

## Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field\*

Naveed Ahmed AZAM<sup>†‡1</sup>, Umar HAYAT<sup>†2</sup>, Ikram ULLAH<sup>2</sup>

<sup>1</sup>Department of Applied Mathematics and Physics, Graduate School of Informatics, Kyoto University, Kyoto 606-8501, Japan

<sup>2</sup>Department of Mathematics, Quaid-i-Azam University, Islamabad 44000, Pakistan

<sup>†</sup>E-mail: azam@amp.i.kyoto-u.ac.jp; umar.hayat@qau.edu.pk

Received July 18, 2018; Revision accepted Apr. 17, 2019; Crosschecked Oct. 10, 2019

**Abstract:** Elliptic curve cryptography has been used in many security systems due to its small key size and high security compared with other cryptosystems. In many well-known security systems, a substitution box (S-box) is the only non-linear component. Recently, it has been shown that the security of a cryptosystem can be improved using dynamic S-boxes instead of a static S-box. This necessitates the construction of new secure S-boxes. We propose an efficient method to generate S-boxes that are based on a class of Mordell elliptic curves over prime fields and achieved by defining different total orders. The proposed scheme is developed in such a way that for each input it outputs an S-box in linear time and constant space. Due to this property, our method takes less time and space than the existing S-box construction methods over elliptic curves. Computational results show that the proposed method is capable of generating cryptographically strong S-boxes with security comparable to some of the existing S-boxes constructed via different mathematical structures.

**Key words:** Substitution box; Finite field; Mordell elliptic curve; Total order; Computational complexity  
<https://doi.org/10.1631/FITEE.1800434>

**CLC number:** TP309

### 1 Introduction


Cryptography deals with techniques that secure private data. In these techniques, data is transformed into an unreadable form using keys that prevent adversaries from extracting useful information. Substitution boxes (S-boxes) are the only non-linear component of many well-known cryptosystems including the advanced encryption system (AES). Therefore, the security of such cryptosystems depends only on the cryptographic properties of their S-boxes. Shannon (1949) proved that a cryptosystem is secure if it can create confusion and diffusion in data up to a certain level. An S-box is cryptographically strong

enough to create the desired confusion and diffusion if it passes certain tests, including tests of non-linearity, approximation, strict avalanche, bit independence, and algebraic complexity.

Nowadays, AES is considered to be the most secure and widely used cryptosystem. Many cryptographers have studied its S-box. Jakobsen and Knudsen (1997), Courtois and Pieprzyk (2002), Murphy and Robshaw (2002), and Rosenthal (2003) have revealed that the AES S-box is vulnerable to algebraic attacks because of its sparse polynomial representation. It has been noted that a cryptosystem based on a single S-box is unable to generate a desirable level of security if the data is highly correlated (Hussain et al., 2014; Azam, 2017). Furthermore, it has been shown that the security of a cryptosystem can be improved using dynamic S-boxes instead of a static S-box (Kazlauskas and Kazlauskas, 2009; Manjula and Mohan, 2013; Rahnama et al., 2013; Katiyar and Jeyanthi, 2016; Maram and Gnanasekar,

<sup>‡</sup> Corresponding author

\* Project supported by the JSPS KAKENHI (No. 18J23484)

 ORCID: Naveed Ahmed AZAM, <http://orcid.org/0000-0002-7941-3419>

© Zhejiang University and Springer-Verlag GmbH Germany, part of Springer Nature 2019

2016; Agarwal et al., 2018). The two principal reasons behind this are: (1) Static S-boxes are vulnerable to data analysis attacks and subkey attacks in which subkeys are obtained using an inverse subbyte, if the inverse of an S-box is known (Rahnama et al., 2013); (2) The algorithms using a dynamic S-box are more complex and can provide more overhead to cryptanalysts when compared with a static S-box (Kazlauskas and Kazlauskas, 2009; Manjula and Mohan, 2013; Katiyar and Jeyanthi, 2016; Maram and Gnanasekar, 2016; Agarwal et al., 2018). Different image encryption algorithms using dynamic S-boxes were presented in Zaibi et al. (2009), Wang and Wang (2014), Devaraj and Kavitha (2016), and Liu et al. (2016). In these studies, it turned out that image cryptosystems based on a dynamic S-box provide better security when compared with the cryptosystems using a static S-box. Due to these reasons, many researchers have proposed new S-box generation techniques based on different mathematical structures, including algebraic and differential equations.

For an S-box design technique, the resultant S-box must have the following characteristics: (1) It must inherit the properties of the underlying mathematical structure. This is an important requirement which leads to efficient generation and good understanding of the cryptographic properties of resultant S-box. (2) It must be generated in low time and space complexity. (3) It must satisfy the security tests. Of course, an S-box generation technique with high time complexity is not suitable for cryptosystems using multiple and dynamic S-boxes. Liu et al. (2005) presented an improved AES S-box based on an algebraic method. Cui and Cao (2007) used an affine function to generate an S-box with 253 non-zero terms in its polynomial representation. Tran et al. (2008) used composition of a Gray code instead of an affine mapping with the AES S-box to generate an S-box with high algebraic complexity. Khan and Azam (2015a, 2015b) proposed different methods for the generation of cryptographically strong S-boxes based on a generalization of the Gray S-box and affine functions. Azam (2017) used the S-boxes introduced by Khan and Azam (2015a) for the encryption of confidential images. Chaotic maps including Baker, logistic, and Chebyshev maps were used to generate new S-boxes in Tang et al. (2005), Chen (2008), and Wang et al. (2010). Similarly, elliptic curves (ECs)

were used in the field of cryptography for the development of highly secure cryptosystems. Miller (1986) presented an EC-based security system, which has a smaller key size and higher security than RSA. Cheon et al. (1999) developed a link between the points on hyper-elliptic curves and the non-linearity of an S-box. Hayat et al. (2018) and Hayat and Azam (2019) first used an EC over a prime field for the generation of dynamic S-boxes. In these works, an S-box is generated using the  $x$ -coordinate of the points on an ordered EC over a prime  $p$ , where the ordering  $\prec$  on the points is performed with respect to their values (i.e., for any two points  $(x_1, y_1)$  and  $(x_2, y_2)$  on the EC,  $(x_1, y_1) \preceq (x_2, y_2)$  if  $y_1^2 \leq y_2^2 \pmod{p}$ ). Actually, the scheme in Hayat and Azam (2019) is a generalization of the method in Hayat et al. (2018). Although these methods are capable of generating cryptographically strong S-boxes, they have the following two weaknesses: (1) They need to compute and store the EC during their generation process. Due to this, the time and space complexities of these schemes are  $O(p^2)$  and  $O(p)$  respectively, where  $p \geq 257$  is the prime of the underlying EC. (2) The output of these methods is uncertain; i.e., for each set of input parameters, the algorithms do not necessarily output an S-box.

