Wireless Pers Commun (2018) 101:439–451
https://doi.org/10.1007/s11277-018-5698-1

A Method of Generating 8 × 8 Substitution Boxes Based on Elliptic Curves

Umar Hayat[1] · **Naveed Ahmed Azam**[2,3] · **Muhammad Asif**[1]

Published online: 9 April 2018

Abstract Elliptic curve cryptography provides better security and is more efficient as compared to other public key cryptosystems with identical key size. In this article, we present a new method for the construction of substitution boxes(S-boxes) based on points on elliptic curve over prime field. The resistance of the newly generated S-box against common attacks such as linear, differential and algebraic attacks is analyzed by calculating their non-linearity, linear approximation, strict avalanche, bit independence, differential approximation and algebraic complexity. The experimental results are further compared with some of the prevailing S-boxes presented in Shi et al. (Int Conf Inf Netw Appl 2:689–693, 1997), Jakimoski and Kocarev (IEEE Trans Circuits Syst I 48:163–170, 2001), Guoping et al. (Chaos, Solitons Fractals 23:413–419, 2005), Guo (Chaos, Solitons Fractals 36:1028–1036, 2008), Kim and Phan (Cryptologia 33: 246–270, 2009), Neural et al. (2010 sixth international conference on natural computation (ICNC 2010), 2010), Hussain et al. (Neural Comput Appl. https://doi.org/10.1007/s00521-012-0914-5, 2012). Comparison reveals that the proposed algorithm generates cryptographically strong S-boxes as compared to some of the other exiting techniques.

Keywords Elliptic curve · Substitution box · Non-linearity · Differential approximation probability · Algebraic complexity

✉ Naveed Ahmed Azam
azam@amp.i.kyoto-u.ac.jp

Umar Hayat
umar.hayat@qau.edu.pk

Muhammad Asif
asif7638115@gmail.com

1 Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan

2 Department of Applied Mathematics and Physics, Graduate School of Informatics, Kyoto University, Kyoto, Japan

3 Faculty of Engineering Sciences, GIK Institute, Topi, Pakistan

1 Introduction

Information security has gained great attention of researchers in the last few decades. Different types of data security techniques are proposed by cryptographers. These techniques can be divided into two basic categories. One is called cryptography and the other is called steganography [8]. The working principle of cryptographic techniques is to convert secret data into an unreadable form by using key(s). In steganography, the confidential data is embedded into another data in such a way that the unauthorized party cannot notice its presence. According to Shannon, a cryptosystem is secure if it can produce confusion and diffusion in the data up to a certain level [9]. In many cryptographic techniques, substitution box is the only non-linear component which creates confusion and diffusion. Generally, an S-box is said to be good if it can provide high resistance against linear, differential and algebraic cryptanalysis [10–15].The resistance of S-box against common attacks is measured by non-linearity (NL), linear approximation probability (LAP), strict avalanche criterion (SAC), bit independence criterion (BIC), differential approximation probability (DAP) and algebraic complexity (AC).

Rijndael block cipher [16] is adopted by National Institute of Standard and Technology (NIST) as Advanced Encryption Standard (AES). Nowadays, AES is one of the most commonly used cryptosystem. Due to the importance of AES many researchers studied cryptographic properties of its S-box. In [17], a simple algebraic representation of AES S-box is presented. Another, representation of AES S-box is presented in [18]. The study in [18] reveals that AES can be expressed by spare over-determined system of multivariate quadratic equation. The non-linear part of AES is further analyzed in [19] by studying its polynomial representation. They found that AES S-box has only few non-zero terms in its permutation polynomial and has low algebraic complexity. The findings in [18, 19] indicate that the security of AES is suspected against algebraic attacks [13–15].

Because of crucial role of S-box in AES, many cryptographers proposed improved S-box transformations based on different mathematical structures such as algebraic and differential equations. In [20], an upgraded version of AES S-box is presented by exchanging the orders of mapping of AES S-box. Affine function is used in improving the complexity of AES S-box against algebraic attacks in [21]. The resultant S-box has 253 non-zero terms. In [22], Gray codes are used before the implementation of AES S-box. This generates an S-box with 255 non-zero terms. A generalization of Gray S-box based on group action is presented in [23]. In [24], affine mapping and orbit of power function are used for generation of multiple strong S-boxes. Mobius functions are used in [7] for the construction of S-boxes. In [3], logistic map and Baker map are used to develop new S-boxes. Based on Baker and Chebyshev maps, a method of generation of good S-boxes is presented in [4]. In [6], S-boxes are constructed by the combination of neural network and chaotic map. Similarly, many other S-box generation techniques are presented e.g., see [25–31].

