Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.040371

ARTICLE

A Mathematical Approach for Generating a Highly Non-Linear Substitution Box Using Quadratic Fractional Transformation

Abid Mahboob[1], Muhammad Asif[2], Rana Muhammad Zulqarnain[3,*], Imran Saddique[4], Hijaz Ahmad[5] and Sameh Askar[6]

[1]Department of Mathematics, Division of Science and Technology, University of Education, Lahore, Pakistan

[2]Department of Mathematics, University of Management and Technology, Sialkot Campus, 51310, Pakistan

[3]School of Mathematical Sciences, Zhejiang Normal University, Jinhua, 321004, China

[4]Department of Mathematics, University of Management and Technology, Lahore, 54770, Pakistan

[5]Section of Mathematics, International Telematic University Uninettuno, Corso Vittorio Emanuele II, Roma, 39-00186, Italy

[6]Department of Statistics and Operations Research, College of Science, King Saud University, P.O. Box 2455, Riyadh, 11451, Saudi Arabia

*Corresponding Author: Rana Muhammad Zulqarnain. Email: ranazulqarnain7777@gmail.com

Received: 15 March 2023 Accepted: 07 June 2023 Published: 29 November 2023

ABSTRACT

Nowadays, one of the most important difficulties is the protection and privacy of confidential data. To address these problems, numerous organizations rely on the use of cryptographic techniques to secure data from illegal activities and assaults. Modern cryptographic ciphers use the non-linear component of block cipher to ensure the robust encryption process and lawful decoding of plain data during the decryption phase. For the designing of a secure substitution box (S-box), non-linearity (NL) which is an algebraic property of the S-box has great importance. Consequently, the main focus of cryptographers is to achieve the S-box with a high value of non-linearity. In this suggested study, an algebraic approach for the construction of 16×16 S-boxes is provided which is based on the fractional transformation $\boldsymbol{Q}(z) = \dfrac{\mathbf{1}}{\boldsymbol{\alpha}(z)^{m} + \boldsymbol{\beta}} (\boldsymbol{mod257})$ and finite field. This technique is only applicable for the even number exponent in the range (2-254) that are not multiples of 4. Firstly, we choose a quadratic fractional transformation, swap each missing element with repeating elements, and acquire the initial S-box. In the second stage, a special permutation of the symmetric group $\boldsymbol{S}_{\mathbf{256}}$ is utilized to construct the final S-box, which has a higher NL score of 112.75 than the Advanced Encryption Standard (AES) S-box and a lower linear probability score of 0.1328. In addition, a tabular and graphical comparison of various algebraic features of the created S-box with many other S-boxes from the literature is provided which verifies that the created S-box has the ability and is good enough to withstand linear and differential attacks. From different analyses, it is ensured that the proposed S-boxes are better than as compared to the existing S-boxes. Further these S-boxes can be utilized in the security of the image data and the text data.

KEYWORDS

Block cipher; S-box; data security; fractional transformation

1 Introduction

The amount of data being exchanged has risen substantially as a result of recent technology advancements and its successful use in daily life. The confidential nature of data necessitates the development of tools and safeguards against misuse. Data from a user must be altered before transmission so that an attacker cannot understand it. Symmetric block ciphers have become among the most extensively utilized approaches for such purposes given their ease of implementation and able to give much-required encryption security [1,2]. By utilizing a symmetric key and a varied number of several rounds, one common sort of block cipher converts an input block of data into a nonsensical output block via substitution and permutation techniques. On the input block of data, substitution, and permutation operations are typically performed in each cycle. A replacement process uses a substitution box (S-box) to swap out an input block with another output block [3]. The most widely used symmetric block cipher is AES, as an illustration.

