to encrypt these plain images, we obtain energy values of 0.0218 and 0.0159, which are comparable to the energy values of AES, Skipjack, APA, and Gray S-boxes. The smaller energy metric indicates the proposed S-boxes efficient performance in image encryption. In addition, in comparison to existing S-boxes, the proposed S-boxes achieve high contrast values of over 8.5. A high value of contrast, in general, suggests that the image has greater randomness. After applying the S-box-1, the objects in the image are entirely distorted because of the nonlinearity of mapping. As a result, the encrypted image's high contrast value indicates that the encryption is robust. Lastly, homogeneity analysis is used to calculate the distance between the scattered elements of GLCM and its diagonal. The results of this statistical analysis are shown in Table 12, which

Table 12 Evaluation of MLC for proposed S-box-1 over different S-boxes

S-boxes	Entropy	Contrast	Correlation	Energy	Homogeneity
Pepper Image					
Plaintext	7.2248	0.3868	0.9308	0.1075	0.8730
Proposed S-box-1	**7.2245**	**8.6561**	**0.1940**	**0.0218**	**0.5243**
AES S-box	7.9211	7.5509	0.0554	0.0202	0.4662
Skipjack S-box	7.7561	7.7058	0.1205	0.0239	0.4708
APA S-box	7.2264	8.1195	0.1473	0.0183	0.4676
[57]/2008	7.2301	7.5283	0.0586	0.0203	0.4623
Baboon Image					
Plaintext	7.4087	0.7677	0.7997	0.0779	0.7624
Proposed S-box-1	**7.4087**	**10.0197**	**0.0252**	**0.0159**	**0.4048**
AES S-box	7.2531	7.5509	0.0554	0.0202	0.4662
Skipjack S-box	7.2531	7.7058	0.1025	0.0193	0.4689
APA S-box	7.2264	8.1195	0.1473	0.0183	0.4676
[57]/2008	7.2301	7.5283	0.0586	0.0203	0.4623

demonstrates that the S-box-1 that was produced reaches satisfactory homogeneity value, suggesting that more robust encryption is feasible. As a result, as demonstrated in Table 12, the proposed S-box-1 image encryption results are comparable to recent results.

Figure 2 shows an example image of Lena along with an encrypted image and histograms, while Figure 3 shows a simple and encrypted image of Baboon along with histograms. As illustrated in the pictures, the proposed S-boxes successfully conceal the visual data present in the plain image, suggesting their effective image encryption capacity. Because of this, we feel the S-box design is appropriate for encryption purposes.

7 Conclusion

In cryptography, the S-box is a principal device used to show a connection between plaintext and ciphertext. They play a vital role in creating confusion in data. In this study, robust S-boxes are introduced which depend on the idea of the Elliptic Curve and Catalan number. As per our information, this is the first time when Catalan number is involved in the creation of S-boxes. After construction, the outcomes of the different statistical and algebraic

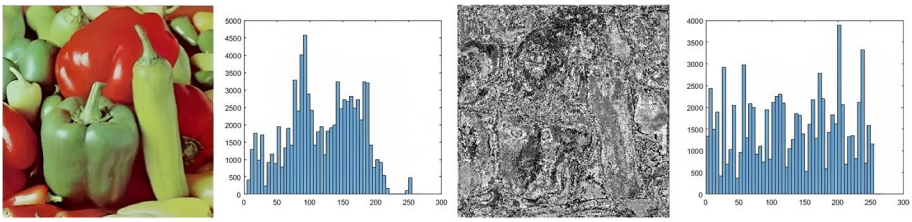

Fig. 2 For the Pepper image, the results of image encryption using the proposed S-box-1 (**a**) Plain Image (**b**) Plain Image's Histogram (**c**) Encrypted Image (**d**) Encrypted Image's Histogram