Elliptic curves (EC) are also used in developing strong cryptosystems. The concept of elliptic curve was first time introduced in cryptography in [32]. Furthermore, a cryptosystem is presented in [32] which is 20 percent faster than Diffie–Hellman protocol. In [33], a cryptosystem based on EC over finite field is discussed. In [34], a relationship between the points of hyperelliptic curves and non-linearity of S-box is presented. The concept of discrete logarithmic problem is used in [35] to develop a highly secure and fast security system. In [36], elliptic curve cryptography (ECC) is compared with RSA. It is noticed that ECC with smaller key size has better security than that of RSA with larger key size. The applications and advantages of ECC are discussed in [37]. Similarly, different

ECC techniques are discussed in [38]. In literature [39–42], elliptic curves are used for generation of pseudo random numbers which are very important for many cryptosystems.

The aim of this paper is to present a simple and efficient algorithm for construction of cryptographically strong S-boxes based on elliptic curves over prime field. The proposed technique uses the x-coordinate of ordered pairs of EC followed by modulo operation 256. Rest of the paper is organized as follow: Sect. 2 contains some preliminaries. The algorithm is presented in Sect. 3. The experimental results and their comparison are given in Sect. 4.

2 Preliminaries

2.1 Modulo Operation

The modulo operation outputs the remainder when one number a is divided by another number b, where $b \leq a$. The result of modulo operation on numbers a and b is often denoted by a mod b. For example, "258 mod 256" is equal to 2 because after dividing 258 by 256, the remainder is 2.

2.2 Elliptic Curve Over a Finite Prime Field

Consider a prime field F_p having p elements, where p is a prime number. For each prime p number there exists exactly one prime field F_p. For any two integers of F_p say a and b, the elliptic curve on field F_p is defined as:

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

provided $(4a^3+27b^2 \neq 0)(\text{mod}\, p)$, where O denotes the infinite point. The number of elements $\#\left(E(F_p)\right)$ in elliptic curve $E(F_p)$ is equal to the number of points lying on elliptic curve over F_p. Hasse Theorem [43] gives the bounds of total number of points on elliptic curve:

$$p + 1 - 2\sqrt{p} \leq \#E\left(F_p\right) \leq p + 1 + 2\sqrt{p}.$$

The expression $4a^3 + 27b^2$ is called the discriminant of the elliptic curve.

3 S-Box Construction Technique

A simple technique for generation of cryptographically strong S-boxes is discussed in this section. The construction technique is based on elliptic curve over a prime field F_p. The proposed algorithm consists of four main steps which are given below:

Step 1. Choose two distinct elements a and b from prime field F_p, where p is large prime. The large value of p is selected so that the corresponding elliptic curve EC has at least 256 ordered pairs. The lower bound of p for proposed algorithm is calculated by using Hasse's Theorem which is $p > 289$.

Step 2. Generate the elliptic curve $E_p(a, b)$ by using the equation:

$$(y^2 = x^3 + ax + b) \pmod p.$$

Step 3. Let $E_{p,x}(a,b)$ denotes the set of x-coordinate of all ordered pairs of $E_p(a,b)$. Now, apply modulo 256 on $E_{p,x}(a,b)$ to get $E^{256}_{p,x}(a,b)$. This operation is used to restrict the values of $E_{p,x}(a,b)$ in the range 0–255.
Step 4. Finally, an S-box S^b_a is generated by selecting first 256 distinct integers of $E^{256}_{p,x}(a,b)$.

A flowchart of the proposed technique is presented in Fig. 1. The proposed algorithm is implemented on several ECs for generation of S-boxes. For example, the S-box S^{785}_{1878} generated by $E_{2861}(1878\,,785)$ is presented in Table 1. The points of $E_{2861}(1878\,,785)$ are shown in Fig. 2.

4 Analysis and Comparison

Different security performance tests including non-linearity test, linear approximation probability, strict avalanche criterion, bit independence criterion, differential approximation probability and algebraic complexity test are applied on the S-box S^{785}_{1878} generated by the proposed algorithm. These tests are implemented to investigate the efficiency of the proposed technique. A brief introduction to these tests and their experimental results are presented in this section. A comparison of results of S^{785}_{1878} with some of the prevailing S-boxes generated by other construction techniques is also presented in this section.

