Efficient Construction of S-boxes Based on a Mordell Elliptic Curve
Over a Finite Field

Naveed Ahmed Azam∗, Umar Hayat, Ikram Ullah
Department of Applied Mathematics and Physics, Graduate School of
Informatics, Kyoto University, Japan
Email: *azam@amp.i.kyoto-u.ac.jp
∗Corresponding author

Abstract: Elliptic curve cryptography (ECC) is used in many security sys-
tems due to its small key size and high security as compared to the other cryp-
tosystems. In many well-known security systems substitution box (S-box) is the
only non-linear component. Recently, it is shown that the security of a cryp-
tosystem can be improved by using dynamic S-boxes instead of static S-boxes.
This fact necessitates the construction of new secure S-boxes. In this paper,
we propose an efficient method for the generation of S-boxes based on a class
of Mordell elliptic curves (MECs) over prime fields by defining different total
orders. The proposed technique is developed carefully so that it output an S-
box inheriting the properties of the underlying MEC for each input in constant
time. Furthermore, it is shown by the computational results that the proposed
method is capable of generating cryptographically strong S-boxes as compared
to some of the existing S-boxes.

Key words: Mordell elliptic curve, Finite field, Substitution box, Total
order, Computational complexity

1 Introduction

Cryptography deals with the techniques to secure the private data. In these
techniques, the data is transformed into an unreadable form by using some keys
so that the adversaries cannot extract any useful information. S-box is the only
non-linear component of many well-known cryptosystems including AES. It is
therefore the security of such cryptosystems solely depends on the cryptographic
properties of their S-box. Shannon [1], proved that a cryptosystem is secure if
it can create confusion and diffusion in the data up to a certain level. An S-box
is cryptographically strong enough to create desire confusion and diffusion if it
satisfies certain tests including the test of non-linearity, approximation, strict
avalanche, bit independence and algebraic complexity.

Nowadays, AES is considered to be the most secured and widely used cryp-
tosystem, and hence many cryptographers studied its S-box. The study in
[2] [3] [4] [5] reveals that the AES S-box is vulnerable against algebraic attacks
because of its sparse polynomial representation. It is also noticed that a cryp-
tosystem based on a single S-box is unable to generate desirable security if
the data is highly correlated [6] [7]. Furthermore, it is shown that the secu-
rity of a cryptosystems can be improved by using dynamic S-boxes instead of
static S-boxes [8]. 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, it is necessary that the resultant S-box: (a) inherits the properties of the underlying mathematical structure. This is an important requirement which leads to the efficient generation and better understanding of the cryptographic properties of the S-box; (b) satisfies the security tests; and (c) is generated in less time and space complexity. Of course, an S-box generation technique with high time complexity is not suitable for the cryptosystems using multiple, and dynamic S-boxes. Liu et al. [9] presented an improved AES S-box based on an algebraic method. Cui et al. [10] used an affine function to generate an S-box with 253 non-zero terms in its polynomial representation. Tran et al. [11] used composition of a Gray code instead of affine mapping with the AES S-box to generate an S-box with high algebraic complexity. Khan et al. [12, 13] proposed different methods for the generation of cryptographically strong S-boxes based on a generalization of Gray S-box, and affine functions. Azam [6] used the later S-boxes for the encryption of confidential images. Chaotic maps including Baker, logistic, and Chebyshev maps are used to generate new S-boxes in [14, 15, 16]. Similarly, elliptic curves (ECs) are also used in the field of cryptography for the development of highly secure cryptosystems. Miller [17] presented an EC based security system which has smaller key size and higher security as compared to RSA. Jung et al. [18] developed a link between the points on hyper-elliptic curves and non-linearity of an S-box. Hayat et al. [19] for the first time used EC over a prime field for the generation of S-box. In this scheme, an S-box is generated by using the x-coordinates of the points on the EC followed by the modulo operation 256. Although the technique is capable of generating cryptographically strong S-boxes, but the output is uncertain. That is, for each set of input parameters the algorithm does not necessarily output an S-box. Furthermore, the time complexity of this scheme is $O(p)$, where $p \geq 257$ is the prime in the underlying EC.

The purpose of this article is to develop such a novel and efficient S-box generation technique based on a finite Mordell elliptic curve (MEC) which generates secure S-box inheriting the properties of the underlying MEC for each set of input parameters. To achieve this, we defined some typical type of total orders on the points on the MEC, and then used $y$-coordinates instead of $x$-coordinates to obtain an S-box. The remaining paper is organized as follows: In Section 2, some basic definitions and results related to EC are discussed. The proposed algorithm is described in Section 3. Section 4 contains the security analysis, and a comparison of the proposed S-box design technique with some of the existing techniques. Finally conclusions are drawn in Section 5.

