Computers, Materials & Continua
DOI: 10.32604/cmc.2022.028765
Article

Tech Science Press

Mordell Elliptic Curve Based Design of Nonlinear Component of Block Cipher

Hafeez ur Rehman[1],*, Tariq Shah[1], Mohammad Mazyad Hazzazi[2], Ali Alshehri[3] and Bassfar Zaid[4]

[1]Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
[2]Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia
[3]Department of Computer Science, University of Tabuk, Tabuk, 71491, Saudi Arabia
[4]Department of Information Technology, University of Tabuk, Tabuk, 71491, Saudi Arabia
*Corresponding Author: Hafeez ur Rehman. Email: hrehman@math.qau.edu.pk
Received: 16 February 2022; Accepted: 14 April 2022

Abstract: Elliptic curves (ECs) are deemed one of the most solid structures against modern computational attacks because of their small key size and high security. In many well-known cryptosystems, the substitution box (S-box) is used as the only nonlinear portion of a security system. Recently, it has been shown that using dynamic S-boxes rather than static S-boxes increases the security of a cryptosystem. The conferred study also extends the practical application of ECs in designing the nonlinear components of block ciphers in symmetric key cryptography. In this study, instead of the Mordell elliptic curve (MEC) over the prime field, the Galois field has been engaged in constructing the S-boxes, the main nonlinear component of the block ciphers. Also, the proposed scheme uses the coordinates of MEC and the operation of the Galois field to generate a higher number of S-boxes with optimal nonlinearity, which increases the security of cryptosystems. The proposed S-boxes resilience against prominent algebraic and statistical attacks is evaluated to determine its potential to induce confusion and produce acceptable results compared to other schemes. Also, the majority logic criteria (MLC) are used to assess the new S-boxes usage in the image encryption application, and the outcomes indicate that they have significant cryptographic strength.

Keywords: Galois field; Mordell elliptic curve; nonlinearity; substitution box

1 Introduction

When it comes to electronic data transfer, digital technology and network communications have had a significant impact during the past few decades. Various issues about the privacy of sensitive data transmissions through open communication networks arise, as most of these networks are exposed to the public. Cryptography, steganography, and watermarking are the most common methods for securing information. The robust watermarking algorithm is presented in [1,2] to assure the safe transmission and storage of medical data and to prevent the leakage of patient information in telemedicine. Consequently, the security of sensitive data has been a significant focus of cryptography in recent decades. The researchers have proposed various information security strategies to counter the most recent security threats. S-box is a nonlinear component in numerous famous algorithms, especially in advanced encryption standards (AES) [3]. The security of all such cryptosystems is thus reliant on the cryptographic aspects of these S-boxes. Because of this, many researchers have expressed an interest in developing new and more effective S-boxes. The S-box is predicated on algebraic systems, which are impervious to linear and differential cryptanalysis; they have received a lot of interest because of their solid cryptographic properties. Thus, secure transmission based on various classes of S-boxes is always promoted. Like the AES, the affine power affine (APA) S-box is presented to increase algebraic complexity while maintaining accessible encryption features [4]. In [5], the action of the symmetric group S_8 over AES is utilized to generate S-boxes. The Gray S-box is generated by adding an extra transformation based on binary gray codes to the basic AES S-box by employing a polynomial of 255 terms instead of a polynomial having 8 terms, which retains all the features and strengthens AES security [6]. Also, the chaotic map-based generators produced secure S-boxes that were impenetrable to the linear, differential, and algebraic attacks. In [7], a sturdy S-Box design is proposed by using a continuous-time Lorenz system as the chaotic system. By effectively exploiting the characteristics of a chaotic map and the evolution process, a method of S-boxes is presented in [8]. However, a parallel and more uncomplicated technique for constructing a block cipher nonlinear component is still required.

1.1 Related Work

ECs have recently gained a lot of interest in the cryptography sector. The techniques based on ECs are the most extensively used for enhancing information security. We will concentrate on EC-based cryptography and the various methods presented by numeral experts in this domain. Cheon et al. [9] characterized S-boxes by offering the relation between nonlinearity of rational functions over F_{2^n} and the points are lying on the corresponding hyper EC. Hayat et al. [10] designed an algorithm for constructing an 8×8 S-box using an x-coordinate of ordered EC over a prime field. Reference [11] is a refinement of the previous work; Hayat et al. use the x-coordinate of an EC over prime field followed by modulo operation to construct a different number of S-boxes. An algorithm for designing 8×8 S-boxes has been developed by Azam et al. [12] by using specific orderings on a class of Mordell elliptic curves (MEC). A search method is used rather than more configuration group rules to build EC points, which is computationally expensive. These techniques can be used to make a various number of 8×8 S-boxes. However, their conclusion is unpredictable because they are independent of any specific EC that may or may not produce an S-box for any input variables. Farwa et al. [13] offered an exceptional and new way for developing a 4×4 S-box by applying an EC over the Galois field $GF\left(2^4\right)$. In this paper, the authors constructed a bijective Boolean function by applying the structure of a group to the elements of EC having the same order as the order of the Galois field. Recently, Rehman et al. [14] designed an algorithm for the construction of a higher number of different 8×8 S-boxes by deploying MEC over the Galois field $GF\left(2^n\right)$ where $n = 8$ or an odd $n \geq 9$.

1.2 Motivation

The following are the key motives for this scheme to boost the performance of ECs based S-boxes and their effectiveness in numerous cryptographic algorithms.

