New Technique for Designing Highly Nonlinear Confusion Component Based on Elliptic Curve and Group Action

Sadiqa Arshad

Abstract— The security of any block cipher heavily depends on the nonlinear component. Static substitution boxes (S-boxes) can be analyzed by attackers and in turn weaken the entire cryptosystem. Dynamic substitution box (S-box) can mitigate this problem and can resist unknown attacks. The underlying structure of dynamic S-boxes should also be strong enough to resist against algebraic attacks. In this paper we have constructed dynamic S-boxes based on elliptic curve points and group action followed by permutation applied on each of newly constructed S-boxes. The smaller key size and strong underlying structure of elliptic curves make it favorable to be used in many cryptosystems. The suggested scheme can generate many S-boxes with reasonable nonlinearity. Simple permutation can enhance nonlinearity of the all these selected S-boxes which can further be used as dynamic S-boxes for any cryptosystems. The cryptographic strength of these S-boxes is analyzed, and computational results shows that the suggested algorithm generates cryptographic strong S-boxes as compared to some existing schemes.

Index Terms— Elliptic curves, Group Action, Permutation, Nonlinear component, Substitution box, Nonlinearity, Bit Independence Criteria

1. Introduction

Data exchange through internet give rise the question of its security. During transmission data can be forged, manipulated, or lost. Over the years different measures are taken to provide security to both network and data. Many tools and applications are available for network security whereas data security requires protection against unauthorize access, manipulation, or theft. Tools used for data security must apply encryption and data masking techniques. Cryptography is used to transform data from human readable format to unreadable format. Different techniques are used to process data such as block ciphers and stream ciphers. In 1945 Claude Shannon gave the idea of combining confusion and diffusion in any encryption algorithm. Modern block ciphers such as DES, AES and Present, all follow Shannon's principle. Diffusion is hiding the relationship between plain text and cipher text and achieved through permutation whereas confusion creates complexity between key and the cipher text. The substitution boxes are the nonlinear component of any block cipher. The input bits to substitution boxes are transformed through nonlinear mathematical equation and produces an output bit. The strength of any block cipher resides in the strength of its substitution boxes. Substitution boxes can vary in size, from Serpent 4-bits to AES 8-bits S-boxes. Large S-boxes are considered more secure as compared to small S-box, but it is generally a tradeoff between security and memory consumption. S-boxes can also be categorized by their structure, data encryption standard (DES) S-boxes are lookup tables with no known mathematical structure is found while other may have algebraic structures. S-boxes with known algebraic structure are more vulnerable to cryptanalysis as compared to S-boxes with no mathematical structure. Block ciphers that are designed before differential cryptanalysis was known publicly, construct S-boxes with random sources but the discovery of differential cryptanalysis changed the overall structure of block ciphers. DES S-boxes are resistant to differential cryptanalysis, and it is assumed that the designer knew about it. The first block cipher DES adopted as standard in 1977 and enjoyed worldwide acceptance for almost thirty years. Due to advancement in technology, it was replaced by advance encryption standard (AES) in 2001. DES used eight S-boxes and its successor AES uses single S-box of dimension 16×16. The static S-box of AES creates confusion through the multiplicative inverse and affine transformation in $GF(2^8)$. Although the software implementation of AES is efficient, but the static behavior of its S-box might be vulnerable to side channel attacks [9]. Two types of S-boxes are used in block encryption, static and dynamic. Static S-box refers that a single S-box is used in each round and in dynamic S-box different S-boxes are used in each round. The statistical properties of static S-box can be studied by hackers and weakness can be used for cryptanalysis. On the other hand, in case of dynamic S-box, it is impossible for the attacker to know which S-box is used in each round and thus enhance the security of the block cipher. According to Bruce Schinier dynamic S-box also prevent from unknown attacks. Blowfish and Twofish are the block ciphers using dynamic S-boxes. Khan et. al, [[23] offer dynamic S-box based on group action and Gray codes on the original AES S-box. The suggested

• *Sadiqa Arshad is currently pursuing PhD degree program in Cryptography in Institute of Space Technology Islamabad,, Pakistan. E-mail: ilyas.sadiqa@gmail.com*

scheme creates up to 256 new S-boxes. Azam et. al,[26] offers dynamic S-boxes based on affine mapping and orbit of the power function. The resulting all S-boxes have nonlinearity equivalent to AES S-box. Thus, several techniques were adopted for the generation of dynamic s-boxes such as algebraic structures [37], chaotic maps [3-6,28-37] and differential equations. Elliptic curves, introduced by Miller and Koblitz independently in 1984 are used in cryptography for key exchange algorithms and random number generation but its sensitivity to initial parameters draws the attention of researchers to use for S-box generation. Hayyat et. al,[5] used two ordered elliptic curves defined over finite ring to create randomness in the points and then generate dynamic S-box. In [21] offered an image encryption scheme using isomorphic elliptic curves generated through a prime field. In this research elliptic curve points are used to scrambled image pixels and later different S-boxes are generated through isomorphic curves. Azam et. al,[5] used Mordell Elliptic curves of special order to generate an S-box using y-component of the points of the curve.