## 2 Preliminaries

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

\[ y^2 \equiv x^3 + ax + b \pmod{p}. \]

We call \(p, a,\) and \(b\) the parameters of the EC \(E_{p,a,b}\). An approximation for the total number of points \(#E_{p,a,b}\) on \(E_{p,a,b}\) can be obtained by using Hasse’s formula \([20]\)

\[ |#E_{p,a,b} - p - 1| \leq 2\sqrt{p}. \]

Mordell elliptic curve (MEC) is a special kind of elliptic curve with \(a = 0\). The significance of MEC \(E_{p,0,b}\) is that some of the MECs have exactly \(p+1\). The following Theorem is taken from \([21]\) gives the information about such MECs.

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

Henceforth, a MEC \(E_{p,0,b}\) where \(p \equiv 2\pmod{3}\) is simply denoted by \(E_{p\equiv 2,b}\).

## 3 Description of the Proposed S-box Designing Technique

In this section, we give an informal intuition of our proposed method. Our aim is to develop such an S-box generation technique based on MEC which outputs an S-box: (a) in constant time for each set of input parameters; (b) that inherits the properties of the underlying MEC; and (c) having high security against cryptanalysis. Note that the S-box design technique proposed by Hayat et al. \([19]\) does not satisfy condition (a) and (b). One of the possible way of designing such technique is to input that EC which contains all values from 0 to 255 without repetition. It is, therefore, the proposed algorithm takes an MEC \(E_{p\equiv 2,b}\) as input, and uses \(y\)-coordinates to generate an S-box instead of \(x\)-coordinates. Now the next task is to use these \(y\)-coordinates in such a way that the resultant S-box inherits the properties of the underlying MEC. Of course, the usage of some arithmetic operations such as modulo operation on the \(y\)-coordinates to get an S-box will destroy the structure of the underlying MEC. It is therefore, we used the concept of total order on the MEC to get an S-box. Order theory is intensively used in formal methods, programming languages, logic, and statistic analysis. Now the natural question is how to define different orderings on the MEC. Note that for each \(x\) value of MEC, there are two \(y\) values. Thus, we can divide the orderings on MEC into two categories: (1) one is that in which the two \(y\) values of each \(x\) appear consecutively; and (2) the other one contains those orderings in which the two \(y\) values of each \(x\) do not appear consecutively. Based on this fact, we defined three different type of orderings on the MEC to generate three different S-boxes for a given MCE \(E_{p\equiv 2,b}\).
3.1 The proposed orderings on a MEC $E_{p^{2,b}}$

The orderings used in the proposed method are discussed below.

(1) A natural ordering on MEC: We define a natural ordering $\prec_N$ on $E_{p^{2,b}}$ based on $x$-coordinates as follows

$$
(x_1, y_1) \prec_N (x_2, y_2) \iff \begin{cases} 
  \text{either if } x_1 < x_2; \text{ or} \\
  \text{if } x_1 = x_2, \text{ and } y_1 < y_2,
\end{cases}
$$

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

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

The next two orderings are introduced based on the following observation deduced from Theorem [1] to diffuse the $y$-coordinates on a MEC.

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

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

$$
(x_1, y_1) \prec_D (x_2, y_2) \iff \begin{cases} 
  \text{either if } x_1 + y_1 < x_2 + y_2; \text{ or} \\
  \text{if } x_1 + y_1 = x_2 + y_2, \text{ and } x_1 < x_2.
\end{cases}
$$

**Lemma 2** The relation $\prec_D$ is a total order on the MEC $E_{p^{2,b}}$.

**Proof.** For each $(x_1, y_1) \in E_{p^{2,b}}$, we have $x_1 + y_1 = x_1 + 1$ and therefore $(x_1, y_1) \prec_D (x_1, 1)$. This implies that $\prec_D$ is reflexive. Next, we need to show that $\prec_D$ satisfies the antisymmetric property. Thus, for $(x_1, y_1), (x_2, y_2) \in E_{p^{2,b}}$, suppose that $(x_1, y_1) \prec_D (x_2, y_2)$, and $(x_2, y_2) \prec_D (x_1, y_1)$ hold. This implies that $x_1 + y_1 = x_2 + y_2$. This is because of the fact that $x_1 + y_1 < x_2 + y_2$, and $x_2 + y_2 < x_1 + y_1$ are the only cases for which the supposition and $x_1 + y_1 \neq x_2 + y_2$ are true, which eventually imply that $x_1 + y_1 = x_2 + y_2$. Now if $x_1 \neq x_2$, then by the supposition and the fact $x_1 + y_1 = x_2 + y_2$, we have $x_1 < x_2$ and $x_2 < x_1$, which lead to the contradiction $x_1 = x_2$. Thus $x_1 + y_1 = x_2 + y_2$ and $x_1 = x_2$ hold, which ultimately imply that $y_1 = y_2$, and therefore $(x_1, y_1) = (x_2, y_2)$. Now, to prove the transitivity 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 $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in E_{p^{2,b}}$. Now if $x_1 + y_1 < x_2 + y_2$ and $x_2 + y_2 < x_3 + y_3$, or $x_1 + y_1 = x_2 + y_2$ and $x_2 + y_2 < x_3 + y_3$, then $x_1 + y_1 < x_3 + y_3$, and 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 $x_2 < x_3$, and hence $x_1 + y_1 = x_3 + y_3$ and $x_1 < x_3$. This completes the proof. ■