1. S-boxes are typically constructed by considering ECs over prime fields. Yet, the outcomes of these studies remain uncertain. i.e., the algorithms do not invariably output an S-box to every set of specified parameters.
2. Furthermore, the prime field-based S-boxes do not encompass all the S-box possibilities.

3. In [11], the authors design an algorithm by choosing a particular EC over the Galois field $GF\left(2^4\right)$ and they are constructing a single 4×4 S-box.
4. In [12], they considered MEC over Galois field $GF(2^n)$, where $n = 8$ or an odd $n \geq 9$ and develop a practical scheme for the generation of 8×8 S-boxes but did not attain the optimal results, also they generate a single 8×8 S-box while utilizing MEC over the Galois field of order 256. However, in this study, we bring a comprehensive approach to design an algorithm by employing MEC over the Galois field $GF(2^n)$, where $n \geq 8$ and generate 8×8 S-boxes having outstanding results.

1.3 Our Contribution

To overcome the shortcomings of current schemes, we have developed a new one. To summarize a lengthy piece of writing, follow these steps:

1. We implemented a simple technique rather than rigorous S-boxes algorithms with exceptional outcomes to construct 8×8 S-boxes in the proposed work.
2. We utilized MEC over the Galois fields $GF(2^n)$ with $n = 8, 9, 10$ and higher with different numbers of primitive irreducible polynomials (PIPs) to generate points of EC.
3. Following the current approach, we used the EC points, prime numbers characteristics that rely on an EC x and y-coordinates, and an Inverse function under a predefined Galois field and PIP.
4. S-box figures can be changed by varying the MEC variable b or by amending the PIP of a degree equivalent to the Galois field $GF(2^n)$.

The following documents still need to be executed: Some introductory details are given in Section 2. The proposed algorithm can be found in Section 3. In Section 4, we compared our newly developed S-boxes to other S-boxes already in use. Section 4 also deals with S-boxes in the image encryption technique and the majority logic criterion (MLC). Towards the end of Section 5, there are several compelling arguments.

2 Preliminaries

In this part, several fundamental and crucial notions like ECs, Galois fields, Euler's phi function, and primitive polynomials are presented.

2.1 Galois Fields

A mathematical concept is known as finite field, or Galois field is considered the cornerstone of all cryptography theory. The representation of Galois field is $GF(p^n)$, where p signifies any prime number and $n \in Z^+$. Galois fields can be roughly divided into two categories: prime fields, which have $p = 1$, and extension fields, which have $p > 1$.

2.2 Euler's Phi Function

Euler's phi function offers the coprime numbers to an integer m, denoted as $\varphi(m)$, [15]. To put it another way, when the number m is greater than one, $\varphi(m)$ is the number of elements in U_m.

2.3 Primitive Irreducible Polynomials (PIPs) and Galois Fields

Galois field and PIPs over the Galois field are explained below in [16]. If it isn't explicitly stated, the base field $GF(2)$ is used in this section.

2.3.1 Definition

For each prime number p and positive integer m with order p^m, there is one finite field. The elements of these finite fields under multiplication form a cyclic group excluding zero. Consequently, there is a generator α that generates finite field apart from zero and $\alpha^{p^m-1} = 1$.

2.3.2 Definition

An irreducible polynomial in $GF(p)[X]$ cannot be reduced into a pair of lower-degree polynomials in $GF(p)[X]$. For example, the polynomial $x^3 + x + 1$ is irreducible in $GF(2^3)$ and $x^3 + 1$ is reducible.

2.3.3 Definition

A polynomial $h(x) \in GF(p^m)[X]$ is known as a primitive polynomial of degree m if all its roots are also primitive elements in the corresponding Galois field. Irreducible polynomials of degree m that are binary primitives are $\frac{\varphi(2^m - 1)}{m}$, where φ represents Euler's phi function. For example, if $p = 2$ and $n = 4$, then $\frac{\varphi(2^4 - 1)}{4} = 2$.

2.3.4 Lemma

An EC of the form $E_{p,b}: y^2 = x^3+b$ is known as MEC, where p is used for prime field. The specialty of this curve is that it has precisely $p + 1$ points for the prime number of forms $p \equiv 2\ (mod 3)$. Also, y-coordinates of this specified MEC are random, Washington [17](6.6 (c) , p.188) .

*2.3.5 Addition, Subtraction, and Multiplication in **GF** $(\mathbf{2^n})$*

The addition and subtraction operations are identical because we are operating in characteristic 2. Adding polynomials in Galois Field [18] is relatively easy. In multiplication let $h^*(x)$ is PIP of order m and $f^*(x), g^*(x)$ are polynomials in $GF(2^n)$, then

$$m^*(x) = (f^*(x) \cdot g^*(x))\ mod\ h^*(x) \tag{1}$$

where $m^*(x)$ is the resultant polynomial.

And $k^*(x)$ provides the multiplicative inverse of $g^*(x)$, i.e.,

$$(g^*(x) \cdot k^*(x))\ mod\ h^*(x) = 1 \tag{2}$$

Multiplying two polynomials and finding the multiplicative inverse of a polynomial need's modulo 2 for coefficients and modulo $h^*(x)$ for polynomials.

3 S-boxes Design by MEC over $GF(2^n)$, for $n \geq 8$

Here, the proposed S-box algorithm is described using two different approaches. In the first technique, we used MEC over Galois field $GF(2^8)$ to generate EC points and design an algorithm involving the x and y coordinates of the specified EC points. In the second technique, rather than selecting a particular Galois field $GF(2^8)$, we created a comprehensive algorithm for the construction of S-boxes by employing MEC over $GF(2^n)$ where $n \geq 9$.