4.1 Bijective

The step 4 of the proposed algorithm ensures that all newly developed S-boxes are bijective.

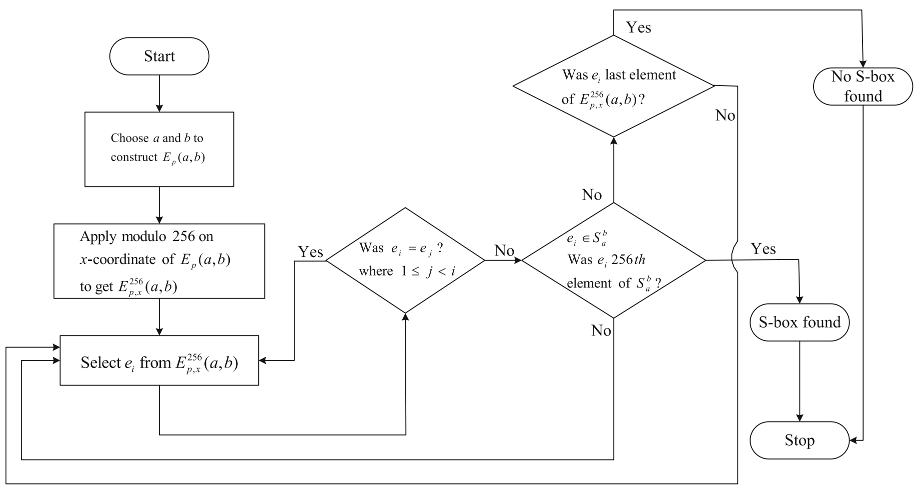

Fig. 1 Flowchart of proposed technique

Table 1 S-box S^{785}_{1878} generated by proposed algorithm over the EC $E_{2861}(1878, 785)$

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

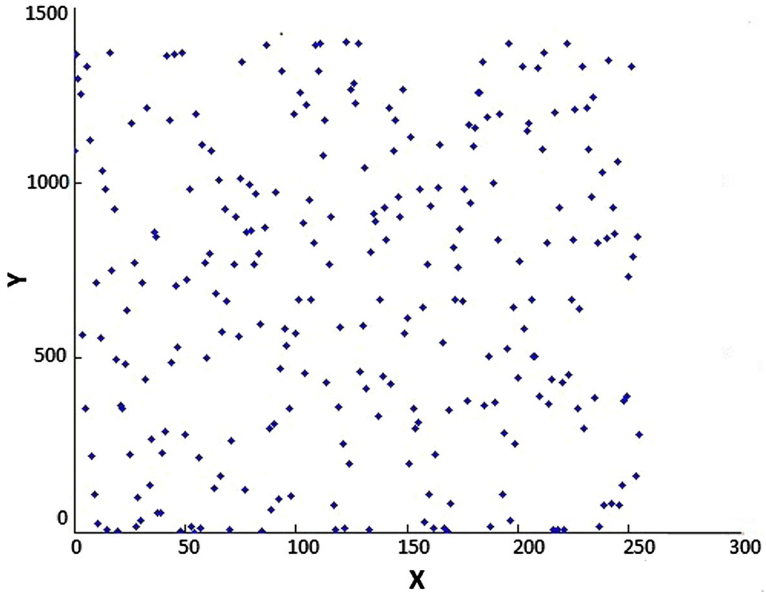

Fig. 2 Points of $E_{2861,x}(1878, 785)$

4.2 Non-linearity (NL)

The concept of non-linearity is introduced in [10] to quantify the confusion creation ability of an S-box. For a given S-box $S : GF(2^8) \to GF(2^8)$, NL is measured by calculating the distance $\delta(S)$ of S to affine functions over $GF(2^8)$:

$$\delta(S) = \min_{\alpha,w,\beta} \#\{x \in GF(2^8) | \alpha \cdot S(x) \neq \beta \cdot x \oplus w\},$$

where $\alpha \in GF(2^8), w \in GF(2), \beta \in GF(2^8)\backslash\{0\}$ and "$\cdot$" denotes the dot product over $GF(2)$.

The optimal value of non-linearity of a bijective S-box over $GF(2^8)$ is 120. It is also noticed in [10], that an S-box with maximum non-linearity may not satisfies other cryptographic criterion. Furthermore, the study in [10] suggests that an S-box with nearly optimal NL and satisfying other security test is of special interest. We calculated the non-linearity of the S-box S_{1878}^{785} generated by the proposed algorithm. The result of this test is 100.