The purpose of this work is to develop a novel and efficient S-box generation technique based on a finite Mordell elliptic curve (MEC), which generates a secure S-box inheriting the properties of the underlying MEC for each set of input parameters. To achieve this, we define some typical types of total orders on the points of the MEC and use the  $y$ -coordinate instead of the  $x$ -coordinate to obtain an S-box.

## 2 Preliminaries

For a prime  $p$  and two non-negative integers  $a$  and  $b \leq p-1$ , the EC  $E_{p,a,b}$  over a prime field  $F_p$  is defined to be the collection of the infinity point  $O$  and all ordered pairs  $(x, y) \in F_p \times F_p$ , satisfying

$$y^2 \equiv x^3 + ax + b \pmod{p},$$

where  $p$ ,  $a$ , and  $b$  are parameters of  $E_{p,a,b}$ . An

approximation for the number  $|E_{p,a,b}|$  of points on  $E_{p,a,b}$  can be obtained using the Hasse formula (Washington, 2008), expressed as

$$\text{abs}(|E_{p,a,b}| - p - 1) \leq 2\sqrt{p},$$

where  $\text{abs}(\ )$  represents the absolute value.

The MEC is a special kind of ECs with  $a=0$ . The significance of some MECs  $E_{p,0,b}$  is that they have exactly  $(p+1)$  points. The following theorem (Washington, 2008) gives the information on such MECs:

**Theorem 1** Let  $p > 3$  be a prime such that  $p \equiv 2 \pmod{3}$ . For each  $b \in \mathbf{F}_p$ , the MEC  $E_{p,0,b}$  has exactly  $(p+1)$  distinct points, and has each integer in  $[0, p-1]$  exactly once as the  $y$ -coordinate.

Hence, an MEC  $E_{p,0,b}$  where  $p \equiv 2 \pmod{3}$  is simply denoted as  $E_{p \equiv 2, b}$ .

### 3 Description of the proposed S-box design technique

In this section, we give an informal idea of our proposed method. Our aim is to develop an S-box generation technique based on an MEC which outputs an S-box: (a) in linear time and constant space for each set of input parameters; (b) inheriting the properties of the underlying MEC; (c) having high security against cryptanalysis. Note that the S-box design techniques proposed by Hayat et al. (2018) and Hayat and Azam (2019) do not satisfy conditions (a) and (b). One of the possible ways of designing such a technique is to input an EC which contains all integers from  $[0, 255]$  without repetition. Therefore, the proposed algorithm takes an MEC  $E_{p \equiv 2, b}$  as an input and uses the  $y$ -coordinate instead of the  $x$ -coordinate to generate an S-box. The next task is to use the  $y$ -coordinate in such a way that the resultant S-box inherits the properties of the underlying MEC. Of course, the use of some arithmetic operations such as the modulo operation will destroy the structure of the underlying MEC. Thus, we use the concept of the total order on the MEC to obtain an S-box. Order theory is intensively used in formal methods, programming languages, logic, and statistical analysis. Now a natural question is how to define different orderings on the MEC. Note that for each  $x$  value of the MEC, there are two  $y$  values. Thus, we can divide

the orderings on the MEC into two categories: (1) one in which the two  $y$  values of each  $x$  appear consecutively; (2) the other one containing those orderings in which the two  $y$  values of each  $x$  do not appear consecutively. Based on this, we define three different types of orderings on the given MEC  $E_{p \equiv 2, b}$  to generate three different S-boxes.

#### 3.1 Orderings on an MEC $E_{p \equiv 2, b}$

The orderings used in the proposed method are discussed below:

1. A natural ordering on an MEC

We define a natural ordering  $\prec_N$  on  $E_{p \equiv 2, b}$  based on the  $x$ -coordinate as follows:

$$(x_1, y_1) \prec_N (x_2, y_2) \Leftrightarrow \text{either } "x_1 < x_2" \text{ or } "x_1 = x_2 \text{ and } y_1 < y_2," \quad (1)$$

where  $(x_1, y_1)$  and  $(x_2, y_2) \in E_{p \equiv 2, b}$ .

The aim of this ordering is to sort the points on the MEC in such a way that the  $x$ -coordinate is in non-decreasing order and the two  $y$  values corresponding to each  $x$  value appear consecutively.

The next two orderings are introduced based on the following observation deduced from Theorem 1 to diffuse the  $y$ -coordinate on an MEC:

**Observation 1** For any two distinct points  $(x_1, y_1)$  and  $(x_2, y_2)$  on the MEC  $E_{p \equiv 2, b}$  such that either  $x_1 + y_1 = x_2 + y_2$  or  $x_1 + y_1 \equiv x_2 + y_2 \pmod{p}$ ,  $x_1 \neq x_2$  holds.