The aim of this paper is to construct dynamic S-boxes which possess an underlying strong mathematical structure and resistant to all known attacks. The contribution of this paper is

- Group action is applied on points of elliptic curves to construct an initial S-box with maximum possible nonlinearity.
- We search for suitable permutation applied on initial S-box to achieve the standard nonlinearity set by AES.
- A series of test are applied such as Nonlinearity, Bit Independence criterion (BIC), Strict Avalanche Criterion (SAC) to examine the cryptographic properties of the suggested S-boxes.

This paper is organized in five sections. Section 2 explains the preliminaries of the mathematical structure of Elliptic curves (ECC). The Elliptic curve used for this paper is discussed in section 3. The suggested algorithm is explained in section 4. Strength of the S-box is examined in the statistical analysis section 5. The last section concludes the paper.

2. Preliminaries

Elliptic curves have been studied by mathematician since long and has applications in various field of cryptography such as public key cryptography, digital signatures pseudo-random number generators and many more. Elliptic curves are defined as smooth, projective, algebraic curves of genus 1. The general form over a finite field F_p is defined as

$$y^2 + e_1xy + e_3y = x^3 + e_2x^2 + e_4x + e_6\,, \quad e_i \in F_p \qquad (1)$$

For characteristic of the curve not equal to 2 or 3, equation (1) reduces to the form

$$y^2 = x^3 + a_1x + a_2 \,(\text{mod}\, p) \qquad (2)$$

Such that $4a_1^3 + 27a_2^2 \,(\text{mod}\, p) \neq 0$. We call a_1, a_2 and p , the elliptic curve $E_{a_1,a_2,p}$ parameters. Different elliptic curves can be defined by changing the values of a_1 and a_2 . In short, the set of points that satisfy equation (1) or (2) is

$$E_{a_1,a_2,p} = \{(\text{x},\text{y}) \in \text{F}_p \,|\, y^2 = x^3 + a_1x + a_2 \,(\text{mod}\, p)\} \, U \{\text{O}\} \qquad (3)$$

Where O acts as a point at infinity. Total number of points can be approximated by Hesse's theorem

$$\#E_{a_1,a_2,p} = |\, E_{a_1,a_2,p} - p - 1 \,| \leq 2\sqrt{p} \qquad (4)$$

2.1 Elliptic Curve Point operations

Given two points $u(x_1, y_1)$ and $\text{v}(x_2, y_2)$ of $E_{a_1,a_2,p}$ the addition results in third point $\text{z}(x_3, y_3)$ that satisfies the curve equation. Addition is performed through the following mathematical equations

$$\begin{aligned}
&\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad u(x_1, y_1) \neq v(x_2, y_2), \\
&x_3 = \lambda - x_1 - x_3 \,(\text{mod}\, p)\,, \quad y_3 = \lambda(x_1 - x_3) - y_2 \,(\text{mod}\, p), \\
&\lambda = \frac{3x_1^2 + e_1}{2y_1}, \qquad u(x_1, y_1) = v(x_2, y_2), \\
&x_3 = \lambda - 2x_1 \,(\text{mod}\, p)\,, \quad y_3 = \lambda(x_1 - x_3) - y_2 \,(\text{mod}\, p).
\end{aligned} \qquad (5)$$

In order to find negative of any point $u(x_1, y_1)$ on the curve, one has to calculate $-u = u(x_1, \text{p} - y_1)$. The elliptic curve discrete log problem is given two points u , v on the curve find a positive integer k such that $u = kv$.

3. The Suggested Substitution box construction

The crux of any block cipher is its substitution box that is responsible to hide the relationship between key and the output. In literature several techniques can be found on construction of S-box using elliptic curves. In this novel technique a curve $E_{2442,5,5011}$ of prime order is selected and through group action a list of S-boxes is generated. We select S-boxes with maximum nonlinearity among the group. We found suitable permutations for each of these initial S-boxes to achieve the standard nonlinearity achieved by AES S-box.