4.3 Linear Approximation Probability (LAP)

In [11], linear approximation probability of an S-box is introduced. This calculates the probability of obtaining a linear approximation of a given S-box. LAP of an S-box depends upon the coincidence of input bits with output bits. The mathematical expression of LAP is given below:

$$N(a,\beta) = \#\{x \in GF(2^8) | \alpha \cdot x = \beta \cdot S(x)\} - 2^{n-1},$$

$$LAP(S) = \frac{1}{2^n}\left\{\max_{\alpha,\beta} |N(a,\beta)|\right\},$$

where $\alpha \in GF(2^8), \beta \in GF(2^8)\backslash\{0\}$ and "$\cdot$" denotes the dot product over $GF(2)$.

The LAP of newly generated S-box S_{1878}^{785} is 0.0547.

4.4 Strict Avalanche Criterion (SAC)

This criterion is developed in [44] by combining the concepts of avalanche effect and completeness. The probability of change in output bits when a single input bit is inverted is calculated in this test. SAC of an S-box is calculated with an 8×8 dependence matrix whose entries are calculated by:

$$\left\{\frac{1}{2^n}\left[w\left(S_i(x+\alpha_j) + S_i(x)\right)\right] \middle| \alpha_j \in GF(2^8),\ w(\alpha_j) = 1 \text{ and } 1 \le i, j \le 8\right\},$$

where $w(\alpha_j)$ is the number of non-zero bits in α_j. SAC is satisfied if all entries of dependence matrix are closer to 0.5. The SAC result for S_{1878}^{785} is presented in Table 2. The minimum value of SAC is 0.4219 while its maximum value is 0.5938.

4.5 Bit Independence Criterion (BIC)

BIC is also proposed in [44] to analyze the independence between pair of output bits when an input bit is complemented. BIC of pair of output bit A and B is calculated by finding correlation coefficient of A and B. The minimum and maximum value of BIC of S_{1878}^{785} are 0.4688 and 0.5293 respectively. The BIC result is given in Table 3.

Table 2 Strict avalanche results of S_{1878}^{785}

0.5312	0.5312	0.4844	0.5000	0.4687	0.4687	0.4844	0.5937
0.4531	0.4688	0.5938	0.5000	0.4844	0.5312	0.5000	0.5000
0.5469	0.5000	0.4844	0.5000	0.5156	0.5000	0.4688	0.4688
0.5469	0.4688	0.4844	0.5312	0.5000	0.5312	0.4844	0.5156
0.4844	0.4688	0.4531	0.4531	0.5156	0.4844	0.4844	0.5468
0.5312	0.5156	0.4844	0.4531	0.4375	0.4844	0.5000	0.4375
0.4688	0.5000	0.4219	0.4844	0.5156	0.5312	0.50000	0.4844
0.5625	0.5469	0.4688	0.5156	0.5938	0.4844	0.5625	0.5312

Table 3 BIC of S_{1878}^{785}

–	0.4688	0.5098	0.5000	0.4863	0.5156	0.5176	0.4785
0.4687	–	0.5195	0.4844	0.4824	0.4902	0.4883	0.4805
0.5098	0.5195	–	0.5293	0.4805	0.5078	0.5078	0.5039
0.5000	0.4844	0.5293	–	0.4844	0.5254	0.4785	0.4785
0.4863	0.4824	0.4805	0.4844	–	0.5000	0.5195	0.4785
0.5156	0.4902	0.5078	0.5254	0.5000	–	0.5098	0.5000
0.5176	0.4883	0.5078	0.4785	0.5195	0.5098	–	0.4766
0.4785	0.4805	0.5039	0.4785	0.4785	0.5000	0.4766	–

4.6 Differential Approximation Probability (DAP)

Differential approximation probability is presented in [12] to find the probability effect of a specific difference in the input bit on the difference of the resultant output bits. The mathematical expression for DAP of an S-box S is given below:

$$DAP(S) = \max_{\Delta x, \Delta y}\{\#\{x \in GF(2^8) \mid S(x + \Delta x) - S(x) = \Delta y\}\},$$

where Δx, $\Delta y \in GF(2^8)$. We applied DAP test on the proposed S-box and the result is given in Table 4. The DAP of S_{1878}^{785} is 0.0391.