S-box is a Vectorial Boolean function that is defined mathematically as, $\varphi\colon \mathbb{Z}_2^u \rightarrow \mathbb{Z}_2^v$ which maps the u input bit into the v output bit. As a crucial part of modern block ciphers, an S-box creates a randomized cipher text from the input plaintext. The single nonlinear component of contemporary block ciphers is the S-box, which provides a complicated link between the plaintext and the cipher text. The algebraic and statistical features of the S-box, such as non-linearity, Bit Independent Criterion (BIC), Strict Avalanche Criterion (SAC), Differential Uniformity (DU), and Linear Approximation Probability (LAP) are used to assess its validity. Numerous methods and technologies are used throughout literature to create securely powerful Substitution-boxes. A method to create robust and resistant S-boxes that can help in the modification of block cryptosystems was proposed by Dragomir et al. [4]. The authors of [5] proposed a novel S-box constructed system using group theory ideas. Reference [6] Describes a unique genetic approach for evolving S-boxes with high non-linearity scores. Artuğer et al. [7] present a new technique for improving the performance of Chaos-Based S-boxes. They have implemented their system on a large number of S-boxes. In [8], an efficient algebraic approach for evolving S-boxes with reasonable strength is presented. Particle Swarm Optimization was used by Musheer et al. [9] to generate a robust S-box. In [10], an efficient S-box with essentially optimum characteristics was created. For this, the authors used a methodical group theoretical method. Javeed et al. [11] created an S-box with outstanding cryptographic features using a freshly created chaotic map and the suitable S_{256} component. In [12], Khan et al. created an S-box utilizing (Difference Distribution Table) DDT and a chaotic logistic map. In contrast to previously established S-boxes based on chaos, it was a significant effort to generate an S-box that had an extremely low value of differential approximation probability. To construct an S-box that has excellent cryptographic features, Ahmad et al. [13] suggested a unique approach that utilizes artificial bee colony optimization and chaotic maps. A unique method to build safe S-boxes using the fractional-order chaotic Chen scheme was put out by Özkaynak et al. [14]. To ensure the accuracy of Chen scheme's numerical findings, they used the predictor-corrector approach. It is a straightforward approach for creating an S-box using Chen's fractional-order chaotic Chen scheme. By utilizing Lorenz equations, Khan et al. [15] established a novel S-box method of construction. To develop a robust S-box, Ahmad et al. looked at the traveling salesman problem and piecewise linear chaotic map [16]. Five strong S-boxes were created by Ullah et al. [17] using a chaotic map and a linear fractional transformation (LFT). Different techniques are utilized for the construction of S-boxes and other techniques to solve different model issues [18–29].

This article is a continuation of the work done by Mahboob et al. [30] to create an S-box using a Quantic Fractional Transformation and finite field. They used the mapping $Q\left(x\right) = \dfrac{1}{a\left(x\right)^m + b}$ to construct a reliable S-box in their research, although it was only effective for odd values of m in the range of (0–255), and the authors also demonstrated that this mapping is bijective for odd values of m but there is no construction of S-boxes is available in literature which uses the fractional transformation $\frac{1}{a\,(z)^m + b}$ when $m \in \{2 + 4n|0 \leq n \leq 63\}$ since the proposed mapping is not bijective in this fashion. We provide a unique approach for the creation of S-boxes utilizing this fractional transformation and use $m = 2$ for an example to create a specimen S-box in this paper. By changing the value of m, we may create several S-boxes. The following is the main contribution of our study in this paper:

1. An innovative and simple fractional transformation is defined for the construction of S-boxes. By altering their parameters, a large number of S-boxes can be constructed using this technique.
2. We use the Quadratic Fractional Transformation (QFT) as an illustration to create a specimen S-box by maintaining the value of $m = 2$.
3. To boost the unpredictability of the first S-box, suitable permutations of the symmetric group were utilized, and the suggested S-box was constructed whose average nonlinearity is 112.75 which is greater than AES S-box.
4. Additionally, visual and tabular comparisons of various algebraic analyses, including NL, BIC, DU, SAC, and LAP of the proposed S-box, were used, and a comparison of these results with the other S-boxes established in literature is presented to demonstrate that the suggested S-box is capable of withstanding linear and differential attacks.

The remainder of the paper is arranged as follows: Section 2 delves into the algebraic structure of the S-box's construction. In Section 3, the constructed S-box is examined through its security analysis, and its results are compared with those of other S-boxes. In Section 4, we illustrate the discussion of our results and discuss our findings. Finally, Section 5 concludes the study.

2 Mathematical Structure

Step 1: To begin, let us define a fractional transformation, $Q\colon \mathbb{Z}_{257} \rightarrow \mathbb{Z}_{257}$ as [30]:

$$Q\,(z) = \frac{1}{\alpha\,(z)^m + \beta}(mod\,257), \alpha\,(z)^m + \beta \neq 0, \tag{1}$$

where $\alpha \in \mathbb{Z}_{257} - \{0\}\,, \beta \in \mathbb{Z}_{257}$, & $m \in \{2 + 4n|0 \leq n \leq 63\}$.

This Eq. (1) is taken from [30].

Given that a bijective 16 × 16 S-box is essentially any rearrangement of the numbers (0–255). The Prime Field $\mathbb{Z}_{257}$ is frequently used to ensure that all outputs remain within this range. Due to this, we restrict the parameters α and β. These parameters allow for the creation of a vast number of S-boxes because each adjustment to one of the parameters results in the creation of a new S-box that differs from the previous ones.

Here we choose $m = 2$, $\alpha = 57$ & $\beta = 24$ to generate a specimen substitution box, then the quadratic fractional transformation (QFT) becomes:

$$Q\,(z) = \frac{1}{57\,(z)^2 + 24}(mod\,257), z \in \mathbb{Z}_{257} \tag{2}$$

After that, put all the elements from $\mathbb{Z}_{257}$ into Eq. (2) and then write the outputs in a set W obtained from the quadratic fractional transformation after solving under $mod\,257$.