Step 1

Select an elliptic curve $E_{a_1,a_2,p}$ of prime order. The lower bound of the prime is $p \geq 257$ to ensure that we have minimum 256 points. From equation (4) the total number of points are $\#(E_{a_1,a_2,p})$. We define the index set of order $\#(E_{a_1,a_2,p})$ as Z_n and define an action as $\rho : Z_n \times E_{a_1,a_2,p} \rightarrow E_{a_1,a_2,p}$ defined as for fixed $G(x,y) \in E_{a_1,a_2,p}$, $\rho(x_i, G(x,y)) = x_i.G(x,y)$ and $\forall x_i \in Z_n, i = 1,2,3...n-1$. This action is applied on all the generators and a series of 8×8 S-boxes are generated with unique entries from $\{0,1,2,3...255\}$. The group action randomize the curve points. We define a mapping for each output of the group action as $ES_i : E_{a_1,a_2,p}(x_i, y_i) \rightarrow Z_p$ such that $ES_i(E_{a_1,a_2,p}(x_i, y_i)) = (x_i y_i) \bmod p$. We select only those S-boxes with sufficient cryptographic properties and named as initial S-box $ES_{G(x_i,y_i)}$ where $G(x_i, y_i)$ is the generator. Table.1 shows the total number of S-boxes generated with sufficient nonlinearity. We have found 23 S-boxes with nonlinearity 106 and four S-boxes with nonlinearity greater than 106. Table [2-4] shows the elements of the initial S-boxes ES_i having maximum nonlinearity.

Table1: Number of S-boxes generated with $G_i(x,y), i \in \{1,2,3,...\}$ of $E_{2442,5,5011}$

S-box	NL	S-box	NL
$ES_{G(68, 3545)}$	106	$ES_{G(1968, 4526)}$,	106
$ES_{G(94, 1676)}$	106	$ES_{G(2693, 2118)}$,	106
$ES_{G(241, 834)}$	106	$ES_{G(2731,301)}$,	106
$ES_{G(2358,3081)}$	106	$ES_{G(2865,4221)}$,	106
$ES_{G(2722,2647)}$	106	$ES_{G(3628,4956)}$,	106
$ES_{G(2764,698)}$	106	$ES_{G(3987,3389)}$,	106
$ES_{G(2909,3044)}$	106	$ES_{G(4064,2456)}$	106
$ES_{G(3693,1016)}$	106	$ES_{G(4508,4623)}$	106
$ES_{G(4027,2263)}$	106	$ES_{G(4742,357)}$,	106
$ES_{G(4483,352)}$	106	$ES_{G(4229,643)}$	106.75
$ES_{G(4710,3651)}$	106	$ES_{G(4284,3322)}$	106.5
$ES_{G(4985,1260)}$,	106	$ES_{G(4523,2304)}$	106.5
$ES_{G(1075, 2560)}$,	106	$ES_{G(4917,2004)}$	107.25
$ES_{G(1277, 2814)}$,	106		

Step 2

In this step we try to find permutation from symmetric group S_{256} for each of the four S-boxes found in step 1 having maximum nonlinearity. Total number of such permutations are $|S_{256}| = 256!$. After thorough search we found 4 different permutations which when applied to initial S-boxes ES_i generated from step 1 to enhance nonlinearity. Table [6-9] in appendix shows these permutations denoted as $\sigma_j, j \in \{1,2,3,4\}$. The final S-boxes $S_1 = \sigma_1(ES_1)$, $S_2 = \sigma_2(ES_2)$, $S_3 = \sigma_3(ES_3)$, $S_4 = \sigma_4(ES_4)$ are shown in Table [10-13].

Table 2: Initial S-box 1 generated from $ES_{G(4229,643)}$

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

Table 3: Initial S-box 2 generated from $ES_{G(4284,3322)}$

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

--

Table 4: Initial S-box 3 generated from $ES_{G(4523,2304)}$

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

--

Table 5: Initial S-box 4 generated from $ES_{G(4917,2004)}$

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

4. CRYPTOGRAPHIC PROPERTIES OF ROBUST NONLINEAR CONFUSION COMPONENT

The cryptographic properties of our proposed S-boxes are analyzed and evaluated through some standard criteria. The security performance of the suggested and already existing S-boxes is also compared in this section. NIST recommended tests such as nonlinearity, strict avalanche criteria (SAC), bits independence criteria (BIC), linear approximation probability and differential approximation are performed in this section.