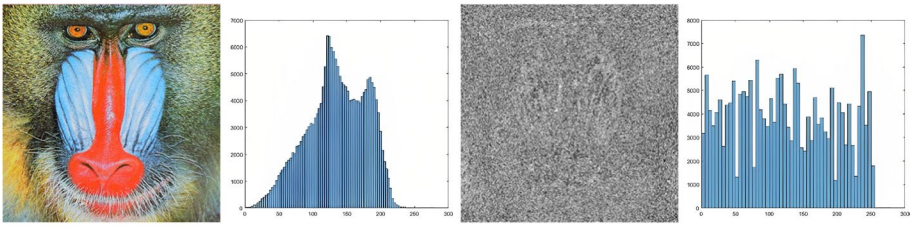

Fig. 3 For the Baboon image, the results of image encryption using the proposed S-box-1 (**a**) Plain Image (**b**) Plain Image's Histogram (**c**) Encrypted Image (**d**) Encrypted Image's Histogram

analyses demonstrate the eminently great cryptographic performance of our new S-boxes. As clear from the different statistical analyses, the proposed S-boxes show great results when contrasted with some notable S-boxes. The proposed S-boxes are exceptionally safe and the outcomes acquired from the various analyses are almost equivalent to the perfect ones. Therefore, it is valuable for safe communication. ECC is much more efficient than RSA for encryption and decryption, but it is still much slower than symmetric algorithms. Furthermore, this study can be expanded in the future and employed in image denoising.

Funding There has been no significant financial support for this work.

Data availability On reasonable request, the corresponding author, Bilal Arshad, will provide the data that support the conclusions of this study.

Declaration

I would like to submit the manuscript entitled "***A Novel Approach for Designing Secure Substitution Boxes Based on Catalan Number and Elliptic Curve***" by Bilal Arshad, Muhammad Ehatisham-ul-Haq, Zamir Hussain, and Awais Asghar to be considered for publication as an original article in the *Multimedia Tools and Applications*. We declare that this manuscript is original, has not been published before, and is not currently being considered for publication elsewhere.

Conflicts of interest We know of no conflicts of interest associated with this publication.

References

1. Abd-El-Atty B (2023) Efficient S-box construction based on quantum-inspired quantum walks with PSO algorithm and its application to image cryptosystem. Complex Intell Syst:1–19
2. Ahmad M, Bhatia D, Hassan Y (2015) A novel ant colony optimization based scheme for substitution box design. Procedia Comput Sci 57:572–580
3. Ali A, Khan MA, Ayyasamy RK, Wasif M (2022) A novel systematic byte substitution method to design strong bijective substitution box (S-box) using piece-wise-linear chaotic map. PeerJ Comput Sci 8:e940
4. Altaleb A, Saeed MS, Hussain I, Aslam M (2017) An algorithm for the construction of substitution box for block ciphers based on projective general linear group. AIP Adv 7(3):035116
5. Amounas F (2013) A novel approach for enciphering data based ecc using catalan numbers. Int J Inform Network Secur (IJINS) 2(4)
6. Anees A, Ahmed Z (2015) A technique for designing substitution box based on van der pol oscillator. Wirel Pers Commun 82(3):1497–1503
7. Anees A, Chen Y-PP (2019) Designing secure substitution boxes based on permutation of the symmetric group. Neural Comput Applic