3.1 Construction of S-box Using MEC over Galois Field GF $(\mathbf{2^8})$

1. Take PIP of degree 8

$$f(x) = x^8 + x^4 + x^3 + x^2 + 1 \tag{3}$$

over the binary field.

2. Choose MEC

$$E_b : y^2 = x^3 + b \tag{4}$$

where $b \in GF(2^8)/\{0\}$.

3. Generate an EC points by utilizing that MEC over the Galois field $GF\left(2^8\right)$.
4. Calculate how many primes there are between the beginning and current parameter b and take an inverse of the parameter b under the Galois field $GF\left(2^8\right)$.
5. Instead of choosing b, the inverse of b under Galois field $GF\left(2^8\right)$ and the sum of primes there are between the beginning value of b and the current value of parameter b, we replace them with the y-coordinates at that place.
6. Adjust the x-coordinates of EC points based on the resulting y-coordinates and parameter b, as shown in Fig. 1.
7. Take an inverse under the Galois field $GF\left(2^8\right)$ of that x-coordinates except zero using specified PIP and generate 8 × 8 S-boxes.

To build a different number of S-boxes, one can adjust the parameters of MEC or the PIP. As the number of PIPs over Galois field $GF\left(2^8\right)$ is 16. Through this technique, we can generate a different number of 16 × 255 S-boxes in which every S-box has nonlinearity between 110 to 112. The S-box having nonlinearity 111.25 is presented in Tab. 1. A diagram of the proposed algorithm is shown in Fig. 1.

Algorithm 1: Construction of S-box Using MEC over GF(2^8)

```
Input: Select PIP of degree 8 with $b \in GF\left(2^8\right) - \{0\}$ and $W \leftarrow [0:255]$
Output: S-box
$Z = \varnothing$
    for each $x \in W$ do
        for each $y \in W$ do
            if $y^2 - \left(x^3 + b\right) = 0$ then
                $Z = Z \cup \{x, y\}$
            end
        end
    end
$B \leftarrow x$ coordinates from set $Z$
$C \leftarrow y$ coordinates from set $Z$
Take the sum of primes $[1:b]$
Take the inverse of $b$ under $GF\left(2^8\right)$
Taking the corresponding element in C in the place of b and sum of primes $[1:b]$
$D \leftarrow$ Rearrange these values in $B$
$j \leftarrow 1:256$
if $D(j) \leftarrow 0$ then
        No change
else take inverse under $GF\left(2^8\right)$
end if
```

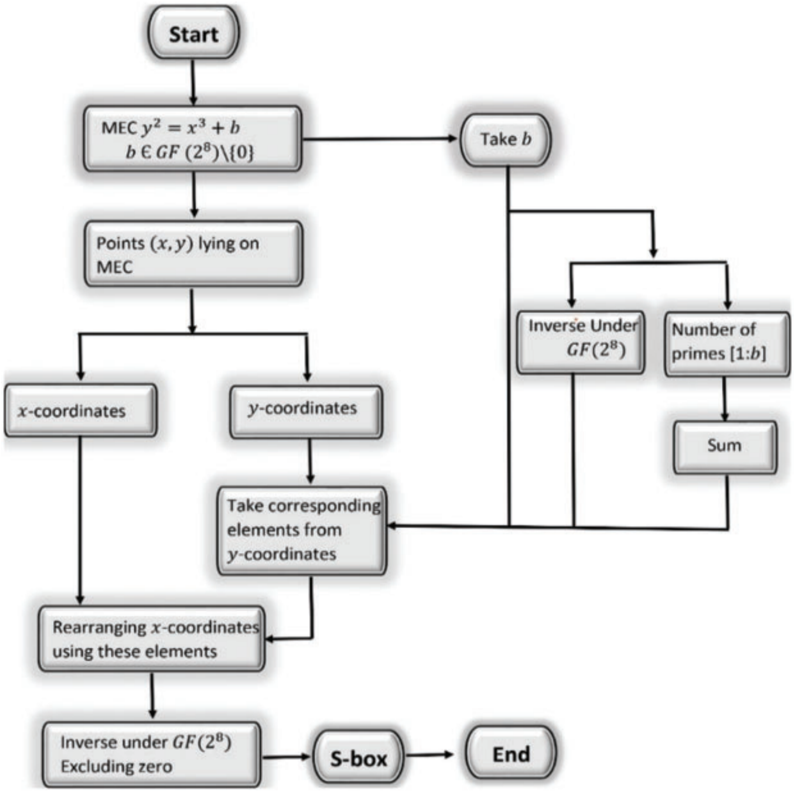
Start
MEC $y^2 = x^3 + b$
$b \in GF(2^8)\backslash\{0\}$
Take b
Points (x, y) lying on MEC
Inverse Under $GF(2^8)$
Number of primes [1:b]
x-coordinates
y-coordinates
Sum
Take corresponding elements from y-coordinates
Rearranging x-coordinates using these elements
Inverse under $GF(2^8)$ Excluding zero
S-box
End

Figure 1: Proposed algorithm using MEC over $GF\left(2^8\right)$

Table 1: Proposed S-box 1 by using MEC over $GF\left(2^8\right)$

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

3.2 Construction of S-box Using MEC over Galois Field GF (2^n)

The Galois fields $GF\ (2^n)$ where $n \geq 9$ is applied in this study to establish a more comprehensive and effective approach for the designing of a large number of distinct 8×8 S-boxes. A diagram of the proposed algorithm is shown in Fig. 2.