$W = \{Q(z)|z \in \mathbb{Z}_{257}\}$

Since it is to be noted that the set W may include the number 256 but never have 0 we deducted 1 from each element of the set W to maintain the range (0–255).

Finally, to keep the S-box bijective, we put all missing numbers from (0–255) in ascending order in set $\{u_1, u_2, \ldots, u_n\}$ and duplicated numbers from (0–255) in descending order in set $\{v_1, v_2, \ldots, v_n\}$ and replace every u_j by v_j for $j = 1, 2, \ldots, n$.

Table 1 explains the above method for eradicating the sequence $\{0, 1, 2, 3, \ldots, 255\}$. After destroying the initial sequence of numbers $\{0, 1, 2, \ldots, 255\}$, we retrieved our initial S-box 16×16 matrix present in Table 2, whose average nonlinearity is 103.25.

Table 1: Initial S-box construction based on quadratic fractional transformation

$z \in Z$	$Q(z) = \dfrac{1}{57(z)^2 + 24} \, mod\,(257)$	$W = \{w_i\}$	$w_i - 1$	S-box elements
0	$Q(0) = \dfrac{1}{57(0)^2 + 24}$	75	74	74
1	$Q(1) = \dfrac{1}{57(1)^2 + 24}$	165	164	164
2	$Q(2) = \dfrac{1}{57(2)^2 + 24}$	154	153	153
3	$Q(3) = \dfrac{1}{57(3)^2 + 24}$	190	189	189
4	$Q(4) = \dfrac{1}{57(4)^2 + 24}$	81	80	80
254	$Q(254) = \dfrac{1}{57(254)^2 + 24}$	190	189	56
255	$Q(255) = \dfrac{1}{57(255)^2 + 24}$	154	153	97

Table 2: Initial S-box

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

Step 2: To improve the random nature of our constructed S-box, we utilized a permutation of symmetric group S_{256} (shown in Table 3) to modify the location of the S-box's elements and generated a proposed S-box (shown in Table 4) with a mean non-linearity value of 112.75.

Table 3: Permutation of S_{256}

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

Table 4: Proposed S-box

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

3 Security Analysis

In this part, we assess the cryptographic performance of recommended S-box (provided in Table 4) to generally recognized traditional S-box performance criteria. Five essential evaluations are utilized to assess the resilience of the S-box: nonlinearity, linear approximation probability, bit independence criterion, differential approximation probability, and strict avalanche criterion. We achieve fantastic results, which shows the high quality of the planned design.

3.1 Nonlinearity (NL)

This is a critical factor for determining the efficacy of S-box in contrast to linear and differential cryptanalysis. Pieprzyk and Finkelstein introduced this test in 1988 [31]. The nonlinearity of $\psi : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$, where ψ is a Boolean function of n variables is defined as the minimum distance among ψ and the set of affine transformations A_n.

$$NL(\psi) = d(\psi, A_n) = {}^{min}_{\gamma \epsilon A_n} d(\psi, \gamma) \tag{3}$$

Accordingly, the NL score is 0 when all affine transformations are linear. For $n \times n$ S-box, the highest value of NL is, $2^{n-1} - 2^{\frac{n}{2}-1}$. Thus, the ideal value of NL over $GF\left(2^8\right)$ is 120 in AES. The high NL value of the S-box is a crucial component for creating a good cryptosystem. The recommended S-box has a minimum value of nonlinearity is 112, the maximum value of nonlinearity is 114, and the mean value of nonlinearity is 112.75. Table 5 displayed the NL scores for 8 Boolean functions, and Fig. 1 contrasts the mean NL number of the final S-box with those of numerous other S-boxes.

Fig. 1 shows the comparison of non-linearity of our purposed S-box and existing S-boxes. The non-linearity is the very important and main component to check the strength of S-box. So, from Fig. 1, it is ensured that our S-box have average non-linearity 112.75 which is higher than other existing S-boxes.