8. Arshad B, Siddiqui N (2020) Construction of highly nonlinear substitution boxes (S- boxes) based on connected regular graphs. Int J Comp Sc Info Sec 18(4):pp. 09-122
9. Arshad N, Moon KS, Kim JN (2013) A secure face cryptography for identity document based on distance measures. J Korea Multi Soc 16(10):1156–1162
10. Arshad B, Siddiqui N, Hussain Z, Ehatisham-ul-Haq M (2022) A novel scheme for designing secure substitution boxes (s-boxes) based on mobius group and finite field. Wirel Pers Commun
11. Aslam M, Beg S, Anjum A, Qadir Z, Khan S, Malik SUR, Mahmud MP (2022) A strong construction of S-box using Mandelbrot set an image encryption scheme. PeerJ Comput Sci 8:e892
12. Azam NA, Hayat U, Ullah I (2018) An injective s-box design scheme over an ordered isomorphic elliptic curve and its characterization. Secur Comm Networks 1–9:2018
13. Azam NA, Hayat U, Ullah I (2019) Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field. Front Inform Technol Electronic Eng 20(10):1378–1389
14. Cassal-Quiroga BB, Campos-Canton E (2020) Generation of dynamical s-boxes for block ciphers via extended logistic map. Math Problem Eng 2020:1–12
15. Cui L, Cao Y (2007) A new s-box structure named affine-power-affine. Int J Innov Comput Inf Control 3(3):751–759
16. Detombe J, Tavares S (1992) Constructing large cryptographically strong S-boxes: advances in cryptology. Proc. of CRYPTO92. Lect Notes Comput Sci:165–181
17. Gao W, Idrees B, Zafar S, Rashid T (2020) Construction of nonlinear component of block cipher by action of modular group PSL(2,$\mathbb{Z}$) on projective line PL(GF(2^8)). IEEE Access
18. Hayat U, Azam NA (2019) A novel image encryption scheme based on an elliptic curve. Signal Process 155:391–402
19. Hayat U, Azam NA, Asif M (2018) A method of generating 8×8 substitution boxes based on elliptic curves. Wirel Pers Commun 101(1):439–451
20. Hayat U, Azam NA, Gallegos-Ruiz HR, Naz S, Batool L (2021) A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings. Arab J Sci Eng:1–13
21. Hussain I, Shah T, Gondal MA, Wang Y (2011) Analyses of SKIPJACK S-box. World Appl Sci J 13(11):2385–2388
22. Hussain I, Shah T, Gondal MA, Khan M, Khan WA (2011) Construct New S-box Using Linear Fractional Trans, World Appl Sci J 14(12):1779–1785
23. Hussain I, Shah T, Gondal MA, Khan M, Khan WA (2011) Construction cryptographically strong 8*8 S-boxes. World Appl Sci journal 13(11):2389–2395
24. Ibrahim S, Abbas AM (2021) Efficient key-dependent dynamic S-boxes based on permutated elliptic curves. Inf Sci 558:246–264
25. Irfan M, Shah T, Siddiqui GF, Rehman A, Saba T, Bahaj SA (2022) Design of Nonlinear Component of block cipher using Gravesian Octonion integers. IEEE Access
26. Jamal SS, Anees A, Ahmad M, Khan MF, Hussain I (2019) Construction of cryptographic S-boxes based on Mobius transformation and chaotic tent-sine system. IEEE Access 7:173273–173285
27. Joan D, Vincent R (2013) The Design of Rijndael: AES-the advanced encryption standard. Springer, New York
28. Kanmani M, Narasimhan V (2019) An optimal weighted averaging fusion strategy for remotely sensed images. Multidim Syst Sign Process 30:1911–1935
29. Kanmani M, Narasimhan V (2019) Particle swarm optimisation aided weighted averaging fusion strategy for CT and MRI medical images. Int J Biomed Eng Technol 31(3):278–291
30. Kanmani M, Narasimhan V (2020) Optimal fusion aided face recognition from visible and thermal face images. Multimed Tools Appl 79:17859–17883
31. Khan M, Shah T (2013) An efficient construction of substitution box with fractional chaotic system. Signal Image Video Process 9:1335–1338
32. Khan M, Shah T, Mahmood H, Gondal MA (2012) An efficient method for the construction of block cipher with multi-chaotic systems. Nonlinear Dyn 71:489–492
33. Khan MAM, Azam NA, Hayat U, Kamarulhaili H (2023) A novel deterministic substitution box generator over elliptic curves for real-time applications. J King Saud Univ-Comp Inform Sci 35(1):219–236
34. Koblitz N (1987) Elliptic curve cryptosystems. Math Comput 48(177):203–209
35. Liu J, Wei B, Cheng X, Wang X (2005) An AES s-box to increase complexity and cryptographic analysis.Vin 19th. In: International conference on advanced information networking and applications, 2005. AINAv2005, vol 1. IEEE, pp 724–728
36. Liu G, Yang W, Liu W, Dai Y (2015) Designing S-boxes based on 3-D four-wing autonomous chaotic system. Nonlinear Dyn. 82:1867–1877
37. Magdy M, Hosny KM, Ghali NI, Ghoniemy S (2022) Security of medical images for telemedicine: a systematic review. Multimed Tools Appl 81(18):25101–25145