2. A diffusion ordering on an MEC

An ordering is defined on  $E_{p \equiv 2, b}$  to diffuse the two  $y$  values of each  $x$  value. Let  $(x_1, y_1)$  and  $(x_2, y_2)$  be any two points on  $E_{p \equiv 2, b}$ . The diffusion ordering  $\prec_D$  is defined to be

$$(x_1, y_1) \prec_D (x_2, y_2) \Leftrightarrow \text{either } "x_1 + y_1 < x_2 + y_2" \text{ or } "x_1 + y_1 = x_2 + y_2 \text{ and } x_1 < x_2." \quad (2)$$

**Lemma 1** For any MEC  $E_{p \equiv 2, b}$ , the relation  $\prec_D$  is a total order.

**Proof** For each  $(x_1, y_1) \in E_{p \equiv 2, b}$ , we have  $x_1 + y_1 = x_1 + y_1$ , and therefore  $(x_1, y_1) \prec_D (x_1, y_1)$ . This implies that  $\prec_D$  is reflexive. Next, we need to prove that  $\prec_D$  has the antisymmetric property. For  $(x_1, y_1)$  and  $(x_2, y_2) \in E_{p \equiv 2, b}$ , suppose that  $(x_1, y_1) \prec_D (x_2, y_2)$  and  $(x_2, y_2) \prec_D (x_1, y_1)$ .

$\prec_D(x_1, y_1)$  hold. This implies that  $x_1+y_1=x_2+y_2$ . This is because  $x_1+y_1 < x_2+y_2$  and  $x_2+y_2 < x_1+y_1$  are the only cases for which the assumption and  $x_1+y_1 \neq x_2+y_2$  hold, implying that  $x_1+y_1=x_2+y_2$ . Now if  $x_1 \neq x_2$ , by the assumption and the fact that  $x_1+y_1=x_2+y_2$ , we have  $x_1 < x_2$  and  $x_2 < x_1$ , leading to  $x_1=x_2$ , which is a contradiction. Thus,  $x_1+y_1=x_2+y_2$  and  $x_1=x_2$  hold, ultimately implying that  $y_1=y_2$ . Therefore,  $(x_1, y_1)=(x_2, y_2)$ . Now to prove the transitive property, suppose that  $(x_1, y_1) \prec_D(x_2, y_2)$  and  $(x_2, y_2) \prec_D(x_3, y_3)$  hold, where  $(x_1, y_1), (x_2, y_2)$ , and  $(x_2, y_2), (x_3, y_3) \in E_{p=2,b}$ . Now if  $x_1+y_1 < x_2+y_2$  and  $x_2+y_2 \leq x_3+y_3$ , or  $x_1+y_1=x_2+y_2$  and  $x_2+y_2 < x_3+y_3$ , then  $x_1+y_1 < x_3+y_3$ . Therefore,  $(x_1, y_1) \prec_D(x_3, y_3)$ . Similarly, if  $x_1+y_1=x_2+y_2=x_3+y_3$ , then  $x_1 < x_2$  and  $x_2 < x_3$ . Hence,  $x_1+y_1=x_3+y_3$  and  $x_1 < x_3$ . This completes the proof.

3. A modulo diffusion ordering on an MEC

The order  $\prec_M$  defined below produces diffusion in both  $x$ - and  $y$ -coordinate of the points on  $E_{p=2,b}$ . Let  $(x_1, y_1)$  and  $(x_2, y_2) \in E_{p=2,b}$ . Then we have

$$\begin{aligned} (x_1, y_1) \prec_M (x_2, y_2) &\Leftrightarrow \\ \text{either } "x_1+y_1 < x_2+y_2 \pmod{p}" & \quad (3) \\ \text{or } "x_1+y_1 = x_2+y_2 \pmod{p} \text{ and } x_1 < x_2." & \end{aligned}$$

**Lemma 2** For any MEC  $E_{p=2,b}$ , the relation  $\prec_M$  is a total order.

Lemma 2 can be proved using arguments similar to those used in the proof of Lemma 1.

The effect of these orderings  $\prec_N, \prec_D$ , and  $\prec_M$  on the  $y$ -coordinate of the MEC  $E_{101=2,1}$  is shown in Fig. 1, by plotting them in non-decreasing order of their points on the MEC with respect to  $\prec_N, \prec_D$ , and  $\prec_M$ , respectively.

Similarly, a relationship among the sets of the  $y$ -coordinate of the MEC  $E_{p=2,b}$  obtained by different proposed orderings ( $\prec_H$  and  $\prec_K$ , where  $H$  and  $K \in \{N, D, M\}$ ) is quantified by computing their correlation coefficient  $\rho_{HK}$ . The correlation results of different MECs are shown in Table 1. Table 1 shows that each ordering has different effects on the  $y$ -coordinate of the underlying MEC.

3.2 The proposed S-box construction method

Let  $E_{p=2,b}$  be an MEC, where  $p \geq 257$ . The lower

bound on the prime  $p$  is 257 for the proposed method, so MEC has at least 256 points. An S-box  $S_{p,b}^H$ , where  $H \in \{N, D, M\}$ , is generated by selecting the  $y$ -coordinate on  $E_{p=2,b}$  which are in the interval  $[0, 255]$  using the function of  $S_{p,b}^H : \{0, 1, \dots, 255\} \rightarrow \{0, 1, \dots, 255\}$  defined as  $S_{p,b}^H(i) = y_i$  such that  $(x_i, y_i) \in E_{p=2,b}$  and  $(x_{i-1}, y_{i-1}) \prec_H(x_i, y_i)$ .

Table 1 Results of the correlation tests

$p$	$b$	$\rho_{ND}$	$\rho_{DM}$	$\rho_{MN}$
101	1	-0.0588	0.0550	-0.0497
827	87	-0.0044	0.0008	0.0027
1013	118	0.0028	-0.0059	0.0003
2027	8	0.0007	-0.0068	-0.0002

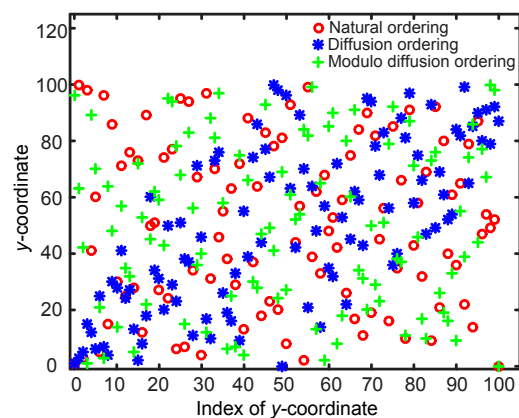


Fig. 1 Arrangements of the  $y$ -coordinate of  $E_{101=2,1}$  with respect to the proposed orderings

It is clear from Theorem 1 that  $S_{p,b}^H$  is a bijection, which further implies that the proposed method generates an S-box for each set of input parameters.