Table 5: Nonlinearity score of proposed S-box

Boolean functions	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5	ψ_6	ψ_7	ψ_8
Score	114	112	114	112	112	112	114	112

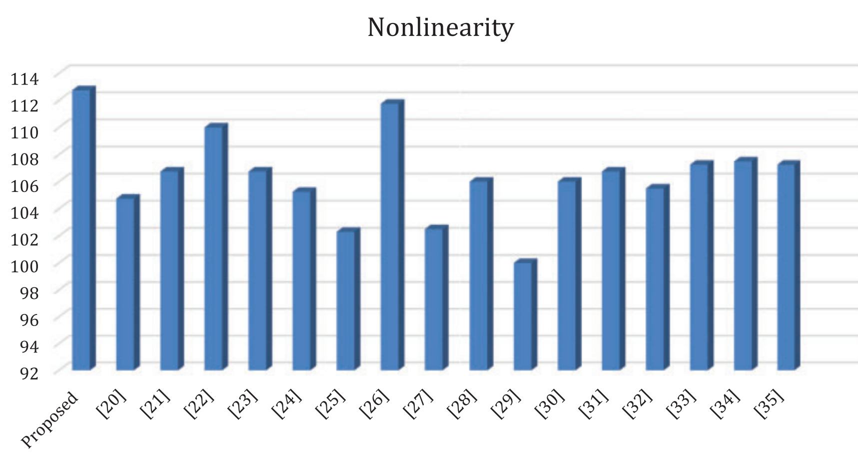

Figure 1: Analysis of mean NL score of suggested S-box with various S-boxes

3.2 Strict Avalanche Criterion (SAC)

In [32], Webster et al. suggested this essential algebraic criterion of S-box. SAC shows that output bits changed by $\frac{1}{2}$ of probability or 50% if a single bit changes in the input result. S-box is considered strong against cryptanalyst attacks whose SAC value is 0.5. The SAC criterion is conducted by using a dependency matrix. The SAC value of the suggested S-box is present in Table 6, which is close to the ideal value of SAC.

Table 6: SAC values

0.5156	0.4844	0.4844	0.5156	0.4844	0.5156	0.5	0.4531
0.4688	0.4688	0.5156	0.4531	0.4844	0.5312	0.5	0.5156
0.5469	0.4688	0.5156	0.5156	0.5	0.5469	0.5	0.4531
0.4688	0.4844	0.5469	0.5469	0.5	0.5156	0.5625	0.4844
0.4844	0.5	0.4531	0.5312	0.5	0.5312	0.5	0.4844
0.4531	0.5	0.4688	0.5312	0.5312	0.5	0.4688	0.5156
0.5	0.4844	0.4688	0.4219	0.4844	0.5156	0.4844	0.5
0.5312	0.5156	0.4688	0.4531	0.5156	0.4844	0.5	0.5

3.3 Bit Independence Criterion (BIC)

This is another relevant criterion for measuring the strength of the S-box, which is defined as the two output bits changing independently when any single input is modified. Webster et al. [32] presented BIC as an effective criterion in symmetric cryptosystems. Table 7 shows the BIC Non-linearity values of the proposed S-box.

Table 8 provide the BIC-SAC values for the final S-box.

Table 7: BIC nonlinearity values

0	106	104	100	104	102	106	100
106	0	104	106	100	100	98	102
104	104	0	106	104	106	104	104
100	106	106	0	104	106	104	106
104	100	104	104	0	104	106	102
102	100	106	106	104	0	108	100
106	98	104	104	106	108	0	106
100	102	104	106	102	100	106	0

Table 8: BIC SAC values

0	0.5098	0.5039	0.5156	0.5215	0.4941	0.4902	0.5059
0.5098	0	0.4863	0.4941	0.5312	0.4941	0.4941	0.5
0.5039	0.4863	0	0.4844	0.4824	0.5176	0.5195	0.4844

(Continued)

Table 8 (continued)

0	0.5098	0.5039	0.5156	0.5215	0.4941	0.4902	0.5059
0.5156	0.4941	0.4844	0	0.5176	0.5098	0.5039	0.4785
0.5215	0.5312	0.4824	0.5176	0	0.5059	0.4746	0.4922
0.4941	0.4941	0.5176	0.5098	0.5059	0	0.5156	0.502
0.4902	0.4941	0.5195	0.5039	0.4746	0.5156	0	0.498
0.5059	0.5	0.4844	0.4785	0.4922	0.502	0.498	0

Table 9 and Fig. 2 provide a comparison of the BIC NL and BIC SAC values of the proposed S-box with existing S-boxes.

Table 9: Analysis between SAC and BIC-NL scores of suggested S-box and other S-boxes

S-boxes	SAC	BIC-NL
Proposed	0.4973	103.64
[33]	0.4931	102
[34]	0.4988	102
[35]	0.4861	108
[36]	0.5031	96
[37]	0.5026	100
[38]	0.483	101.57
[39]	0.502	103.7
[40]	0.5037	103.92
[41]	0.4978	103.92
[42]	0.4812	96
[43]	0.5066	96
[17]	0.4939	102
[44]	0.4946	96
[45]	0.5034	98
[46]	0.4980	103.5
[47]	0.501	107

3.4 Differential Uniformity (DU)

Biham et al. [48] devised this test. To overcome differential assaults, a low value of differential uniformity (DU) is proposed, and S-box is deemed more secure. Eq. (4) provides a mathematical formula for calculating the DU.