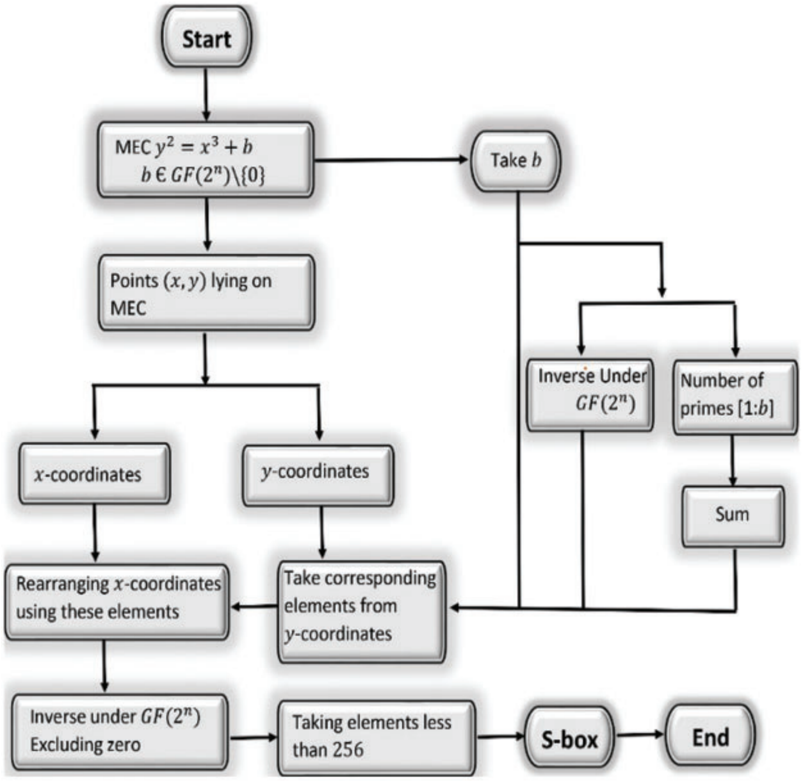
Start
MEC $y^2 = x^3 + b$
$b \in GF(2^n)\setminus\{0\}$
Take b
Points (x, y) lying on MEC
x-coordinates
y-coordinates
Inverse Under $GF(2^n)$
Number of primes [1:b]
Sum
Rearranging x-coordinates using these elements
Take corresponding elements from y-coordinates
Inverse under $GF(2^n)$ Excluding zero
Taking elements less than 256
S-box
End

Figure 2: Proposed algorithm using MEC over $GF(2^n)$

3.2.1 Construction of S-box Using MEC over Galois field GF $\left(2^9\right)$

1. Choose PIP of order degree 9

$$f\ (x) = x^9 + x^4 + 1 \tag{5}$$

Also, an independently one can take any other PIP of degree 9 over the binary field.

2. Consider MEC

$$E_b : y^2 = x^3 + b \tag{6}$$

where b be the element of Galois field $GF(2^9)$ excluding zero.

3. Utilize MEC over the Galois field $GF(2^9)$ and generate EC points.
4. Compute the inverse of the parameter b under the Galois field $GF(2^9)$, find the number of primes between the smallest possible value of parameter b and the value b used for specified MEC.

5. Calculate the position of b, its inverse under the Galois field $GF(2^9)$, the number obtained by summing the number of primes and taking the corresponding y-coordinates from EC points at that place.
6. Managing parameter b and the resultant y-coordinates, re-adjust the x-coordinates of corresponding EC points.
7. Taking the inverse of each x-coordinate except zero under the Galois field $GF(2^9)$ with corresponding PIP.
8. Finally, randomly take those elements less than 256 to construct an S-box.

The number of S-boxes can be varied by modifying the MEC parameter b or the PIP. The total number of PIPs over Galois field $GF(2^9)$ is calculated by $\frac{\varphi\left(2^9-1\right)}{9}$, where phi represents the Euler totient function. This technique allows one to construct a different number of 48 × 511 S-boxes. The S-box created using this technique is given in Tab. 2.

Table 2: Proposed S-box 2 by using MEC over $GF\left(2^9\right)$

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

3.2.2 Construction of S-box Using MEC over Galois Field $GF(2^{10})$

1. Choose PIP of order degree 10 over the binary field.

2. Consider MEC

$$E_b: y^2 = x^3 + b \tag{7}$$

where b be the element of Galois field $GF(2^{10})/\{0\}$.

3. Utilize MEC over the Galois field $GF(2^{10})$ and generate EC points.
4. Compute the inverse of the parameter b under the Galois field $GF(2^{10})$, find the number of primes between the smallest possible value of parameter b and the value b used for specified MEC.
5. Calculate the position of b, its inverse under the Galois field $GF(2^{10})$, the number obtained by summing the number of primes and taking the corresponding y-coordinates from EC points at that place.
6. Managing parameter b and the resultant y-coordinates, re-adjust the x-coordinates of corresponding EC points.
7. Taking the inverse of each x-coordinate except zero under the Galois field $GF(2^{10})$ with corresponding PIP.
8. Finally, randomly take those elements less than 256 to get an S-box.

The number of S-boxes can be varied by modifying the MEC parameter b or the PIP. The total number of PIPs over Galois field $GF(2^{10})$ is calculated by $\varphi\left(2^{10}-1\right)/10$, where phi represents the Euler totient function. This technique allows one to generate 62 × 1023 different S-boxes. The S-box created using this technique is given in Tab. 3.