**Lemma 3** For any prime  $p \geq 257$  such that  $p \equiv 2 \pmod{3}$  with an integer  $b \in [0, p-1]$  and  $H \in \{N, D, M\}$ , the S-box  $S_{p,b}^H$  can be generated in time  $O(p)$  and constant space.

**Proof** The generation of  $S_{p,b}^H$  requires calculating and sorting 256 points on the MEC with the  $y$ -coordinate in  $[0, 255]$ . The calculation of 256 points on the MEC can be done in  $O(p)$ , since for each  $y \in [0, 255]$ , a for-loop of size  $p$  suffices to find an integer  $x$  such that  $(x, y)$  is a point on the MEC. However, the sorting of these 256 points can be done in constant time with respect to the ordering  $H$ . Thus,  $S_{p,b}^H$  can be

generated in  $O(p)$ . Furthermore, the generation process stores only 256 points on the MEC for the sorting purpose. Therefore, it takes constant space.

It is evident from Lemma 3 that the time and space complexities of the proposed S-box generation method over MEC  $E_{p,b}$  are independent of parameter  $b$  and the ordering on the underlying MEC. An algorithmic description of the proposed generation method is given in Algorithm 1.

**Algorithm 1** The proposed S-box generation method

**Input:** An MEC  $E_{p,b}$ , where  $p \equiv 2 \pmod{3}$ , with a total order  $H \in \{N, D, M\}$

**Output:** S-box  $S_{p,b}^H$

- 1:  $A := \emptyset$  /\* The set of 256 points of the MEC with the  $y$ -coordinate in  $[0, 255]$  \*/
- 2: **for** each  $y=0, 1, \dots, 255$  **do**
- 3:     **for** each  $x=0, 1, \dots, p-1$  **do**
- 4:         **if**  $x^3 + b = y^2 \pmod{p}$  **then**
- 5:              $A := A \cup \{(x, y)\}$
- 6:         **end if**
- 7:     **end for**
- 8: **end for**
- 9: Sort  $A$  with respect to the ordering  $H$
- 10: Output all  $y$ -coordinate of the points in  $A$  preserving their order as the S-box  $S_{p,b}^H$

The S-boxes  $S_{1667,351}^N$ ,  $S_{3299,1451}^D$ , and  $S_{4229,2422}^M$  generated by the proposed technique are presented in Tables A1–A3 (see Appendix).

### 4 Security analysis

Several standard tests are applied on the S-boxes obtained by the proposed method to test their cryptographic strength. A brief introduction to these security tests and their results for some of the newly generated S-boxes  $S_{1667,351}^N$ ,  $S_{1949,544}^N$ ,  $S_{3023,626}^N$ ,  $S_{3299,1451}^D$ ,  $S_{3041,1298}^D$ ,  $S_{3347,2937}^D$ ,  $S_{4229,2422}^M$ ,  $S_{4217,1156}^M$  and  $S_{3299,1400}^M$  are discussed in this section.

#### 4.1 Non-linearity (NL)

It is important for an S-box to create confusion in the data up to a certain level to keep the data secure from an adversary. The confusion creation capability

of an S-box  $S$  over the Galois field  $GF(2^8)$  is measured by its non-linearity  $N(S)$ , which is defined as

$$N(S) = \min_{\alpha, \beta, \gamma} \{x \in GF(2^8) : \alpha \cdot S(x) \neq \beta \cdot x \oplus \gamma\},$$

where  $\alpha \in GF(2^8)$ ,  $\beta \in GF(2^8) \setminus \{0\}$ ,  $\gamma \in GF(2)$ , and “ $\cdot$ ” represents the dot product over  $GF(2)$ .

An S-box with high non-linearity (NL) is capable of generating high confusion in the data. However, it was shown in Meier and Staffelbach (1990) that an S-box with high NL may not have other cryptographic properties. The NL of some of the newly constructed S-boxes is listed in Table 2. Note that each listed S-box has an NL of 106, which is large enough to create high confusion.

**Table 2 Non-linearity (NL) of the newly generated S-boxes**

S-box	NL	S-box	NL
$S_{1667,351}^N$	106	$S_{3347,2937}^D$	106
$S_{1949,544}^N$	106	$S_{4229,2422}^M$	106
$S_{3023,626}^N$	106	$S_{4217,1156}^M$	106
$S_{3299,1451}^D$	106	$S_{3299,1400}^M$	106
$S_{3041,1298}^D$	106		

#### 4.2 Approximation attacks

A cryptographically strong S-box must have high resistance against approximation attacks. Approximation attacks can be divided into two categories, namely, linear approximation attacks and differential approximation attacks, which are explained below.

##### 4.2.1 Linear approximation probability (LAP)

The resistance of an S-box  $S$  against linear approximation attacks is measured by calculating its maximum number  $L(S)$  of coincident input bits with the output bits. The mathematical expression of  $L(S)$  is as follows:

$$L(S) = \frac{1}{2^8} \left\{ \max_{\alpha, \beta} \left\{ \text{abs} \left( \left| \left\{ x \in GF(2^8) \mid \alpha \cdot x = \beta \cdot S(x) \right\} \right| - 2^7 \right) \right\} \right\}.$$

An S-box  $S$  is highly resistive against linear approximation attacks if it has a low value of  $L(S)$ . The

LAP of the newly generated S-boxes is listed in Table 3. The average LAP of all of the listed S-boxes is 0.1371, which is very low. Hence, the proposed scheme is capable of generating S-boxes with high resistance against linear approximation attacks.