$$DU_{\psi} = max_{\Delta r \neq 0, \Delta s}[\#\{r \in M | \psi(r) \oplus \psi(r \oplus \Delta r) = \Delta d\}] \quad (4)$$

where $M = \{0, 1, 2, \ldots, 255\}$, Δs and Δr denote output and input differentials respectively, ψ is a Boolean function and the symbol $\oplus$ represents the XOR operation. Table 10 depicts the suggested S-box's differential distribution table. The maximum DU score of the suggested S-box is 12 and the differential probability (DP) value is 0.0468. This low DP score demonstrated that the S-box is highly resistant to differential assaults. Table 11 compares DU with several S-boxes, and Fig. 3 depicts a graphical comparison of the suggested S-box's DP values with those of previously developed S-boxes in the literature.

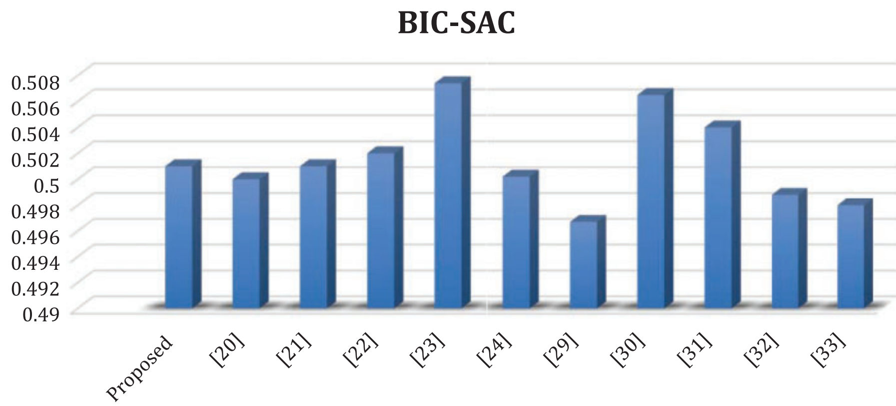

Figure 2: Analysis among BIC-SAC values of proposed S-box with other S-boxes

Table 10: Input/output XOR distribution table

6	6	6	6	8	6	8	8	6	6	6	6	8	8	6	6
6	8	6	8	6	8	6	6	8	8	6	6	6	6	6	8
6	6	8	6	8	8	8	6	6	6	6	6	8	6	6	6
6	6	6	8	8	6	8	6	10	6	6	6	6	6	6	6
8	6	6	6	6	8	6	6	6	8	6	6	6	6	6	6
6	6	8	8	6	8	6	6	6	6	6	6	8	8	6	6
6	8	8	6	6	6	10	6	8	8	6	6	8	10	6	6
6	6	8	6	6	6	6	6	6	6	8	6	6	6	8	6
6	8	8	10	6	6	6	6	6	6	6	6	6	10	8	6
6	6	6	8	8	6	8	6	6	8	6	8	6	6	6	6
6	6	8	8	6	6	8	4	8	8	8	6	6	8	8	6
6	8	6	8	8	6	4	6	6	8	6	8	10	4	6	8
6	8	6	10	8	6	6	6	6	6	6	6	8	6	6	6
10	6	8	6	6	6	10	8	6	6	6	6	6	6	6	6
8	8	6	6	6	6	10	8	6	6	4	6	6	12	8	6
6	8	8	8	8	8	8	6	8	4	8	8	6	6	6	0

3.5 Linear Approximation Probability (LAP)

LAP criterion is used to check the strength and resistance of the S-box to linear assaults. In [49], Matsui provided this algebraic feature of S-box. The S-box is considered more secure whenever the value of LAP is smaller. A mathematical formula to calculate LAP is:

$$LAP = max_{\lambda_p,\lambda_q \neq 0} \left| \frac{\#\{p|p.\lambda_p = \psi\ (p)\ .\lambda_q\}}{2^n} - \frac{1}{2} \right| \tag{5}$$

where λ_p and λ_q denote the input and output mask, respectively, 2^n is the total number of elements of the S-box and ψ represents the Boolean functions. The LAP value of the created S-box is 0.13281. Table 11 indicates the comparison among the LAP scores of the suggested S-box and various other S-boxes.