4.7 Algebraic Complexity (AC)

Linear polynomial for an S-box is defined in [45]. The algebraic complexity of an S-box is measured by the number of non-zero terms in its linear polynomial expression. In Table 5, coefficients of polynomial corresponding to S_{1878}^{785} are presented. The AC of S-box S_{1878}^{785} generated by the proposed algorithm is 255.

4.8 Performance Comparison

The former tests are also applied on some of the well-known S-boxes presented in [1–7] to compare the efficiency of proposed algorithm with other S-box generation algorithms. The results are presented and compared in Table 6.

Table 4 DAP of S_{1878}^{785}

0.0234	0.0312	0.0391	0.0312	0.0312	0.0312	0.0234	0.0312	0.0234	0.0312	0.0312	0.0234	0.0234	0.0312	0.0234	0.0312
0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0312	0.0312	0.0312	0.0234	0.0234	0.0234	0.0312	0.0234	0.0312	0.0312
0.0312	0.0312	0.0234	0.0234	0.0234	0.0312	0.0312	0.0234	0.0312	0.0234	0.0234	0.0312	0.0312	0.0234	0.0312	0.0234
0.0234	0.0312	0.0234	0.0234	0.0312	0.0391	0.0234	0.0156	0.0312	0.0234	0.0312	0.0234	0.0234	0.0312	0.0234	0.0234
0.0234	0.0234	0.0234	0.0312	0.0234	0.0234	0.0234	0.0234	0.0234	0.0156	0.0234	0.0234	0.0234	0.0312	0.0312	0.0234
0.0312	0.0234	0.0234	0.0234	0.0312	0.0234	0.0234	0.0312	0.0234	0.0234	0.0234	0.0312	0.0234	0.0234	0.0234	0.0234
0.0234	0.0390	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0156	0.0234	0.0234	0.0234	0.0312	0.0234
0.0312	0.0234	0.0234	0.0234	0.0312	0.0234	0.0234	0.0234	0.0234	0.0312	0.0234	0.0312	0.0234	0.0234	0.0312	0.0234
0.0234	0.0312	0.0156	0.0234	0.0234	0.0234	0.0234	0.0234	0.0312	0.0312	0.0234	0.0312	0.0234	0.0312	0.0234	0.0234
0.0234	0.0234	0.0234	0.0234	0.0312	0.0312	0.0312	0.0156	0.0312	0.0234	0.0234	0.0312	0.0234	0.0234	0.0312	0.0234
0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0391	0.0391	0.0234	0.0234	0.0312	0.0234	0.0312	0.0234	0.0312	0.0234
0.0234	0.0312	0.0234	0.0234	0.0312	0.0312	0.0312	0.0312	0.0234	0.0234	0.0312	0.0156	0.0234	0.0234	0.0312	0.0234
0.0234	0.0312	0.0312	0.0234	0.0234	0.0234	0.0234	0.0234	0.0312	0.0234	0.0234	0.0234	0.0312	0.0234	0.0312	0.0234
0.0234	0.0234	0.0312	0.0390	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0156	0.0312	0.0234	0.0234
0.0234	0.0312	0.0312	0.0234	0.0234	0.0234	0.0391	0.0312	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234
0.0234	0.0312	0.0234	0.02344	0.02344	0.0391	0.0234	0.0312	0.0234	0.0234	0.0312	0.0234	0.0312	0.0234	0.0234	0

Table 5 AC of S_{1878}^{785}

0	238	101	176	255	34	86	90	193	221	207	45	63	116	145	39
233	101	178	45	58	240	165	244	89	201	199	179	182	121	206	249
190	106	85	75	201	178	152	142	37	106	174	154	92	136	229	121
168	84	228	249	72	153	28	9	122	246	130	192	90	87	78	238
12	193	178	53	71	72	87	189	148	81	121	187	58	42	231	93
172	30	76	158	124	98	202	244	123	64	31	169	31	211	180	66
83	124	254	111	134	48	18	75	195	120	206	168	201	241	22	242
102	175	77	195	247	179	29	18	36	230	117	136	91	243	107	186
41	12	17	163	83	41	170	14	52	229	219	188	25	145	5	72
2	24	197	43	157	158	3	93	200	224	157	118	237	105	105	39
82	172	62	60	203	173	182	22	152	53	233	17	118	50	130	207
152	175	178	149	138	102	197	245	194	112	85	74	10	195	26	94
127	191	203	16	43	11	230	201	84	4	106	42	60	40	27	212
222	142	155	137	233	120	86	238	221	31	206	99	169	18	254	203
141	179	196	255	253	55	80	193	4	4	112	192	3	94	83	131
142	253	137	128	218	109	222	29	223	182	61	135	32	213	72	54