4.2.2 Differential approximation probability (DAP)

The strength of an S-box against differential approximation attacks is measured by calculating its DAP. For an S-box  $S$ , the DAP  $D(S)$  is the maximum probability of a specific change  $\Delta y$  in the output bits  $S(x)$  when the input bits  $x$  are changed to  $x \oplus \Delta x$ , i.e.,

$$D(S) = \frac{1}{2^8} \left\{ \max_{\Delta x, \Delta y} \left\{ \left| \left\{ x \in \text{GF}(2^8) \mid S(x \oplus \Delta x) = S(x) \oplus \Delta y \right\} \right| \right\} \right\}$$

where  $\Delta x$  and  $\Delta y \in \text{GF}(2^8)$ , and  $\oplus$  denotes the bit-wise addition over  $\text{GF}(2)$ .

The smaller the value of DAP, the higher the security of the S-box against differential approximation attacks. The experimental results of DAP on the newly generated S-boxes are presented in Table 4. Table 4 shows that the newly generated S-boxes have high resistance against differential attacks.

**Table 3 Linear approximation probability (LAP) of the newly generated S-boxes**

S-box	LAP	S-box	LAP
$S_{1667,351}^N$	0.1328	$S_{3347,2937}^D$	0.1406
$S_{1949,544}^N$	0.1328	$S_{4229,2422}^M$	0.1328
$S_{3023,626}^N$	0.1406	$S_{4217,1156}^M$	0.1328
$S_{3299,1451}^D$	0.1484	$S_{3299,1400}^M$	0.1406
$S_{3041,1298}^D$	0.1328		

**Table 4 Differential approximation probability (DAP) of the newly generated S-boxes**

S-box	DAP	S-box	DAP
$S_{1667,351}^N$	0.0391	$S_{3347,2937}^D$	0.0391
$S_{1949,544}^N$	0.0391	$S_{4229,2422}^M$	0.0391
$S_{3023,626}^N$	0.0391	$S_{4217,1156}^M$	0.0391
$S_{3299,1451}^D$	0.0391	$S_{3299,1400}^M$	0.0391
$S_{3041,1298}^D$	0.0391		

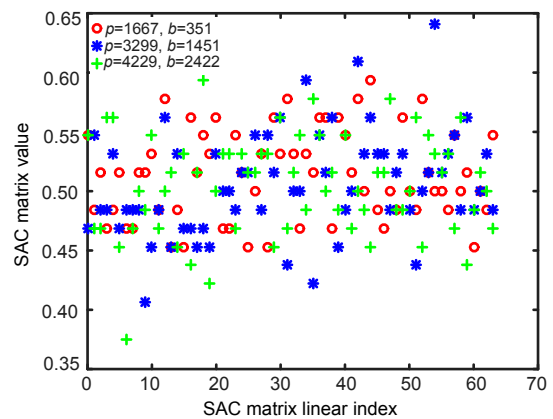
4.3 Strict avalanche criterion (SAC)

The diffusion creation capability of an S-box is calculated by the SAC. The SAC of an S-box  $S$  is the measure of change in output bits when a single input bit is changed. The SAC of an S-box  $S$  with Boolean functions  $S_i$  ( $1 \leq i \leq 8$ ) is computed by calculating an eight-dimensional square matrix  $M(S)=[m_{ij}]$  using each of the eight elements  $\alpha_j \in \text{GF}(2^8)$  with only one non-zero bit. The elements  $m_{ij}$  of  $M(S)$  are computed as follows:

$$m_{ij} = \frac{1}{2^8} \left( \sum_{x \in \text{GF}(2^8)} \omega(S_i(x \oplus \alpha_j) \oplus S_i(x)) \right)$$

where  $\omega(\mathbf{v})$  denotes the number of non-zero bits in vector  $\mathbf{v}$ .

The SAC test is fulfilled if all entries of  $M(S)$  are close to 0.5. The entries of the SAC matrix corresponding to each newly generated S-boxes ( $S_{1667,351}^N$ ,  $S_{3299,1451}^D$ , and  $S_{4229,2422}^M$ ) are plotted in a linear order in Fig. 2. The averages of the minimum and maximum of  $M(S)$  corresponding to each of the newly generated S-boxes are 0.4115 and 0.6094, respectively. Table 5 shows that the S-boxes generated by the proposed method based on MECs are capable of generating high diffusion in the data.



**Fig. 2 Strict avalanche criterion (SAC) matrix plot for  $S_{1667,351}^N$ ,  $S_{3299,1451}^D$ , and  $S_{4229,2422}^M$**

4.4 Bit independence criterion (BIC)

The BIC is an important test to measure the diffusion creation strength of an S-box. The main idea is

to investigate the dependence of a pair of output bits when an input bit is inverted.

The BIC of an S-box  $S$  over  $GF(2^8)$  with  $S_i$  Boolean functions is calculated by computing an eight-dimensional square matrix  $N(S)=[n_{ij}]$ , expressed as

$$n_{ij} = \frac{1}{2^8} \left( \sum_{\substack{x \in GF(2^8) \\ 1 \leq k \leq 8}} \omega(S_i(x \oplus \alpha_j) \oplus S_i(x) \oplus S_k(x + \alpha_j) \oplus S_k(x)) \right)$$

Of course  $n_{ii}=0$ . An S-box is good if all off-diagonal values of its BIC matrix are close to 0.5. The experimental results of this test on the newly generated S-boxes  $S_{1667,351}^N$ ,  $S_{3299,1451}^D$ , and  $S_{4229,2422}^M$  excluding the value of 0 are shown in a linear order in Fig. 3. The minimum and maximum of the BIC matrix  $N(S)$  of each of the newly generated S-boxes are listed in Table 6. Fig. 3 and Table 6 show that the S-boxes generated by the proposed methods are strong enough to generate high diffusion in the data.