Table. 10: Sbox1 generated after the permutation

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

4.1 Nonlinearity

It is the most essential and fundamental tool to measure the strength of S-box. It ensures that the output vector cannot be written as a linear combination of its input vectors. The nonlinearity of any Boolean function is the measure of minimum hamming distance from all affine functions. Mathematically we can compute nonlinearity shown in equation (5) using Walsh spectrum.

$$N_f = 2^{n-1} - \frac{1}{2}\max|\text{Walsh spectrum}| \tag{6}$$

The following equation is used to determine the Walsh spectrum.

$$S_f = \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus w.x} \tag{7}$$

The upper bound of any 8×8 S-box can be computed as $N_f = 2^{n-1} - 2^{\frac{n}{2}-1} = 120$. Higher nonlinearity indicates the resistance of the S-box against linear attacks. The nonlinearity of AES S-box is 112 and considered the bench mark up till now. The nonlinearity of initial S-boxes $S_{G(x,y)}$ are given in Table 14. All these S-boxes have nonlinearity greater or equal to 106 which is clear indication that the nonlinear component can create confusion in the cipher text. However, the output of step B produces much better S-box with nonlinearity equal or closer to 112. Table 15 shows the nonlinearity comparison of the suggested algorithm with standard S-boxes and one can easily conclude that the suggested S-boxes possess good nonlinearity and can safely be used for cryptographic purposes.

Table. 14: Nonlinearity of S-boxes generated from generator of elliptic curve $S_{G(x,y)}$

S-box	$S_{G(4229,643)}$	$S_{G(4284,3322)}$	$S_{G(4917,2004)}$	$S_{G(4523,2304)}$	Ref. [5]	Ref. [22]	Ref. [23]	Ref. [6]
Nonlinearity	106.75	106.5	107.25	106.5	106	107	106.25	106

Table.15: Nonlinearities of newly constructed S-boxes

S-box	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Average
S-box 1	112	112	112	112	112	112	112	112	112
S-box 2	112	112	112	112	112	112	112	112	112
S-box 3	112	112	112	112	112	112	112	112	111.5
S-box 4	112	112	112	112	112	112	112	112	112
AES	112	112	112	112	112	112	112	112	112
APA [11]	112	112	112	112	112	112	112	112	112
SkipJack [22]	104	104	108	108	108	104	104	106	105.75
S_8 Liu [8]	105	105	104	100	107	105	106	107	104.875
Hussain [17]	104	100	108	106	102	106	104	108	104.75
Residue Prime [18]	94	100	104	104	102	100	98	94	99.5

4.2 Bit Independence Criteria

Bit independence criteria is used to check the randomness of the cipher text if a plain text has changed slightly. This important property to analyze an S-box is presented by Adam and Tavares [1]. It is used to measure the independence of output bits j and k of an n bits Boolean function if a single input bit i has changed. It is discussed in [1] that if the two output bits Boolean functions f_j, f_k then $f_j \oplus f_k = f$ must be highly nonlinear and satisfy SAC. BIC takes values in [0 1] and ideally it is equal to 0 and in worst case equal to 1. The average BIC results with nonlinearity and SAC are discussed in Table 16.

Table.11: S-box 2 generated after the permutation

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

Table. 12: S-box 3 generated after the permutation

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

Table. 16: The outcomes of BIC for SAC for S-box 4

0	0.502	0.4824	0.4902	0.4941	0.502	0.502	0.5039
0.502	0	0.5039	0.5059	0.5195	0.5156	0.4805	0.5254
0.4824	0.5039	0	0.4883	0.502	0.5117	0.4902	0.502
0.4902	0.5059	0.4883	0	0.5312		0.4863	0.5039
0.4941	0.5195	0.502	0.5312	0	0.5117	0.4941	0.5059
0.5137	0.5156	0.5117	0.5195	0.5117	0	0.498	0.4941
0.502	0.4805	0.4902	0.4863		0.498	0	0.4883
0.5039	0.5254	0.502	0.5039	0.5059	0.4941	0.4883	0

Table.17: The outcomes of BIC for NL for S-box 4

0	112	112	112	112	112	112	112
112	0	112	112	112	112	112	112
112	112	0	112	112	112	112	112
112	112	112	0	112	112	112	112
112	112	112	112	0	112	112	112
112	112	112	112	112	0	112	112
112	112	112	112	112	112	0	112
112	112	112	112	112	112	112	0

4.3 Strict Avalanche Criteria (SAC)

Strict avalanche criteria was first introduced by Adams and Travers. It refers to the characteristics of Boolean functions of an S-box. If the inversion of a single input bit cause half of the output bits to be changed then the given Boolean function is said to satisfy SAC. Mathematically Boolean function $g: Z_2^n \rightarrow Z_2^m$ exhibits avalanche effect if:

$$\sum_{x \in GF(2^8)} ht(g(x \oplus a_i^n) \oplus g(x) = m2^{n-1} \qquad (8)$$

where ht is the hamming weight and $a_i (1 \leq i \leq 8)$. An S-box is considered strong if it satisfies higher order SAC. Table shows the SAC result of the Sbox4. Since all the entries in the table are closer to 0.5 which shows that the newly constructed S-box is resistance against attacks.