38. Malik MSM, Ali A, Khan MA, Ehatisham-ul-Haq M, Mehmood SN, Rehman M, Ahmad W (2020) Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. IEEE Access:1–1
39. Miller VS (1985) Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques (pp. 417-426). Springer, Berlin, Heidelberg
40. Naseer Y, Shah T, Shah D, Hussain S (2019) A novel algorithm of constructing highly nonlinear S-p-boxes. Cryptography 3(1):6
41. Ozkaynak F (2020) On the effect of chaotic system in performance characteristics of chaos-based S-box designs. Physica A Stat Mech Appl 550:124072
42. Ozkaynak F, Ozer AB (2010) A method for designing strong S-boxes based on chaotic Lorenz system. Phys Lett A 374:3733–3738
43. Ozkaynak F, Yavuz S (2013) Designing chaotic S-boxes based on time-delay chaotic system. Nonlinear Dyn. 74:551–557
44. Pund-Dange S, Desai CG (2017) Data hiding technique using Catalan-Lucas number sequence, Indian. J Sci Technol 10(4)
45. Razaq A, Yousaf A, Shuaib U, Siddiqui N, Ullah A, Waheed A (2017) A novel construction of substitution box involving coset diagram and a bijective map, security and communication. Networks |Article ID 5101934
46. Razaq A, Yousaf A, Shuaib U, Siddiqui N, Ullah A, Waheed A (2017) A novel construction of substitution box involving coset diagram and a bijective map, Hindawi security and communication. Networks
47. Razaq A, Al-Olayan HA, Ullah A, Riaz A, Waheed A (2018) A novel technique for the construction of safe substitution boxes based on cyclic and symmetric groups. Secur Comm:1–9
48. Razaq A, Alolaiyan H, Ahmad M, Yousaf MA, Shuaib U, Aslam W, Alawida M (2020) A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups. IEEE Access 8:75473–75490
49. Sani RH, Behnia S, Akhshani A (2021) Creation of S-box based on a hierarchy of Julia sets: image encryption approach. Multidim Syst Sign Process
50. Sarfraz M, Hussain I, Ali F (2016) Construction of S-box based on Mobius transformation and increasing its confusion creating ability through invertible function. int J Comput Sci Inform Sec 14(2)
51. Shahzad I, Mushtaq Q, Razaq A (2019) Construction of new S-box using action of quotient of the modular group for multimedia security. Sec Comm Networks 1–13:2019
52. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Techn J 28(4):656–715
53. Siddiqui N, Naseer A, Ehatisham-ul-Haq M (2020) A novel scheme of substitution-box design based on modified pascal's triangle and elliptic curve. Wirel Pers Commun
54. Siddiqui N, Yousaf F, Murtaza F, Ehatisham-ul-Haq M, Ashraf MU, Alghamdi AM (2020) A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field. PLoS One 15(11)
55. Siddiqui N, Khalid H, Murtaza F, Ehatisham-Ul-Haq M, Azam M A., a novel algebraic technique for design of computational substitution-boxes using action of matrices on galois field. Digital Object Identifier. https://doi.org/10.1109/ACCESS.2020
56. Theresa XB, Madheswari K (2018) Thermal and visible video fusion using curvelet transform. Int J Appl Eng Res 13(11):8831–8836
57. Tran MT, Bui DK, Duong AD (2008) Gray S-box for advanced encryption standards. In: In 2008 international conference on computational intelligence and security, vol 1. IEEE, pp 253–258
58. Ullah I, Azam N A., Hayat U., efficient and secure substitution box and random number generators over Mordell elliptic curves. J Inform Sec Appl. https://doi.org/10.1016/j.jisa.2020.102619
59. Ullah A., Jamal S. S., Shah T., A novel algebraic technique for the construction of strong substitution box, Wirel Pers Commun, volume 99, issue 1, pp 213–226, March 2018.
60. Vinay DR (2021) A cryptographic based approach for data hiding in advanced video sequences. Turkish J Comput Math Educ (TURCOMAT) 12(6):2031–2038
61. Zahid AH, Al-Solami E, Ahmad M (2020) A novel modular approach based substitution-box design for image encryption. IEEE Access 8:150326–150340
62. Zhang Y-Q, Hao J-L, Wang X-Y (2020) An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map, IEEE. Access 8:4175_54188