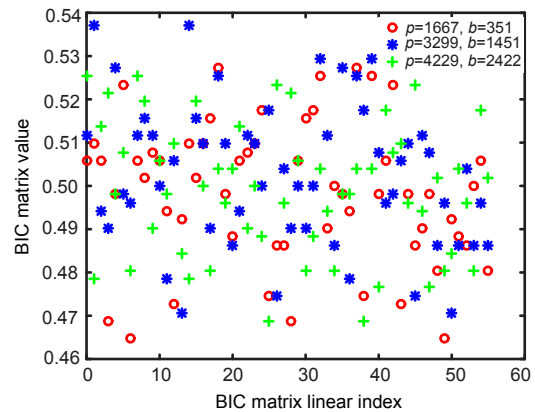
**Table 5** Strict avalanche criterion (SAC) of the newly generated S-boxes

S-box	SAC	
	Maximum	Minimum
$S_{1667,351}^N$	0.5938	0.4531
$S_{1949,544}^N$	0.6250	0.4219
$S_{3023,626}^N$	0.6563	0.4219
$S_{3299,1451}^D$	0.6406	0.4063
$S_{3041,1298}^D$	0.6094	0.4219
$S_{3347,2937}^D$	0.6094	0.4063
$S_{4229,2422}^M$	0.5938	0.3750
$S_{4217,1156}^M$	0.6094	0.3906
$S_{3299,1400}^M$	0.6250	0.3594

### 4.5 Algebraic complexity (AC)

The resistance of an S-box against algebraic attacks is measured by computing its linear polynomial. The AC of an S-box is the number of non-zero terms in its linear polynomial. The greater the AC, the more secure the S-box against algebraic attacks. The AC of the newly generated S-boxes is computed (Table 7).

The minimum and maximum of the AC of the newly generated S-boxes are 253 and 255, respectively, which are very close to the optimal value of 255. Thus, the proposed method can generate S-boxes with a good AC.



**Fig. 3** Bit independence criterion (BIC) matrix plot for  $S_{1667,351}^N$ ,  $S_{3299,1451}^D$ , and  $S_{4229,2422}^M$

**Table 6** Bit independence criterion (BIC) of the newly generated S-boxes

S-box	BIC	
	Maximum	Minimum
$S_{1667,351}^N$	0.5273	0.4648
$S_{1949,544}^N$	0.5293	0.4629
$S_{3023,626}^N$	0.5313	0.4707
$S_{3299,1451}^D$	0.5371	0.4707
$S_{3041,1298}^D$	0.5273	0.4844
$S_{3347,2937}^D$	0.5254	0.4746
$S_{4229,2422}^M$	0.5254	0.4688
$S_{4217,1156}^M$	0.5313	0.4766
$S_{3299,1400}^M$	0.5449	0.4727

**Table 7** Algebraic complexity (AC) of the newly generated S-boxes

S-box	AC	S-box	AC
$S_{1667,351}^N$	254	$S_{3347,2937}^D$	255
$S_{1949,544}^N$	254	$S_{4229,2422}^M$	253
$S_{3023,626}^N$	255	$S_{4217,1156}^M$	253
$S_{3299,1451}^D$	255	$S_{3299,1400}^M$	255
$S_{3041,1298}^D$	254		



## 5 Comparison and discussion

A detailed comparison of the proposed S-box construction method is described in this section.

### 5.1 Time and space complexities

It is always desirable to have algorithms with low time and space complexities from an implementation point of view. The time and space complexities of the proposed method and other S-box generation methods (Hayat et al., 2018; Hayat and Azam, 2019) based on ECs are compared (Table 8). Note that each method in Hayat et al. (2018) and Hayat and Azam (2019) has quadratic time complexity, while the proposed method takes linear time in the underlying prime  $p$  for the generation of an S-box. However, the space complexity of the methods in Hayat et al. (2018) and Hayat and Azam (2019) is  $O(p)$ , where  $p$  is the underlying prime, while it is constant for the proposed method. Hence, the newly developed method is more suitable for implementation when compared with all existing S-box generation methods over ECs.

**Table 8 Comparison of the time and space complexities between the proposed method and other methods over ECs**

S-box	Time complexity	Space complexity
Hayat et al. (2018)'s	$O(p^2)$	$O(p)$
Hayat and Azam (2019)'s	$O(p^2)$	$O(p)$
Ours	$O(p)$	$O(1)$

### 5.2 Generation efficiency

For a good dynamic S-box construction scheme, it is necessary to ensure the generation of S-boxes for each valid input parameter, and construct a sufficient number of distinct S-boxes. It is evident from Theorem 1 that the proposed method always generates an S-box for each input, while the outputs of the methods in Hayat et al. (2018) and Hayat and Azam (2019) are uncertain; i.e., they do not guarantee the construction of S-boxes for each input. This implies that the proposed method is better than existing methods over ECs.

The proposed method can generate at most  $(p-1)$  distinct S-boxes for a given prime  $p$  and an ordering,

since for each  $b \in [1, p-1]$  it can generate exactly one S-box. We generate all S-boxes by the proposed method for different primes ( $p=257, 263, 269, 281, 293, 1013, 1019, 1031, 1049, 1061, \text{ and } 1997$ ) and each ordering developed in this study. The number of distinct S-boxes for each ordering is the same for all the primes (Table 9). Table 9 shows that the number of distinct S-boxes generated by the proposed S-box design scheme attains the optimal value and increases with the increase of the size of the prime. Hence, one can generate the desired number of distinct S-boxes using the proposed method.

**Table 9 Number of distinct S-boxes constructed by the proposed scheme for some primes**

$p$	Number of distinct S-boxes	$p$	Number of distinct S-boxes
257	256	1019	1018
263	262	1031	1030
269	268	1049	1048
281	280	1061	1060
293	292	1997	1996
1013	1012		

### 5.3 Cryptographic properties

The cryptographic properties of some of the S-boxes constructed by the proposed method are compared with those of some of the well-known existing S-boxes in Daemen and Rijmen (2002), Tang et al. (2005), Chen et al. (2007), Chen (2008), Kim and Phan (2009), Wang et al. (2010), Gautam et al. (2015), and Hayat et al. (2018) generated by different mathematical structures. Properties of the S-boxes used in this comparison are listed in Table 10. Note that the NL of the S-boxes ( $S_{1667,351}^N, S_{3299,1451}^D, \text{ and } S_{4229,2422}^M$ ) is greater than that of the S-boxes in Tang et al. (2005), Chen et al. (2007), Chen (2008), Kim and Phan (2009), Gautam et al. (2015), and Hayat et al. (2018). Hence, the newly generated S-boxes create better confusion in the data compared with the S-boxes in those works. This implies that the proposed technique is capable of generating S-boxes with better NL compared with some of the existing techniques. Moreover, the LAP of the newly generated S-boxes is smaller than or equal to that of the S-boxes in Tang et al. (2005), Chen et al. (2007), Chen (2008), Wang et al. (2010), and Gautam et al.