Table.13: S-box 4 generated after the permutation

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

4.4 Linear approximation probability

Linear cryptanalysis is a power full cryptanalysis technique introduced by Matsui in [Crypto 90] against DES but since this type of attack can be launched against any block cipher therefore the substitution box should be designed to resist against linear approximation attack. This test approximates the coincident of input bits to the output bits. The mathematical expression is

$$LAP = \frac{1}{2^8}\left\{\max|\alpha.x = \beta.S(x)| - 2^7\right\}, \quad x \in GF(2^8). \tag{9}$$

Table listed the values for linear approximation, since all the values are closer to zero which shows the strength of the substitution box against linear attack.

Table.18: Strict Avalanche Criteria for S-box 4

0.5312	0.5312	0.5156	0.5156	0.5	0.5312	0.5469	0.5156
0.5469	0.5312	0.4531	0.4688	0.4531	0.5	0.5156	0.4688
0.5	0.5156	0.5	0.5312	0.5156	0.4844	0.5312	0.5156
0.5156	0.4688	0.5	0.5312	0.5625	0.5	0.5312	0.4375
0.5	0.5469	0.4531	0.5156	0.4844	0.4531	0.4531	0.5625
0.4531	0.4531	0.5469	0.4688	0.5156	0.4688	0.5156	0.4531
0.4531	0.5156	0.5469	0.4688	0.4531	0.5625	0.4531	0.5469
0.5	0.4688	0.5156	0.5312	0.4531	0.4844	0.5156	0.5156

4.5 Differential Approximation

Differential cryptanalysis was publicly introduced by Ali Biham and Shamir [1]. It is a chosen-plain text attack in which a plain text with fixed differences is chosen and the corresponding output differences are measured. These input and output differences are called differentials. The attacker analyzes these differences and try to establish some statistical pattern and eventually guess the key. It is a very strong attack against any block cipher and if launched successfully, can recover key in time less than brute force attack. Thus, to analyze a substitution box against differential attack a difference distribution table is analyzed and checked how frequent an output difference occurs. Mathematically if Δx and Δy represents the input and output difference then how often the equation $\Delta y = S(x \oplus \Delta x) \oplus S(x)$ holds. Difference distribution table depicts the maximum probability of Δy and can be measured through the equation

$$DDT = \frac{1}{2^8}\left\{\max[|\,S(x \oplus \Delta x) \oplus S(x) = \Delta y\,]\right\} \tag{10}$$

The entries of DDT table are closer to zero ensures that the S-box is highly resistant against differential attacks.

5. Conclusion

Substitution boxes holds the central and sensitive position in block ciphers. The strength of a block cipher is measured through strength of its S-boxes. Algebraic structures-based S-boxes are designed in this paper using elliptic curves and permutation. Unlike chaotic sequences, elliptic curve points are less random and thus cannot used to create S-boxes directly. We tried to create randomness through concatenation and then achieve standard nonlinearity through permutation. Since large elliptic curves may have thousands of points which can be utilized to generate dynamic S-boxes for the block cipher. The method used in this approach uses only reduction modulo and can easily be implemented. We applied different statistical tests to check the strength of newly constructed S-boxes and the results shows that the suggested algorithm can generate cryptographically strong S-boxes.

Table. 19: Comparison of cryptographic properties of different S-boxes

S-boxes	Nf_{min}	Nf_{max}	Nf_{avg}	SAC	BIC-NL	DP	LAP
Suggested	112	112	112	0.4993	113.7875		0.0625
Ref. [2]	108	112	111.5	0.5037	103.9	0.0391	0.123
Ref. [12]	96	106	102.5	0.5058	112	0.01563	0.06525
Ref. [3]	106	108	107.5	0.4943	104.36	0.039	0.125
Ref. [4]	110	112	110.25	0.5	105.2	0.0391	0.125
Ref. [29]	100	110	106.75	0.5002	104	0.1172	0.125
Ref. [30]	104	110	106.25	0.5032	103.9	0.0391	0.1328
Ref. [35]	104	110	107	0.5101	106.25	0.0391	0.1484
Ref. [31]	106	108	106.5	0.5009	104.07	0.0391	0.1328
Ref. [15]	106	110	108	0.4988	102.86	0.04687	0.1406
Ref. [38]	110	112	110.25	0.4953	104.07	0.0391	0.125
Ref. [32]	100	108	105	0.5002	103	0.04687	0.125
Ref. [39]	106	110	107.75	0.4976	105.07	0.0391	0.125
Ref. [16]	104	108	106.25	0.5009	103.63	0.0391	0.1328
Ref. [14]	104	110	106	0.4978	103.92	0.04687	0.1563
Ref. [36]	104	108	106.75	0.5031	103.64	0.04687	0.1484
Ref. [34]	100	108	104.7	0.4982	103.1	0.0391	0.1406
Ref. [27]	98	110	105	0.4937	105.7	0.125	0.1172
Ref. [40]	108	110	108.75	0.4946	102.78	0.0391	0.1328
Ref. [19]	100	108	105	0.5007	104.14	0.0391	0.1328
Ref. [41]	102	108	105	0.5029	102.9	0.04687	0.14844
Ref. [33]	112	112	112	0.4956	112	0.01563	0.0625
Ref. [7]	96	106	102.5	0.5178	102.5	0.21094	-
Ref. [28]	102	112	110	0.5066	109	0.03125	0.1093
Ref. [8]	98	106	103.5	0.4958	103.5	0.05469	0.1328
Ref. [9]	96	104	100.5	0.4973	102.78	0.0391	0.15625