Table 6 Comparison of newly generated S-boxes with some of the existing S-boxes

S-box	Bijective	NL	LAP	SAC (Max)	SAC (Min)	BIC (Max)	BIC (Min)	DAP	AC
[1]	Yes	108	0.156	0.502	0.406	0.503	0.47	0.046	255
[2]	Yes	98	0.0352	0.5781	0.4453	0.5156	0.4922	0.046	256
[3]	Yes	103	0.0352	0.5703	0.4414	0.5039	0.4961	0.0391	255
[4]	Yes	102	0.078	0.6094	0.3750	0.5215	0.4707	0.0391	254
[5]	Yes	104	0.109	0.593	0.39	0.499	0.454	0.0469	255
[6]	Yes	106	0.0469	0.5938	0.4375	0.5313	0.4648	0.0391	251
[7]	Yes	100	0.125	0.593	0.493	0.476	0.0137	0.0391	255
S_{1878}^{785}	Yes	100	0.0547	0.5937	0.4219	0.5293	0.4688	0.0391	255
S_{1710}^{2429}	Yes	104	0.0391	0.625	0.3906	0.53125	0.4707	0.0391	255

Table 6 shows that the NL of S-boxes in [2, 7] is less than or equal to the NL of the S-box constructed by the proposed algorithm. The LAP of S_{1878}^{785} is less than that of the S-boxes presented in [1, 4, 5, 7]. This fact reveals that the S_{1878}^{785} creates high confusion in the data and hence higher resistance against linear attack [11] as compared to [1, 4, 5, 7]. The SAC and BIC results of S_{1878}^{785} and other S-boxes used in Table 6 are almost the same. Thus, the S-box generated by the proposed technique and S-boxes presented in Table 6 create diffusion in the data of equal magnitude. The DAP of S_{1878}^{785} is less than or equal to the DAP of S-boxes [1–7]. Thus, the proposed encryption technique generates S-box with high resistance against differential cryptanalysis [12] as compared to the others. The AC of S_{1878}^{785} is maximum which shows that it is secure against algebraic attacks [13–15]. Similarly, the analysis results of another newly generated S-box S_{1710}^{2429} over EC

$E_{2609}(1710, 2429)$ are listed in Table 6. It is evident from Table 6 that the performance of S_{1710}^{2429} is also comparable with the other S-boxes.

5 Conclusion

A novel S-box construction technique is presented in this article. The proposed algorithm uses the x-coordinate of ordered pairs of an elliptic curve over prime field $E_p(a, b)$ for the generation of cryptographically strong S-box S_b^a, where p is a prime greater than 289 and a and b belong to finite field F_p. Several tests are applied on newly developed S-boxes S_b^a to analyze their cryptographic strength. Furthermore, cryptographic properties of S_b^a are compared with some of the existing prevailing S-boxes. Experimental results showed that the proposed algorithm is capable of generating S-boxes with high resistance against linear, differential and algebraic attacks.

The S-boxes generated by the proposed technique depend upon the selection of p, a and b. In other words, by changing either p, a or b, another S-box will be generated. Thus, the proposed algorithm can also be extended to an image encryption technique that uses dynamic S-boxes generated by varying the values of parameters p, a and b. In such encryption technique p, a and b will behave as keys. Furthermore, the proposed algorithm can be extended for generation of more secure S-boxes based on classification of Rossby wave triads by elliptic curves, see [46].