(2015), while the DAP of the newly generated S-boxes is smaller than or equal to that of the S-boxes in Tang et al. (2005), Chen et al. (2007), Chen (2008), Kim and Phan (2009), Wang et al. (2010), Gautam et al. (2015), and Hayat et al. (2018). Thus, the S-boxes generated by the proposed technique have the same or better security against approximation attacks compared with other S-boxes. Similarly, the SAC, BIC, and AC test results of the newly generated S-boxes are comparable to their counterparts of the S-boxes listed in Table 10. Hence, the proposed S-box generation technique based on an MEC is capable of generating S-boxes with cryptographic properties comparable to those of some of the existing S-box construction techniques based on different mathematical structures.

## 6 Conclusions

In this study, we have presented an S-box design method based on the  $y$ -coordinate of a finite Mordell elliptic curve (MEC), where the underlying prime is congruent to 2 (mod 3). The technique uses some special types of total orders on the points on the MEC, and generates an S-box. The main advantage of the proposed method is that it has linear time complexity and constant space complexity and generates an S-box for each set of input parameters, which is impossible in any existing S-box generation scheme over elliptic curves. Several standard security tests

were performed on the S-boxes generated by the proposed method to analyze its cryptographic efficiency. Experimental results showed that the proposed method can generate cryptographically strong S-boxes. Furthermore, computational results showed that the cryptographic properties of the newly generated S-boxes are comparable to those of some of the well-known existing S-boxes generated by different mathematical structures.

## Compliance with ethics guidelines

Naveed Ahmed AZAM, Umar HAYAT, and Ikram ULLAH declare that they have no conflict of interest.

## References

- Agarwal P, Singh A, Kilicman A, 2018. Development of key-dependent dynamic S-boxes with dynamic irreducible polynomial and affine constant. *Adv Mech Eng*, 10(7): 1-18. <https://doi.org/10.1177/1687814018781638>
- Azam NA, 2017. A novel fuzzy encryption technique based on multiple right translated AES gray S-boxes and phase embedding. *Secur Commun Netw*, 2017:1-9. <https://doi.org/10.1155/2017/5790189>
- Chen G, 2008. A novel heuristic method for obtaining S-boxes. *Chaos Sol Fract*, 36(4):1028-1036. <https://doi.org/10.1016/j.chaos.2006.08.003>
- Chen G, Chen Y, Liao XF, 2007. An extended method for obtaining S-boxes based on three-dimensional chaotic baker maps. *Chaos Sol Fract*, 31(3):571-579. <https://doi.org/10.1016/j.chaos.2005.10.022>
- Cheon JH, Chee S, Park C, 1999. S-boxes with controllable nonlinearity. *Proc 17<sup>th</sup> Int Conf on Theory and Application of Cryptographic Techniques*, p.286-294. [https://doi.org/10.1007/3-540-48910-X\\_20](https://doi.org/10.1007/3-540-48910-X_20)

**Table 10 Comparison of the newly generated S-boxes with some of the existing S-boxes**

S-box	NL	LAP	DAP	SAC		BIC		AC
				Maximum	Minimum	Maximum	Minimum	
Daemen and Rijmen (2002)'s	112	0.0620	0.0156	0.5620	0.4530	0.5040	0.4800	9
Tang et al. (2005)'s	103	0.1328	0.0391	0.5703	0.3984	0.5352	0.4727	255
Chen et al. (2007)'s	100	0.1328	0.0547	0.6094	0.4219	0.5313	0.4746	255
Chen (2008)'s	102	0.1484	0.0391	0.6094	0.3750	0.5215	0.4707	254
Kim and Phan (2009)'s	104	0.1090	0.0469	0.5930	0.3900	0.4990	0.4540	255
Wang et al. (2010)'s	106	0.1406	0.0391	0.5938	0.4375	0.5313	0.4648	251
Gautam et al. (2015)'s	74	0.2109	0.0547	0.6875	0.1094	0.5508	0.4023	253
Hayat et al. (2018)'s	104	0.0391	0.0391	0.6250	0.3906	0.5313	0.4707	255
$S_{1667,351}^N$	106	0.1328	0.0391	0.5938	0.4531	0.5273	0.4648	254
$S_{3299,1451}^D$	106	0.1484	0.0391	0.6406	0.4063	0.5371	0.4707	255
$S_{4229,2422}^M$	106	0.1328	0.0391	0.5938	0.3750	0.5254	0.4688	253

NL: non-linearity; LAP: linear approximation probability; DAP: differential approximation probability; SAC: strict avalanche criterion; BIC: bit independence criterion; AC: algebraic complexity