Table 11: Analysis between DU and LAP scores of recommended S-boxes with some other S-boxes

S-boxes	DU	LAP
Proposed	12	0.1328
[33]	10	0.125
[34]	30	0.125
[35]	6	0.0859
[36]	12	0.1484
[37]	12	0.1172
[38]	14	0.167
[39]	10	0.125
[40]	10	0.125
[41]	12	0.1563
[42]	16	0.1796
[43]	12	0.1445
[17]	16	0.125
[44]	10	0.1328
[45]	12	0.1328
[46]	10	0.14063
[47]	6	0.109

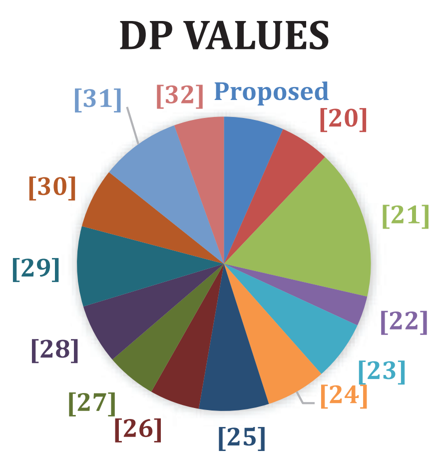

Figure 3: Pie chart of DP values of recommended S-box with some other S-boxes

4 Results and Discussion

Researchers' major emphasis for the creation of powerful substitution boxes is a significant nonlinearity score. Our S-box has a mean nonlinearity of 112.75, which is higher than the AES S-box as well as the other S-boxes from the literature shown in Table 6.

1. The S-box creators' ultimate goal is to obtain the ideal SAC value of 0.5. Our S-box has a SAC score of 0.4973, which is close to 0.5 when contrasted to other S-boxes in Table 10. We can claim that our S-box is impervious to cryptanalysis.
2. The proposed S-box BIC NL and BIC SAC scores are 103.64 and 0.501, respectively. Table 9 and Fig. 2 provide a comparison of the values of BIC NL and BIC SAC.
3. Low DP S-boxes are resilient to different types of attacks. The DP score of the created S-box in Fig. 3 is 0.0468, which is lower than the DP numbers of many other S-boxes.
4. The recommended S-box's LAP value is 0.13281. This low value implies that the proposed S-box is resistant to linear assaults. Table 11 compares the LAP value of created S-box to that of other S-boxes.

5 Conclusion

In this study an algebraic strategy for generating the substitution boxes was introduced. This methodology depends on fractional transformation and finite field. We designed a general form of transformation and choose quadratic fraction transformation as an example to generate an S-box. The nonlinearity of the proposed S-box after applying the permutations of S_{256} is 112.75 which is higher than AES S-box. The other algebraic properties of the S-box are good enough to stand against linear and differential approaches. The comparison between the algebraic and statistical properties of our S-box with many other S-boxes from the literature indicates that the recommended S-box withstands cryptanalysis attacks and can be used further to improve a security. Although a static prototype S-box is created in this study, it will be feasible to create dynamic S-boxes in the future by utilizing the suggested mathematical methodology, which will enable the creation of a robust and effective cryptosystem that will safeguard sensitive and private data.

6 Limitation

This study develops a fractional transformation for creating substitution boxes that are applied to even values of m when $m = \{2, 6, 10, \ldots, 254\}$ and we simply swap each missing element with a repeating element to keep the S-box bijective. If m is a multiple of 4, it is impossible to construct an S-box and it is impossible to maintain the bijectivity of the S-box because elements repeat more than once.

Acknowledgement: The authors present their appreciation to King Saud University for funding the publication of this research.

Funding Statement: The authors received the funding for this study from King Saud University, Riyadh, Saudi Arabia under the research supporting project Number RSP 2024R167. Sameh Askar received this grant from King Saud University.

Author Contributions: The authors confirm their contribution to the paper as follows: Study conception and design: A. Mehboob, M.Asif, R. M. Zulqarnain; data collection: M. Asif, I. Saddique; analysis and interpretation of results: A. Mehboob, I. Siddique, H. Ahmad, S. Askar; draft manuscript preparation: A. Mehmood, R. M. Zulqarnain, H. Ahmad, S. Askar, All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: All data generated or analyzed during this study are included in this article and are available from the corresponding author upon reasonable request.