Appendix

Table 6 Permutation σ_1 applied on initial S-box $ES_{G(4229,643)}$

8	75	148	47	50	199	189	99	227	142	204	127	239	102	208	83
116	31	17	71	235	138	23	251	187	27	145	202	168	120	21	203
26	136	256	13	28	84	93	129	76	39	4	255	137	134	55	11
34	157	152	108	1	216	46	153	80	146	243	2	160	97	49	197
200	106	135	232	70	218	223	185	170	53	12	118	175	242	241	244
121	212	248	234	77	162	214	111	237	144	36	48	14	178	94	20
105	98	253	9	163	19	103	131	41	132	32	117	45	78	246	177
114	159	42	35	249	110	225	112	59	15	228	100	164	245	56	51
219	33	151	52	209	166	40	217	171	30	233	140	192	91	10	113
158	236	3	143	194	25	156	69	85	179	81	191	215	180	16	196
240	222	141	221	62	210	154	201	139	184	5	122	206	238	61	182
37	155	224	130	190	18	250	7	24	54	109	64	126	73	79	92
66	181	174	230	29	96	150	72	89	38	63	161	172	43	167	101
149	186	58	95	229	124	254	213	133	205	90	65	165	87	125	104
6	252	183	74	57	44	67	207	82	188	195	128	88	173	226	123
176	198	22	60	247	107	193	169	220	119	68	115	147	86	231	211

Table7: Permutation σ_2 applied on $ES_{G(4284,3322)}$

219	123	246	127	109	104	184	185	25	86	250	38	249	88	146	26
7	13	105	141	216	58	6	232	253	148	145	73	2	70	245	189
32	153	237	51	18	87	124	17	128	76	222	161	166	197	99	227
176	210	195	113	103	205	235	3	10	234	52	12	42	75	173	59
95	8	180	110	209	151	157	65	16	34	102	98	117	196	229	133
158	137	39	69	35	170	83	4	111	233	112	156	138	244	119	159
31	21	200	44	252	149	230	240	50	248	201	57	49	11	14	130
221	61	67	208	82	30	89	55	242	28	174	85	143	239	43	218
125	15	202	225	54	187	79	1	27	154	214	131	72	71	255	41
207	63	228	107	62	20	241	236	152	155	64	178	116	194	90	192
114	175	132	247	186	78	135	19	213	211	92	193	142	80	212	47
74	190	91	68	164	81	224	167	9	56	29	206	191	179	77	168
217	243	46	226	198	139	96	22	182	199	163	238	160	150	188	53
144	120	66	183	162	215	181	101	5	129	223	172	60	45	118	94
136	122	177	220	106	33	169	97	40	37	254	219	36	109	251	93
100	126	256	24	204	121	140	134	84	115	165	147	48	231	171	23

Table. 8 Permutation σ_3 applied on Sbox3 $ES_{G(4523,2304)}$

128	174	112	121	141	58	71	154	169	33	219	115	172	135	28	179
254	43	214	7	215	102	158	46	233	253	182	21	15	106	201	198
16	17	145	202	173	132	170	138	230	24	126	165	85	252	163	157
225	151	34	105	38	41	220	60	168	9	129	222	232	207	13	101
114	235	10	37	45	51	116	160	238	171	74	237	44	30	4	47
248	221	77	3	103	242	142	66	56	203	107	25	14	236	161	223
210	117	240	196	156	192	153	213	144	184	59	39	181	87	166	194
200	1	62	247	217	228	146	22	167	76	95	119	27	256	199	120
90	94	61	12	2	97	68	226	249	124	191	162	136	183	93	84
127	180	251	148	231	205	86	186	245	100	209	134	241	216	36	111
150	26	63	122	239	31	52	20	80	206	147	40	109	19	64	70
243	69	32	246	108	5	159	92	143	255	204	110	104	197	130	50
11	133	73	140	78	82	65	178	49	67	118	137	55	113	187	190
149	250	96	193	218	177	139	98	18	54	175	208	79	88	234	244
75	6	99	188	23	229	81	8	125	91	48	155	211	185	123	195
72	89	53	35	212	57	29	176	224	83	152	42	131	227	164	189