Algorithm 2: Construction of S-box Using MEC over GF(2^n) .

```
**Input**: Select PIP of degree $n$ with $b \in GF\left(2^n\right) - \{0\}$ and $T \leftarrow [0: 2^n - 1]$
**Output**: S-box
$M = \varnothing$
    **for** each $x \in T$ **do**
        **for** each $y \in T$ **do**
            **if** $y^2 - \left(x^3 + b\right) = 0$ **then**
                $M = M \cup \{x, y\}$
            **end**
        **end**
    **end**
$B \leftarrow x$ coordinates from set $M$
$C \leftarrow y$ coordinates from set $M$
Take the sum of primes $[1: b]$
Take the inverse of $b$ under $GF\left(2^n\right)$
Taking the corresponding element in C in the place of $b$ and sum of primes $[1: b]$
$D \leftarrow$ Rearrange these values in $B$
$i \leftarrow 1: length(D)$
**if** $D\left(i\right) \leftarrow 0$ **then**
        No change
**else** take inverse under $GF(2^n)$
**end if**
Taking randomly all those elements less than 256
```

Table 3: Proposed S-box 3 by using MEC over $GF\left(2^{10}\right)$

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

4 Security Analysis

The cryptographic integrity of the proposed scheme is obtained using several conventional tests. This section will briefly review these security tests and the offered method's results compared to other methods.

4.1 Nonlinearity (NL)

An S-box must confuse the data to a certain amount to keep the data safe from an attacker. The NL security test is a measure that computes the ability of an S-box to confuse the data, as represented in the following

$$N^*\left(S\right) = \min_{\mu,\beta,\eta}\{\alpha \in GF(2^n) | \mu.S(\alpha) = \beta \cdot \alpha \otimes \eta\} \tag{8}$$

where $\mu \in GF(2^n)$, $\beta \in GF\left(2^n\right) \setminus \{0\}$, $\eta \in GF(2)$, and "·" denotes the dot product over $GF(2)$.

An S-box with considerable NL can inflict a lot of data confusion. The optimal value of an 8 × 8 S-box is 120, which is calculated as $2^{n-1} - 2^{\frac{n}{2}-1}$, [19]. In Tab. 4, the NL of newly designed S-boxes and some existent S-boxes are given comparatively. One can notice clearly that the newly formed S-boxes have more significant NL when compared to the EC-based S-boxes in [10,12].

Table 4: Comparison of NL of the proposed S-boxes with existing S-boxes

S-box	Scheme	Minimum value	Maximum value	Average value
Proposed 1	EC	110	112	111.25
Proposed 2	EC	100	110	105.75
Proposed 3	EC	104	108	105.25
Ref [20]	Chaos	100	110	105
Ref [21]	Group	98	110	105.5
Ref [10]	EC	–	–	104
Ref [22]	EC	–	–	106
Ref [12]	EC	–	–	106
Ref [23]	Chaos	98	106	103
Ref [24]	Chaos	104	110	106
Ref [25]	Pseudo-random	102	106	104
Ref [26]	Chaos	102	108	106
Ref [27]	Chaos	104	108	105.8

4.2 Strict Avalanche Criterion (SAC)

Webster and Tavares [28] were the first to introduce SAC in 1985. The SAC is built on the principles of avalanche and completion. The requirement of SAC is fulfilled when a single bit of information is updated; half of the matching output bits must change. The offered S-boxes meet the SAC criteria according to the calculated performance indexes. In Tab. 5, the proposed S-boxes SAC values are compared to the existing S-boxes, which shows that our S-boxes have an optimal SAC value.

4.3 Bit Independent Criterion (BIC)

The other vital test to study any cryptographic technique is BIC [29], which is operated to evaluate the independence of pair of output bits when the input bit is changed. Tab. 5 displays the outcomes of BIC analysis of the proposed S-boxes, and in the significance of encryption stability, the BIC of the proposed S-boxes is satisfactory. Performance Indexes of S-boxes given in Tab. 5 reveal that the rank of our proposed S-box is comparable with S-boxes from literature, and we marked that the offered S-boxes satisfied BIC close to the satisfactorily probable value.

Table 5: Comparison of proposed S-boxes SAC and BIC with Some existing Schemes

	SAC			BIC	
S-box	**Min**	**Max**	**Avg**	**Min**	**Avg**
Proposed 1	0.4219	0.5625	0.4878	110	111.43
Proposed 2	0.4063	0.5781	0.4998	88	102.714
Proposed 3	0.4219	0.5938	0.5049	98	103.643
Ref [10]	0.391	0.625	–		–
Ref [12]	0.406	0.641	–		98

(Continued)

Table 5: Continued

	SAC			BIC	
S-box	**Min**	**Max**	**Avg**	**Min**	**Avg**
Ref [20]	0.4063	0.6094	0.5010		104.3
Ref [24]	0.4219	0.5938	0.5039		102.3
Ref [26]	0.4219	0.5938	0.5002		105.4
Ref [30]	0.3671	0.5975	0.5058		104.2
Ref [31]	0.4982	0.5781	0.4218		103.1
Ref [32]	0.4219	0.5469	0.5115		108

4.4 Linear Approximation Probability (LP)

Linear approximation attacks on S-boxes can be approximated by determining the maximum number of coincidental input and output bit pairs. If an S-box has a lower LP, it is extremely resistant to linear attacks [29]. According to Tab. 6, the LP values of the new S-boxes are significantly lower than those of other S-boxes.