Compliance with Ethical Standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Shi, X. Y., Xiao, H., You, X. C., & Lam, K. Y. (1997). A method for obtaining cryptographically strong 8 × 8 S-boxes. *International Conference on Information Network and Application, 2,* 689–693.
2. Jakimoski, G., & Kocarev, L. (2001). Chaos and cryptography: block encryption ciphers. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48,* 163–170.
3. Guoping, T., Xiaofeng, L., & Yong, C. (2005). A novel method for designing S-boxes based on chaotic maps. *Chaos, Solitons & Fractals, 23,* 413–419.
4. Guo, C. (2008). A novel heuristic method for obtaining S-boxes. *Chaos, Solitons & Fractals, 36,* 1028–1036.
5. Kim, J., & Phan, R. C. W. (2009). Advanced differential-style cryptanalysis of the NSA's skipjack block cipher. *Cryptologia, 33,* 246–270.
6. Neural, Y. W., Li, Y., Min, L., & Sihong, S. A method for designing S-box based on chaotic neural network. In *2010 Sixth international conference on natural computation (ICNC 2010).*
7. Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., & Mehmood, H. (2012). A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-012-0914-5.
8. Hussain, I., Azam, N. A., & Shah, T. (2014). Stego optical encryption based on chaotic S-box transformation. *Optics & Laser Technology, 61,* 50–56.
9. Shannon, C. E. (1949). Communications theory of secrecy systems. *Bell Labs Technical Journal, 20,* 656–715.
10. Willi, M., & Othmar, S. (1990). Nonlinearity criteria for cryptographic functions. *Advances in Cryptology–EUROCRYPT '89 LNCS, 434,* 549–562.
11. Mitsuru, M. (1994). Linear cryptanalysis method for DES cipher. *Advances in Cryptology–EUROCRYPT '93 LNCS, 765,* 386–397.
12. Eli, B., & Adi, S. (1991). Differential crypt analysis of DES-like cryptosystems. *Advances in Cryptology - CRYPTO '90 LNCS, 537,* 2–21.

13. Thomas, J., & Knudsen, L, R. (1997). The interpolation attack on block ciphers. In *International workshop on fast software encription (FSE)*, *Fast Software Encription* (pp. 28–40).
14. Nicolas, C., Alexander, K., Jacques, P., & Adi, S. (2000). Effcient algorithms for solving overdefined systems of multivariate polynomial equations. In *International conference on the theory and application of cryptographic techniques EUROCRYPT 2000*: *advances in cryptology-EUROCRYPT* (pp. 392–407).
15. Courtois, N. T., & Josef, P. (2002). Cryptanalysis of block ciphers with overdefined systems of equations. *ASIACRYPT 2002 LNCS, 2501,* 267–287.
16. Daemen, J., & Rijmen, V. (1999). AES proposal: Rijndael (Version 2). NIST AES, csrc.nist.gov/encryption/aes.
17. Ferguson, N., Schroeppel, R., & Whiting, D. A. (2001). Simple algebraic representation of Rijndael. In *Selected areas in cryptography SAC 01, LNCS 2259* (pp. 103–111).
18. Murphy, S., & Robshaw, M. J. (2002). Essential algebraic structure within the AES. In *Proceedings of the 22th annual international cryptology* (pp. 1–16). Berlin: Springer.
19. Rosenthal, J. (2003). A polynomial description of the Rijndael advanced encryption standard. *Journal of Algebra and its Applications, 2,* 223–236.
20. Liu, J., Wai, B., Cheng, X., & Wang, X. (2005). An AES S-box to increase complexity and cryptographic analysis. In *Proceedings of the 19th international conference on advanced information networking and applications*, Taiwan (pp. 724–728).
21. Cui, L., & Cao, Y. (2007). A new S-box structure named affine power-affine. *International Journal of Innovative Computing, Information and Control, 3,* 751–759.
22. Tran, M. T., Bui, D. K., & Doung, A. D. (2008). Gray S-box for advanced encryption standard. *International Conference on Computational Intelligence and Security, 1,* 253–258.
23. Khan, M., & Azam, N. A. (2014). Right translated AES Gray S-box. *Security and Network Communication*. https://doi.org/10.1002/sec.1110.
24. Khan, M., & Azam, N. A. (2015) S-boxes based on affine mapping and orbit of power function. *3D Research.* https://doi.org/10.1007/s13319-015-0043-x.
25. Hao, Y., Longyan, L., & Yong, W. (2010). An S-box construction algorithm based on spatiotemporal chaos. In *International conference on communications and mobile computing*.
26. Yong, W., Kwok, W., Changbing, L., & Yang, L. (2012). A novel method to design S-box based on chaotic map and genetic algorithm. *Physics Letters A, 376,* 827–833.
27. Wang, Y., Wong, K. W., Li, C., & Li, Y. (2012). A novel method to design S-box based on chaotic map and genetic algorithm. *Physics Letters A, 376*(376), 827–833.
28. Hussain, I., Azam, N. A., & Shah, T. (2014). Stego optical encryption based on chaotic S-box transformation. *Optics and Laser Technology, 61,* 50–56.
29. Khan, M., Shah, T., & Syeda, I. B. (2016). Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Computing and Applications, 27,* 677–685. https://doi.org/10.1007/s00521-015-1887-y.
30. Vijayan, P., Paul, V., & Wahi, A. (2017). Dynamic colour table: A novel S-box for cryptographic applications. *International Journal of Communication Systems*. https://doi.org/10.1002/dac.3318.
31. Özkaynak, F., Çelik, V., & Özer, A. B. (2017). A new S-box construction method based on the fractional-order chaotic Chen system. *SIViP, 11,* 659. https://doi.org/10.1007/s11760-016-1007-1.
32. Miller, V. (1986). Uses of elliptic curves in cryptography. *Advances in Cryptology, 85,* 417–426.
33. Neal, K. (1987). Elliptic curve cryptosystems. *Mathematics of Computation, 48*(177), 203–209.
34. Jung, H. C., Seongtaek, C., & Choonsik, P. (1999). S-boxes with controllable nonlinearity, EUROCRYPT'99. *LNCS, 1592,* 286–294.
35. Neal, K., Alfred, M., & Scott, V. (2000). The state of elliptic curve cryptography. *Designs, Codes and Cryptography, 19,* 173–193.
36. Amara, M., & Siad, A.(2011). Elliptic curve cryptography and its applications. In *7th international workshop on systems, signal processing and their applications* (pp. 247–250).
37. Vansfone, S. A. (1997). Elliptic curve cryptography. The answer to strong, fast public-key cryptography for securing constrained environments. *Information Security Technical Report, 2*(2), 78–87.
38. Williams, S. (2000). *Cryptography and network security* (4th ed.). New York: Prentice Hall.
39. Gong, G., Berson, T. A., & Stinson, D. R. (2000). Elliptic curve pseudorandom sequence generators. In *Selected areas in cryptography* (Kingston, ON, 1999), (pp. 34–48). Berlin: Springer.
40. Caragiu, M., Johns, R. A., & Gieseler, J. (2006). Quasi-random structures from elliptic curves. *Journal of Algebra, Number Theory and Applications, 6,* 561–571.
41. Farashahi, R. R., & Sidorenko, S. B. A. (2007). Efficient pseudorandom generators based on the DDH assumption. In Okamoto, T., Wang, X. (eds.) *PKC 2007. LNCS* (Vol. 4450, pp. 426–441). Heidelberg: Springer.