Table. 9: Permutation σ_4 applied on $ES_{G(4917,2004)}$

253	222	194	250	151	248	49	62	134	26	31	198	186	226	39	15
169	19	11	57	47	103	77	115	29	200	240	141	201	243	34	189
81	197	152	38	146	65	221	176	205	28	5	190	114	24	92	148
86	98	130	164	188	45	40	22	43	48	131	149	210	236	27	20
129	225	234	172	96	12	237	121	215	208	209	157	124	125	199	233
7	122	187	211	44	59	231	63	252	53	145	166	185	54	91	13
41	42	241	61	76	139	87	181	88	126	112	254	212	184	179	71
137	32	165	108	60	161	180	107	147	95	46	69	64	21	214	242
6	229	140	36	117	25	123	68	213	135	113	83	55	52	232	228
35	183	74	153	111	66	224	58	50	4	104	136	110	144	217	227
85	97	72	163	177	116	89	75	192	138	207	133	159	2	155	17
10	70	18	150	128	106	100	79	102	239	78	9	109	249	206	220
30	230	119	120	82	195	93	73	182	171	118	8	143	202	203	67
174	158	255	84	244	256	175	167	193	154	94	178	251	80	238	23
1	245	235	191	162	37	173	170	14	3	105	33	196	127	142	160
223	216	204	101	156	219	247	90	132	16	56	168	51	218	99	246

REFERENCES

1. Adams, C., & Tavares, S. (1990). "The structured design of cryptographically good S-boxes". Journal of cryptology, 3(1), 27-41.
2. Abd EL-Latif, A. A., Abd-El-Atty, B., & Venegas-Andraca, S. E. (2019). "A novel image steganography technique based on quantum substitution boxes,"Optics & Laser Technology, 116, 92-102.
3. Ahmed, H. A., Zolkipli, M. F., & Ahmad, M. (2019). "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. Neural Computing and Applications," 31(11), 7201-7210.
4. Alzaidi, A. A., Ahmad, M., Doja, M. N., Al Solami, E., & Beg, M. S. (2018). "A new 1D chaotic map and $\beta $-hill climbing for generating substitution-boxes," IEEE Access, 6, 55405-55418.
5. Azam, N. A., Hayat, U., & Ullah, I. (2019). "Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field," Frontiers of Information Technology & Electronic Engineering, 20(10), 1378-1389.
6. Azam, N. A., Hayat, U., & Ullah, I. (2018). "An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization," Security and communication networks, 2018.
7. Açikkapi, M. Ş., Özkaynak, F., & Özer, A. B. (2019). "Side-channel analysis of chaos-based substitution box structures," IEEE Access, 7, 79030-79043.
8. Abd el-Latif, A. A., Abd-el-Atty, B., Amin, M., & Iliyasu, A. M. (2020)." Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," Scientific reports, 10(1), 1-16.
9. Abd El-Latif, A. A., Abd-El-Atty, B., Mazurczyk, W., Fung, C., & Venegas-Andraca, S. E. (2020). "Secure data encryption based on quantum walks for 5G Internet of Things scenario," IEEE Transactions on Network and Service Management, 17(1), 118-131.[83]
10. Ashokkumar, C., Roy, B., Venkatesh, M. B. S., & Menezes, B. L. (2020). ""S-Box" Implementation of AES is NOT side channel resistant," Journal of Hardware and Systems Security, 4(2), 86-97.
11. [non linearity table] Cui, L., & Cao, Y. (2007). "A new S-box structure named affine-power-affine," International Journal of Innovative Computing, Information and Control, 3(3), 751-759.
12. Daemen, J., & Rijmen, V. (2013). "The design of Rijndael: AES-the advanced encryption standard," Springer Science & Business Media.
13. Farah, T., Rhouma, R., & Belghith, S. (2017), " A novel method for designing S-box based on chaotic map and teaching–learning-based optimization," Nonlinear dynamics, 88(2), 1059-1074.
14. Farhan, A. K., Ali, R. S., Natiq, H., & Al-Saidi, N. M. (2019). "A new S-box generation algorithm based on multistability behavior of a plasma perturbation model," IEEE Access, 7, 124914-124924.
15. Farah, M. A., Guesmi, R., Kachouri, A., & Samet, M. (2020). "A new design of cryptosystem based on S-box and chaotic permutation," Multimedia Tools & Applications, 79.
16. Farah, M. A., Farah, A., & Farah, T. (2020), "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," Nonlinear Dynamics, 99(4), 3041-3064.
17. Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., & Mahmood, H. (2013),"A group theoretic approach to construct cryptographically strong substitution boxes," Neural Computing and Applications, 23(1), 97-104.
18. Hussain, I., Shah, T., Mahmood, H., Gondal, M. A., & Bhatti, U. Y. (2011),"Some analysis of S-box based on residue of prime number,"Proc Pak Acad Sci, 48(2), 111-115.
19. Hayat, U., Azam, N. A., & Asif, M. (2018),"A method of generating 8× 8 substitution boxes based on elliptic curves,"Wireless Personal Communications, 101(1), 439-451.
20. Haider, M. I., Ali, A., Shah, D., & Shah, T. (2021)," Block cipher's nonlinear component design by elliptic curves: an image encryption application," Multimedia Tools and Applications, 80(3), 4693-4718.
21. Hayat, U., Azam, N. A., Gallegos-Ruiz, H. R., Naz, S., & Batool, L. (2021)," A Truly Dynamic Substitution Box Generator for Block Ciphers Based on Elliptic Curves Over Finite Rings," Arabian Journal for Science and Engineering, 1-13.