4.5 Differential Approximation Probability (DP)

A differential approximation probability is offered in [33] to find the probability impact of a particular disparity in the input bit on the variance of the resulting output bits. The DAP of an S-box S is shown below in the mathematical phrase: $g^*, h^* \in GF\left(2^8\right)$,

$$DP\left(S\right) = \max_{g^*.h^*}\{\#\left\{g \in GF\left(2^8\right) \middle| \, S\left(g + g^*\right) - S(g) = h^*\right\}\} \tag{9}$$

The S-box has more potential against differential attacks if it has a lower value of DP. The experimental outcomes of DP of the newly spawned S-boxes are presented in Tab. 6, which indicates that the newly designed S-boxes have high resistance against differential attacks.

Table 6: Comparison of proposed S-boxes LP and DP with preexisting S-boxes

S-box	LP	Max (LP)	DP
Proposed 1	0.0703125	146	0.0234375
Proposed 2	0.15625	168	0.046875
Proposed 3	0.148438	166	0.046875
Ref [10]	0.14500	–	0.03900
Ref [12]	0.132800	–	0.039100
Ref [29]	0.062	–	0.01560
Ref [30]	0.1484	–	0.0391
Ref [34]	0.06250	144	0.015625
Ref [35]	0.0159	164	0.028100
Ref [36]	0.1484	162	0.0468
Ref [37]	0.125	–	0.0391

4.6 NPCR and UACI Analysis

It's common for hackers to make minor adjustments to an image before using the recommended method. You can compare the original with the substituted image. Using this method, they discovered the relationship between the original and encrypted images. A one-pixel change in the original image considerably impacts the image following substitution. This section combines two key tests, the unified average change intensity (UACI) and the several pixels changing rate (NPCR), to determine the design's resistance to differential attacks. NPCR can be summed up as

$$NPCR = \frac{\sum_{g^*,h^*} F(g^*, h^*)}{M^* \times N^*} \times 100\% \tag{10}$$

And UACI is defined as

$$UACI = \frac{1}{M^* \times N^*} \left[\sum_{g^*,h^*} \frac{abs(F_1^*(g^*, h^*) - F_2^*(g^*, h^*))}{255} \right] \times 100\% \tag{11}$$

where M^* and N^* denotes the image height. Tab. 7 depicts the proposed scheme NPCR and UACI values, indicating that our system is more resistant to various attacks.

Table 7: Comparison of proposed S-boxes NPCR and UACI with existing schemes of S-boxes

Algorithms	NPCR	UACI
Proposed S-box 1	99.61	33.57
Proposed S-box 2	99.60	33.64
Proposed S-box 3	99.64	33.73
Ref [14]	99.64	33.68
Ref [38]	99.58	28.62
Ref [39]	98.47	32.21
Ref [40]	99.42	24.94
Ref [41]	99.54	28.27
Ref [42]	99.61	33.08
Ref [43]	99.59	33.45

4.7 Statistical Analysis

When evaluating statistical analyses, one uses the majority logic criteria (MLC) [44]. Also, an S-box is used to encrypt a test image by swapping pixel values in this standard. Even though this isn't an encryption technology, the actual and encrypted data are analyzed statistically using this criterion. Multiple statistical analyses, including as homogeneity, correlation, contrast, energy, and entropy, can be evaluated using the MLC as a standard. This evaluation determines whether the S-box can be used to encrypt an image or not. Lena's image of 256 × 256 is operated for the MLC study, and the outcomes of the presented scheme are given in Tab. 8. The MLC analysis showed that the diffusion level of the newly developed S-boxes is up to the mark. All of this can be seen in Fig. 3.

Table 8: Comparison of MLC Analyses of proposed S-boxes with other Schemes of S-boxes

S-boxes	Entropy	Contrast	Correlation	Energy	Homogeneity
Proposed 1	7.94	9.99240	0.0034	0.0156	0.3887
Proposed 2	7.94	9.6416	0.0130	0.0156	0.3886
Proposed 3	7.94	9.9893	0.0025	0.0156	0.3890
Ref [34]	7.24	7.4568	0.0785	0.0223	0.4731
Ref [42]	7.94	9.9764	0.0487	0.0161	0.4171
Ref [45]	7.96	8.5969	0.0019	0.0174	0.4070
Ref [46]	–	10.3986	0.0072	0.0158	0.4214
Ref [47]	7.75	9 .8198	0.0573	0.0163	0.4228