42. Omar, R., & Zbigniew, K. (2015). On pseudo-random number generators using elliptic curves and chaotic systems. *Applied Mathematics and Information Sciences, 9*(1), 31–38.
43. Brown, D. R. L. (2009). *SEC 1: Elliptic curve cryptography*. Mossossaiga: Certicom Corp.
44. Webster, A. F., & Tavares, S. E. (1986). On the design of S-boxes. *Advances in Cryptology–CRYPT0 '85 LNCS, 218,* 523–534.
45. Lidl, R., & Niederreiter, H. (1994). *Introduction to finite fields and their applications* (2nd ed.). Cambridge: Cambridge University Press.
46. Bustamante, M. D., & Hayat, U. (2013). Complete classification of discrete resonant Rossby/drift wave triads on periodic domains. *Communications in Nonlinear Science and Numerical Simulation, 18,* 2402–2419.

Umar Hayat received his Ph.D. degree from the University of Warwick, UK in 2011. He was post doctoral research fellow at University College Dublin, Ireland in 2012. During 2014, he was a visiting research fellow at the International Center for Theoretical Physics, Trieste, Italy. He is currently working as an assistant professor at Quaid-i-Azam University Islamabad, Pakistan. His main research interests include Algebraic Geometry and its applications. He has successfully used elliptic curves to solve problems from practical domains.

Naveed Ahmed Azam is a research fellow at the Department of Applied Mathematics and Physics, Graduate School of Informatics, Kyoto University, Japan. He obtained his M.Sc. and M.Phil. Degrees in Mathematic from the Quaid-i-Azam University, Islamabad. His research interests include Cryptography and Discrete Mathematics and has published papers related to the above topics in top journals.

Muhammad Asif obtained his Master degree in Mathematics from Punjab University, Lahore, Pakistan in 2014. He is currently perusing his M.Phil. Degree in Mathematics from Quaid-i-Azam University, Islamabad, Pakistan.