22. Kim*, J., & Phan**, R. C. W. (2009),” Advanced differential-style cryptanalysis of the NSA's skipjack block cipher,” Cryptologia, 33(3), 246-270.
23. Khan, M., & Azam, N. A. (2015). “Right translated AES gray S-boxes,” Security and Communication Networks, 8(9), 1627-1635.
24. Khan, M., & Azam, N. A. (2015),” S-boxes based on affine mapping and orbit of power function,” 3D Research, 6(2), 12.
25. Khan, M. F., Ahmed, A., Saleem, K., & Shah, T. (2019),”A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system,” IEEE Access, 7, 84980-84991.
26. Khan, M., & Shah, T. (2015),”A novel construction of substitution box with Zaslavskii chaotic map and symmetric group,” Journal of Intelligent & Fuzzy Systems, 28(4), 1509-1517.[ref2 74]
27. Khan, M. F., Ahmed, A., Saleem, K., & Shah, T. (2019),”A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system,”IEEE Access, 7, 84980-84991.
28. Jamal, S. S., Anees, A., Ahmad, M., Khan, M. F., & Hussain, I. (2019),”Construction of cryptographic S-boxes based on mobius transformation and chaotic tent-sine system.,”IEEE Access, 7, 173273-173285.
29. Lu, Q., Zhu, C., & Deng, X. (2020),” An efficient image encryption scheme based on the LSS chaotic map and single S-box,” IEEE Access, 8, 25664-25678.
30. Lambić, D. (2020). A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. Nonlinear Dynamics, 100(1), 699-711.
31. Liu, H. Kadir, A. & Xu, C. (2020). Cryptanalysis and constructing S-Box based on chaotic map and backtracking. Applied Mathematics and Computation, 376, 125153.
32. Malik, M. S. M., Ali, M. A., Khan, M. A., Ehatisham-Ul-Haq, M., Shah, S. N. M., Rehman, M., & Ahmad, W. (2020),”Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices,” IEEE Access, 8, 35682-35695.
33. Özkaynak, F., Çelik, V., & Özer, A. B. (2017),”A new S-box construction method based on the fractional-order chaotic Chen system,” Signal, Image and Video Processing, 11(4), 659-664.
34. Shafique, A. (2020),”A new algorithm for the construction of substitution box by using chaotic map,” The European Physical Journal Plus, 135(2), 1-13.
35. 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, 2017.
36. Tesař, P. (2010),”A new method for generating high non-linearity s-boxes,” Radioengineering, 19(1), 23-26.
37. Wang, Y., Zhang, Z., Zhang, L. Y., Feng, J., Gao, J., & Lei, P. (2020),”A genetic algorithm for constructing bijective substitution boxes with high nonlinearity,” Information Sciences, 523, 152-166.
38. Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., & Liu, J. (2019),”A novel block encryption algorithm based on chaotic S-box for wireless sensor network,” IEEE Access, 7, 53079-53090.
39. Zhang, T., Chen, C. P., Chen, L., Xu, X., & Hu, B. (2018),” Design of highly nonlinear substitution boxes based on I-Ching operators,” IEEE transactions on cybernetics, 48(12), 3349-3358.
40. 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, 54175-54188.