- Courtois NT, Pieprzyk J, 2002. Cryptanalysis of block ciphers with overdefined systems of equations. Proc 8<sup>th</sup> Int Conf on Theory and Application of Cryptology and Information Security, p.267-287.  
[https://doi.org/10.1007/3-540-36178-2\\_17](https://doi.org/10.1007/3-540-36178-2_17)
- Cui LG, Cao YD, 2007. A new S-box structure named affine-power-affine. *Int J Innov Comput Inform Contr*, 3(3): 751-759.
- Daemen J, Rijmen V, 2002. The Design of Rijndael-AES: the Advanced Encryption Standard. Springer, Berlin, Germany.
- Devaraj P, Kavitha C, 2016. An image encryption scheme using dynamic S-boxes. *Nonl Dynam*, 86(2):927-940.  
<https://doi.org/10.1007/s11071-016-2934-7>
- Gautam A, Gaba GS, Miglani R, et al., 2015. Application of chaotic functions for construction of strong substitution boxes. *Ind J Sci Technol*, 8(28):1-5.  
<https://doi.org/10.17485/ijst/2015/v8i28/71759>
- Hayat U, Azam NA, 2019. A novel image encryption scheme based on an elliptic curve. *Signal Process*, 155:391-402.  
<https://doi.org/10.1016/j.sigpro.2018.10.011>
- Hayat U, Azam NA, Asif M, 2018. A method of generating 8×8 substitution boxes based on elliptic curves. *Wirel Pers Commun*, 101(1):439-451.  
<https://doi.org/10.1007/s11277-018-5698-1>
- Hussain I, Azam NA, Shah T, 2014. Stego optical encryption based on chaotic S-box transformation. *Opt Laser Technol*, 61:50-56.  
<https://doi.org/10.1016/j.optlastec.2014.01.018>
- Jakobsen T, Knudsen LR, 1997. The interpolation attack on block ciphers. Proc 4<sup>th</sup> Int Workshop on Fast Software Encryption, p.28-40.  
<https://doi.org/10.1007/BFb0052332>
- Katiyar S, Jeyanthi N, 2016. Pure dynamic S-box construction. *Int J Comput*, 1:42-46.
- Kazlauskas K, Kazlauskas J, 2009. Key-dependent S-box generation in AES block cipher system. *Informatika*, 20(1):23-34.
- Khan M, Azam NA, 2015a. Right translated AES gray S-boxes. *Secur Commun Netw*, 8:1627-1635.  
<https://doi.org/10.1002/sec.1110>
- Khan M, Azam NA, 2015b. S-boxes based on affine mapping and orbit of power function. *3D Res*, 6(2), Article 43.  
<https://doi.org/10.1007/s13319-015-0043-x>
- Kim J, Phan RCW, 2009. Advanced differential-style cryptanalysis of the NSA's skipjack block cipher. *Cryptologia*, 33(3):246-270.  
<https://doi.org/10.1080/01611190802653228>
- Liu JM, Wai BD, Cheng XG, et al., 2005. An AES S-box to increase complexity and cryptographic analysis. Proc 19<sup>th</sup> Int Conf on Advanced Information Networking and Applications, p.724-728.  
<https://doi.org/10.1109/AINA.2005.84>
- Liu Y, Wang J, Fan JH, et al., 2016. Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences. *Multim Tools Appl*, 75(8):4363-4382.  
<https://doi.org/10.1007/s11042-015-2479-7>
- Manjula G, Mohan HS, 2013. Constructing key dependent dynamic S-box for AES block cipher system. Proc 2<sup>nd</sup> Int Conf on Applied and Theoretical Computing and Communication Technology, p.613-617.  
<https://doi.org/10.1109/ICATCCT.2016.7912073>
- Maram B, Gnanasekar JM, 2016. Evaluation of key dependent S-box based data security algorithm using Hamming distance and balanced output. *TEM J*, 5(1):67-75.  
<https://doi.org/10.18421/TEM51-11>
- Meier W, Staffelbach O, 1990. Nonlinearity criteria for cryptographic functions. Proc Advances in Cryptology—EUROCRYPT, p.549-562.  
[https://doi.org/10.1007/3-540-46885-4\\_53](https://doi.org/10.1007/3-540-46885-4_53)
- Miller VS, 1986. Use of elliptic curves in cryptography. Proc Advances in Cryptology—CRYPTO, p.417-426.  
[https://doi.org/10.1007/3-540-39799-X\\_31](https://doi.org/10.1007/3-540-39799-X_31)
- Murphy S, Robshaw MJB, 2002. Essential algebraic structure within the AES. Proc 22<sup>nd</sup> Annual Int Cryptology Conf, p.1-16. [https://doi.org/10.1007/3-540-45708-9\\_1](https://doi.org/10.1007/3-540-45708-9_1)
- Rahnama B, Kiran Y, Dara R, 2013. Countering AES static S-box attack. Proc 6<sup>th</sup> Int Conf on Security of Information and Networks, p.256-260.  
<https://doi.org/10.1145/2523514.2523544>
- Rosenthal J, 2003. A polynomial description of the Rijndael advanced encryption standard. *J Algebr Appl*, 2(2):223-236. <https://doi.org/10.1142/S0219498803000532>
- Shannon CE, 1949. Communication theory of secrecy systems. *Bell Syst Tech J*, 28(4):656-715.  
<https://doi.org/10.1002/j.1538-7305.1949.tb00928.x>
- Tang GP, Liao XF, Chen Y, 2005. A novel method for designing S-boxes based on chaotic maps. *Chaos Sol Fract*, 23(2):413-419.  
<https://doi.org/10.1016/j.chaos.2004.04.023>
- Tran MT, Bui DK, Duong AD, 2008. Gray S-box for advanced encryption standard. Proc Int Conf on Computational Intelligence and Security, p.253-258.  
<https://doi.org/10.1109/CIS.2008.205>
- Wang XY, Wang Q, 2014. A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. *Nonl Dynam*, 75(3):567-576.  
<https://doi.org/10.1007/s11071-013-1086-2>
- Wang Y, Yang L, Li M, et al., 2010. A method for designing S-box based on chaotic neural network. Proc 6<sup>th</sup> Int Conf on Natural Computation, p.1033-1037.  
<https://doi.org/10.1109/ICNC.2010.5582968>
- Washington LC, 2008. Elliptic Curves: Number Theory and Cryptography (2<sup>nd</sup> Ed.). Chapman & Hall/CRC, London, UK.
- Zaibi G, Kachouri A, Peyrard F, et al., 2009. On dynamic chaotic S-Box. Proc Global Information Infrastructure Symp, p.1-5. <https://doi.org/10.1109/GIIS.2009.5307035>

## Appendix: S-boxes generated by the proposed method

**Table A1 The S-box ( $S_{1667,351}^N$ ) generated by the proposed method based on natural ordering**

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

**Table A2 The S-box ( $S_{3299,1451}^D$ ) generated by the proposed method based on diffusion ordering**

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

**Table A3** The S-box ( $S_{4229,2422}^M$ ) generated by the proposed method based on modulo diffusion ordering

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