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

References

[1] C. Paar, J. Pelzl and B. Preneel, *Understanding Cryptography*, 1st ed., Berlin, Germany: Springer, 2010.
[2] A. Shamir, "Stream ciphers: Dead or alive?" in *ASIACRYPT*, pp. 78, 2004.
[3] D. Lambić and M. Živković, "Comparison of random S-Box generation methods," *De L'institut Mathématique*, vol. 93, no. 107, pp. 109–115, 2013.
[4] I. R. Dragomir and M. Lazăr, "Generating and testing the components of a block cipher," in *2016 8th Int. Conf. on Electronics, Computers and Artificial Intelligence (ECAI)*, Ploiesti, Romania, IEEE, pp. 1–4, 2016.
[5] I. Hussain, T. Shah, H. Mahmood and M. A. Gondal, "A projective general linear group based algorithm for the construction of substitution box for block ciphers," *Neural Computing and Applications*, vol. 22, no. 6, pp. 1085–1093, 2013.
[6] Y. Wang, Z. Zhang, L. Y. Zhang, J. Feng, J. Gao *et al.,* "A genetic algorithm for constructing bijective substitution boxes with high nonlinearity," *Information Sciences*, vol. 523, no. 1, pp. 152–166, 2020.
[7] F. Artuğer and F. Özkaynak, "A novel method for performance improvement of chaos-based substitution boxes," *Symmetry*, vol. 12, no. 4, pp. 571, 2020.
[8] S. Hussain, S. S. Jamal, T. Shah and I. Hussain, "A power associative loop structure for the construction of non-linear components of block cipher," *IEEE Access*, vol. 8, pp. 123492–123506, 2020.
[9] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami and W. Alhakami, "Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications," *IEEE Access*, vol. 8, pp. 116132–116147, 2020.
[10] M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar and A. Razaq, "Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes," *IEEE Access*, vol. 8, pp. 39781–39792, 2020.
[11] A. Javeed, T. Shah and A. Ullah, "Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group," *Wireless Personal Communications*, vol. 112, no. 1, pp. 467–480, 2020.
[12] M. A. Khan, A. Ali, V. Jeoti and S. Manzoor, "A chaos-based substitution box (S-Box) design with improved differential approximation probability (DP)," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 42, no. 2, pp. 219–238, 2018.
[13] M. Ahmad, M. N. Doja and M. S. Beg, "ABC optimization based construction of strong substitution-boxes," *Wireless Personal Communications*, vol. 101, no. 3, pp. 1715–1729, 2018.
[14] F. Özkaynak, V. Çelik and A. B. Özer, "A new S-box construction method based on the fractional-order chaotic Chen system," *Signal Image and Video Processing*, vol. 11, no. 4, pp. 659–664, 2017.
[15] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad and M. A. Khan, "A novel substitution box for encryption based on Lorenz equations," in *2017 Int. Conf. on Circuits, System and Simulation (ICCSS)*, London, UK, IEEE, pp. 32–36, 2017.
[16] M. Ahmad, N. Mittal, P. Garg and M. M. Khan, "Efficient cryptographic substitution box design using travelling salesman problem and chaos," *Perspectives in Science*, vol. 8, no. 3, pp. 465–468, 2016.
[17] A. Ullah, S. S. Jamal and T. Shah, "A novel construction of substitution box using a combination of chaotic maps with improved chaotic range," *Nonlinear Dynamics*, vol. 88, no. 4, pp. 2757–2769, 2017.
[18] I. Khalid, T. Shah, S. M. Eldin, D. Shah, M. Asif *et al.,* "An integrated image encryption scheme based on elliptic curve," *IEEE Access*, vol. 11, pp. 5483–5501, 2022.