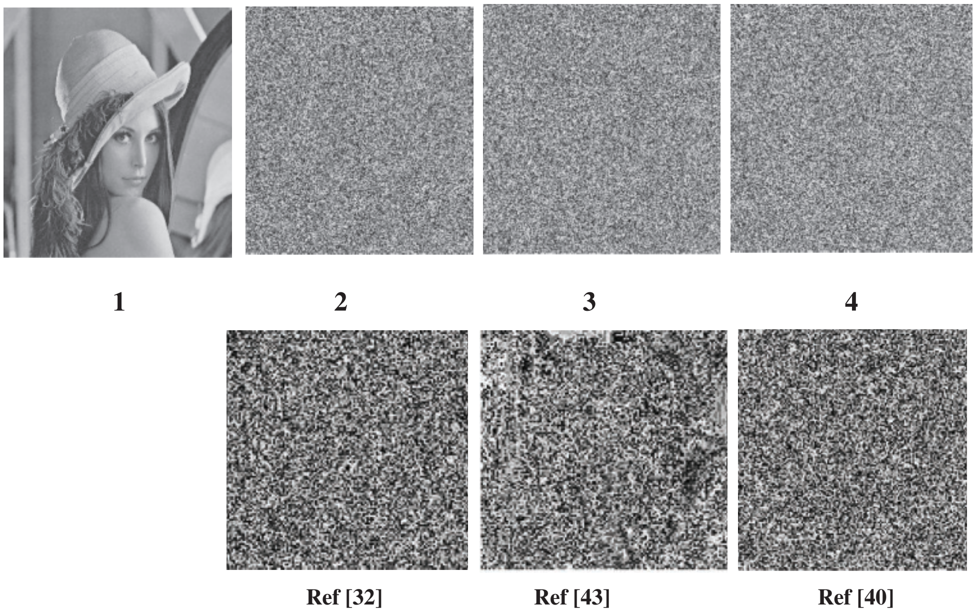

Figure 3: (1) Original Lena Image (2,3,4) Encrypted Lena image using S-box 1, S-box 2, and S-box 3

4.8 Comparative Analysis

Various cryptographic tests assess the proposed algorithm to examine its potential against different cryptographic attacks. The comparison of the proposed technique with other algorithms is discussed briefly in the following point-by-point discussion.

1. In Tab. 4, different algorithms are listed based on Chaos, group, Galois field, and EC. By using MEC over a 256-order Galois field, one can see that we generate 4080 S-boxes having nonlinearity between 110 to 112.The algorithms in [10,12,22] were constructed using EC over the prime field but did not achieve outstanding results compared to our proposed technique.

2. The proposed S-boxes BIC and SAC values are more satisfactory than the algorithms in [10,12,30–32] mentioned in Tab. 5. Furthermore, our BIC and SAC values are optimal, indicating that the offered S-boxes can cause enough diffusion in the data.
3. The proposed S-boxes LP values are also acceptable compared to the different algorithms in Tab. 6. Similarly, the lower value of the DP of the proposed scheme shows that our method is more invulnerable to various attacks.
4. The NPCR and UACI values of the proposed S-boxes are comparatively better than the cited algorithms in Tab. 7. Furthermore, the MLC analysis in Tab. 8 shows that the offered algorithm is more significant for image encryption.
5. The number of S-boxes creation ability of the proposed algorithm is very high compared to other EC-based algorithms noted in Tab. 9, proclaiming that the presented scheme is novel and more significant.

Table 9: The comparison of possible S-boxes constructed using MEC over the $GF(2^n)$ and MEC over the prime field P

MEC over $\boldsymbol{GF(2^n)}$		MEC over prime field $\boldsymbol{P}$	
N	S-boxes	P	S-boxes
8	4080	257	256
9	24528	521	520
10	63426	1031	1030
11	364366	2053	2052
12	638820	4099	4098

Note: $p = 2^n + l$, where l is the least integer which gives a prime number p greater than 2^n.

The above analysis shows that the proposed scheme has good resistance against various cryptographic attacks compared to existing algorithms. The results of the MLC tests reveal that the proposed algorithm has good image encryption features.

5 Conclusion

In this article, we considered MEC over the binary extension field $GF(2^n)$, where $n \geq 8$ and developed a comprehensive algorithm for the construction of S-boxes. Generally, EC-based algorithms are considered over prime fields where the possibilities of generating distinct S-boxes are not as great as the binary extension field. The outputs of different tests imply that the proposed algorithm is also resilient to various cryptographic attacks. Also, the presented S-boxes are assessed by a substitution process to study the importance of the proposed algorithm in image encryption applications. In the future, the various types of ECs over the binary extension field can also be utilized to construct different cryptographic algorithms.

Funding Statement: The authors extend their gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through the research groups program under grant number R. G. P. 2/109/43.

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

References

[1] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[2] X. R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.

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

[4] L. Cui and Y. Cao, "A new S-box structure named affine-power-affine," *International Journal of Innovative Computing, Information and Control*, vol. 3, no. 3, pp. 751–759, 2007.

[5] I. Hussain, T. Shah and H. Mahmood, "A new algorithm to construct secure keys for AES," *International Journal of Contemporary Mathematical Sciences*, vol. 5, no. 26, pp. 1263–1270, 2010.

[6] M. T. Tran, D. K. Bui and A. D. Duong, "Gray S-box for advanced encryption standard," *Int. Conf. on Computational Intelligence and Security, IEEE*, vol. 1, pp. 253–258, 2008.

[7] F. Özkaynak and A. B. Özer, "A method for designing strong S-Boxes based on chaotic Lorenz system," *Physics Letters A*, vol. 374, no. 36, pp. 3733–3738, 2010.

[8] Y. Wang, K. W. Wong, C. Li and Y. Li, "A novel method to design S-box based on chaotic map and genetic algorithm," *Physics Letters A*, vol. 376, no. 6, pp. 827–833, 2012.

[9] J. H. Cheon, S. Chee and C. Park, "S-boxes with controllable nonlinearity," in *Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg, Springer, pp. 286–294, 1999.

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

[11] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, no. 2–3, pp. 391–402, 2019.

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

[13] S. Farwa, A. Sohail and N. Muhammad, "A novel application of elliptic curves in the dynamical components of block ciphers," *Wireless Personal Communications*, vol. 115, no. 2, pp. 1309–1316, 2020.

[14] H. U. Rehman, T. Shah, A. Aljaedi, M. M. Hazzazi and A. R. Alharbi, "Design of nonlinear components over a mordell elliptic curve on galois fields," *Computers, Materials & Continua*, vol. 71, no. 1, pp. 1313–1329, 2022.