[19] I. Khalid, T. Shah, K. A. Almarhabi, D. Shah, M. Asif *et al.,* "The spn network for digital audio data based on elliptic curve over a finite field," *IEEE Access*, vol. 10, pp. 127939–127955, 2022.
[20] A. Mahboob, M. Asif, I. Siddique, A. Saleem, M. Nadeem *et al.,* "A novel construction of substitution box based on polynomial mapped and finite field with image encryption application," *IEEE Access*, vol. 10, pp. 119244–119258, 2022.
[21] M. Asif, J. K. K. Asamoah, M. M. Hazzazi, A. R. Alharbi, M. U. Ashraf *et al.,* "A novel image encryption technique based on cyclic codes over galois field," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, pp. 1–9, 2022.
[22] S. Hussain, M. Asif, T. Shah, A. Mahboob and S. M. Eldin, "Redesigning the serpent algorithm by PA-Loop and its image encryption application," *IEEE Access*, vol. 11, pp. 29698–29710, 2023.
[23] A. S. Alanazi, N. Munir, M. Khan, M. Asif and I. Hussain, "Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes," *IEEE Access*, vol. 9, pp. 93795–93802, 2021.
[24] M. Khan, S. S. Jamal, M. M. Hazzazi, K. M. Ali, I. Hussain *et al.,* "An efficient image encryption scheme based on double affine substitution box and chaotic system," *Integration*, vol. 81, no. 3, pp. 108–122, 2021.
[25] M. Asif, S. Mairaj, Z. Saeed, M. U. Ashraf, K. Jambi *et al.,* "A novel image encryption technique based on mobius transformation," *Computational Intelligence and Neuroscience*, vol. 2021, no. 2, pp. 1–14, 2021.
[26] M. Asif and T. Shah, "BCH Codes with computational approach and its applications in image encryption," *Journal of Intelligent & Fuzzy Systems*, vol. 37, no. 3, pp. 3925–3939, 2019.
[27] A. Mahboob, M. Asif, R. M. Zulqarnain, I. Siddique, H. Ahmad *et al.*, "An innovative technique for constructing highly non-linear components of block cipher for data security against cyber attacks," *Computer Systems Science & Engineering*, vol. 47, no. 2, pp. 2547–2562, 2023.
[28] A. Mahboob, I. Siddique, M. Asif, M. Nadeem and A. Saleem, "Construction of highly non linear component of block cipher based on mclaurin series and mellin transformation with application in image encryption," *Multimedia Tools and Applications*, pp. 1–19, 2023.
[29] D. Shah, T. Shah and S. S. Jamal, "A novel efficient image encryption algorithm based on affine transformation combine with linear fractional transformation," *Multidimensional Systems and Signal Processing*, vol. 31, pp. 885–905, 2020.
[30] A. Mahboob, M. Asif, M. Nadeem, A. Saleem, I. Siddique *et al.,* "A cryptographic scheme for construction of substitution boxes using quantic fractional transformation," *IEEE Access*, vol. 10, pp. 132908–132916, 2022.
[31] J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," *IEE Proceedings E-Computers and Digital Techniques*, vol. 135, no. 6, pp. 325–335, 1988.
[32] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Conf. on the Theory and Application of Cryptographic Techniques*, Berlin, Heidelberg, Germany, Springer, pp. 523–534, 1985.
[33] I. Hussain, T. Shah, M. A. Gondal, W. A. Khan and H. Mahmood, "A group theoretic approach to construct cryptographically strong substitution boxes," *Neural Computing and Applications*, vol. 23, no. 1, pp. 97–104, 2013.
[34] S. S. Jamal, T. Shah and A. Attaullah, "A group action method for construction of strong substitution box," *3D Research*, vol. 8, no. 2, pp. 1–10, 2017.
[35] L. Shuai, L. Wang, L. Miao and X. Zhou, "S-boxes construction based on the Cayley graph of the symmetric group for UASNs," *IEEE Access*, vol. 7, pp. 38826–38832, 2019.
[36] A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah *et al.,* "A novel construction of substitution box involving coset diagram and a bijective map," *Security and Communication Networks*, vol. 2017, no. 48, pp. 1–16, 2017.
[37] I. Hussain, T. Shah, M. A. Gondal and W. A. Khan, "Construction of cryptographically strong 8×8 S-boxes," *World Applied Sciences Journal*, vol. 13, no. 11, pp. 2389–2395, 2011.
[38] S. S. Jamal, M. U. Khan and T. Shah, "A watermarking technique with chaotic fractional S-box transformation," *Wireless Personal Communications*, vol. 90, no. 4, pp. 2033–2049, 2016.

[39] A. H. Zahid, A. M. Iliyasu, M. Ahmad, M. M. U. Shaban, M. J. Arshad *et al.,* "A novel construction of dynamic S-box with high nonlinearity using heuristic evolution," *IEEE Access*, vol. 9, pp. 67797–67812, 2021.

[40] A. A. Abd EL-Latif, B. Abd-El-Atty and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics & Laser Technology*, vol. 116, no. 3, pp. 92–102, 2019.

[41] A. K. Farhan, R. S. Ali, H. Natiq and N. M. Al-Saidi, "A new S-box generation algorithm based on multistability behavior of a plasma perturbation model," *IEEE Access*, vol. 7, pp. 124914–124924, 2019.

[42] M. Khan, T. Shah and S. I. Batool, "Construction of S-box based on chaotic Boolean functions and its application in image encryption," *Neural Computing and Applications*, vol. 27, no. 3, pp. 677–685, 2016.

[43] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso and M. Aldape-Pérez, "Substitution box generation using Chaos: An image encryption application," *Applied Mathematics and Computation*, vol. 332, no. 1, pp. 123–135, 2018.

[44] M. Khan, T. Shah, H. Mahmood and M. A. Gondal, "An efficient method for the construction of block cipher with multi-chaotic systems," *Nonlinear Dynamics*, vol. 71, no. 3, pp. 489–492, 2013.

[45] S. S. Jamal and T. Shah, "A novel algebraic technique for the construction of strong substitution box," *Wireless Personal Communications*, vol. 99, no. 1, pp. 213–226, 2018.

[46] A. H. Zahid, E. Al-Solami and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," *IEEE Access*, vol. 8, pp. 150326–150340, 2020.

[47] B. Arshad, N. Siddiqui and Z. Hussain, "A novel method for designing substitution boxes based on mobius group," 2021. https://doi.org/10.21203/rs.3.rs-173305/v1

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

[49] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Workshop on the Theory and Application of of Cryptographic Techniques*, Berlin, Heidelberg, Germany: Springer, pp. 386–397, 1993.