[15] E. W. Weisstein, "Totient function," 2003. [Online]. Available: https://Mathworld.Wolfram.Com/.

[16] S. Maitra, K. C. Gupta and A. Venkateswarlu, "Results on multiples of primitive polynomials and their products over GF (2)," *Theoretical Computer Science*, vol. 341, no. 1–3, pp. 311–343, 2005.

[17] L. C. Washington, "Elliptic curves," in *Number Theory and Cryptography*, CRC press, 2008.

[18] C. J. Benvenuto, "Galois field in cryptography," *University of Washington*, vol. 1, no. 1, pp. 1–11, 2012.

[19] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Workshop on the Theory and Application of Cryptographic Techniques*, Berlin, Heidelberg, Springer, pp. 549–562, 1989.

[20] A. Belazi and A. A. Abd El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Optik*, vol. 130, no. August 3, pp. 1438–1444, 2017.

[21] M. Khan and T. Shah, "An efficient construction of substitution box with fractional chaotic system," *Signal, Image and Video Processing*, vol. 9, no. 6, pp. 1335–1338, 2015.

[22] N. A. Azam, U. Hayat and I. Ullah, "An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization," *Security and Communication Networks*, vol. 18, no. 2, pp. 9, 2018.

[23] M. A. Gondal, A. Raheem and I. Hussain, “A scheme for obtaining secure S-boxes based on chaotic Baker’s map,” *3D Research*, vol. 5, no. 3, pp. 17, 2014.

[24] U. Cavusoglu, A. Zengin, I. Pehlivan and S. Kacar, “A novel approach for strong S-box generation algorithm design based on chaotic scaled Zhongtang system,” *Nonlinear Dynamics*, vol. 87, no. 2, pp. 1081–1094, 2017.

[25] K. Kazlauskas, G. Vaicekauskas and R. Smaliukas, “An algorithm for key-dependent S-box generation in block cipher system,” *Informatica*, vol. 26, no. 1, pp. 5165, 2015.

[26] F. U. Islam and G. Liu, “Designing S-box based on 4D-4wing hyperchaotic system,” *3D Research*, vol. 8, no. 1, pp. 9, 2017.

[27] G. Liu, W. Yang, W. Liu and Y. Dai, “Designing S-boxes based on 3-D four-wing autonomous chaotic system,” *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1867–1877, 2015.

[28] 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, Springer, pp. 523–534, 1985.

[29] C. Adams and S. Tavares, “The structured design of cryptographically good S-boxes,” *Journal of Cryptology*, vol. 3, no. 1, pp. 27–41, 1990.

[30] G. Jakimoski and L. Kocarev, “Chaos and cryptography: Block encryption ciphers based on chaotic maps,” *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 2, pp. 163–169, 2001.

[31] 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. 4, no. 11, pp. 659–664, 2016.

[32] A. Belazi, A. A. Abd El-Latif, A. V. Diaconu, R. Rhouma and S. Belghith, “Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms,” *Optics and Lasers in Engineering*, vol. 88, no. 11–12, pp. pp 37–50, 2017.

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

[34] S. Farwa, T. Shah and L. Idrees, “A highly nonlinear S-box based on a fractional linear transformation,” *Springer Plus*, vol. 5, no. 1, pp. 1–12, 2016.

[35] F. Özkaynak, “Construction of robust substitution boxes based on chaotic systems,” *Neural Computing and Applications*, vol. 31, no. 8, pp. 3317–3326, 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, 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.

[38] K. Loukhaoukha, J. Y. Chouinard and A. Berdai, “A secure image encryption algorithm based on Rubik’s cube principle,” *Journal of Electrical and Computer Engineering*, vol. 12, no. 7, pp. 7–13, 2012.

[39] G. A. Sathishkumar and D. N. Sriraam, “Image encryption based on diffusion and multiple chaotic maps,” 2011. [Online]. Available: https://arxiv.org/abs/1103.3792.

[40] C. K. Huang and H. H. Nien, “Multi chaotic systems-based pixel shuffle for image encryption,” *Optics Communications*, vol. 282, no. 11, pp. 2123–2127, 2009.

[41] C. K. Huang, C. W. Liao, S. L. Hsu and Y. C. Jeng, “Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system,” *Telecommunication Systems*, vol. 52, no. 2, pp. 563–571, 2013.

[42] 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.

[43] X. Wang, X. Zhu and Y. Zhang, “An image encryption algorithm based on Josephus traversing and mixed chaotic map,” *IEEE Access*, vol. 6, no. 17, pp. 23733–23746, 2018.

[44] A. K. Farhan, N. M. Al-Saidi, A. T. Maolood, F. Nazarimehr and I. Hussain, "Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder," *Entropy*, vol. 21, no. 10, pp. 958, 2019.

[45] Y. Naseer, T. Shah, S. Hussain and A. Ali, "Steps towards redesigning cryptosystems by a non-associative algebra of IP-loops," *Wireless Personal Communications*, vol. 108, no. 3, pp. 1379–1392, 2019.

[46] F. Ali Khan, J. Ahmed, J. S. Khan, and J. Ahmad "A new technique for designing 8 × 8 substitution box for image encryption applications," in *2017 9th Computer Science and Electronic Engineering (CEEC)*, IEEE, pp. 7–12, 2017.

[47] Y. Naseer, T. Shah, D. Shah and S. Hussain, "A novel algorithm of constructing highly nonlinear Sp-boxes," *Cryptography*, vol. 3, no. 1, pp. 6, 2019.