(3) A modulo diffusion ordering on MEC: The order $\prec_M$ defined below produces diffusion in both $x$-coordinates and $y$-coordinates of the points
on $E_{p=2,b}$. Let $(x_1, y_1), (x_2, y_2) \in E_{p=2,b}$, then

$$(x_1, y_1) \prec_M (x_2, y_2) \iff \begin{cases} 
\text{either if } (x_1 + y_1 < x_2 + y_2)(\mod p); \text{ or} \\
\text{if } x_1 + y_1 \equiv x_2 + y_2(\mod p), \text{ and} \\
x_1 < x_2.
\end{cases} \quad (3)$$

**Lemma 3** The relation $\prec_M$ is a total order on the MEC $E_{p=2,b}$.

Lemma 3 can be proved by using the similar arguments as used in the proof of Lemma 2. The effect of these orderings $\prec_N, \prec_D$ and $\prec_M$ on $y$-coordinates of MEC $E_{101\equiv 2,1}$ is shown in Figure 1 by plotting them in a non-decreasing order of their points on MEC w.r.t. $\prec_N, \prec_D$ and $\prec_M$, respectively. Similarly, a relation among the sets of all $y$-coordinates of MEC $E_{p=2,b}$ obtained by different proposed orderings $\prec_H$ and $\prec_K$ where $H, K \in \{N, D, M\}$ is quantified by computing their correlation coefficient $\rho_{HK}$. The correlation results for different MECs are shown in Table 1. It is evident from the results that each ordering has different effect on the $y$-coordinates of the underlying MEC.

### 3.2 The proposed construction technique

Let $E_{p=2,b}$ be a Mordell elliptic curve (MEC), where $p \geq 257$. The lower bound on the prime $p$ is 257 for the proposed method so that MEC has at least 256
Table 1: Results of the correlation test

| p   | b | $\rho_{ND}$ | $\rho_{ND}$ | $\rho_{DM}$ |
|-----|---|-------------|-------------|-------------|
| 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     |

Table 2: The S-box $S_{1667,351}^{H}$ generated by the proposed method based on the natural ordering

| 154 | 217 | 227 | 110 | 85 | 9 | 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  |190 | 200 | 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 | 7  | 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 |

points. An S-box $S_{p,b}^{H}$, where $H \in \{N, D, M\}$ is generated by selecting the $y$-coordinates on $E_{p \equiv 2, b}$ which are in the interval $[0, 255]$ as $S_{p,b}^{H}: \{0, 1, \ldots, 255\} \rightarrow \{0, 1, \ldots, 255\}$ defined as $S_{p,b}^{H}(i) = y_i$, such that $(x_i, y_i) \in E_{p \equiv 2, b}$, and $(x_{i-1}, y_{i-1}) \prec_{H} (x_i, y_i)$.

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

**Proof.** The generation of $S_{p,b}^{H}$ requires calculation of 256 points on the MEC with $y$-coordinates in $[0, 255]$, and then their sorting. Of course this can be done in constant time, and space complexity.

The S-boxes $S_{1667,351}^{H}$, $S_{3299,1451}^{H}$, and $S_{4229,2422}^{H}$ generated by the proposed technique are presented in Tables (2)-(4), respectively.

### 4 Security Analysis and Comparison

Several standard tests are applied on the S-boxes obtained by the proposed method to test their cryptographic strength. A brief introduction to these se-
Table 3: The S-box $S_{3299,1451}^D$ generated by the proposed method based on the diffusion ordering

|     | 33 | 151 | 65 | 207 | 12 | 103 | 96 | 123 | 190 | 126 | 82 | 155 | 21 | 1 | 229 | 186 |
|-----|----|-----|----|-----|----|-----|----|-----|-----|-----|----|-----|----|---|----|-----|
| 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 | 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 | 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 4: The S-box $S_{4229,2422}^M$ generated by using the proposed method based on the modulo diffusion ordering

|     | 15 | 13 | 247 | 249 | 167 | 183 | 179 | 173 | 101 | 204 | 165 | 210 | 214 | 205 | 199 | 19 |
|-----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|----|----|----|---|
| 164 | 38 | 85 | 72  | 98  | 90  | 113 | 12  | 229 | 217 | 165 | 228 | 125 | 195 | 26 | 216 |
| 207 | 30 | 182 | 219 | 14  | 215 | 232 | 135 | 241 | 145 | 17  | 244 | 223 | 114 | 29 | 70 |
| 104 | 81 | 71  | 99  | 101 | 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 |
Table 5: Non-linearity of the newly generated S-boxes

| S-boxes          | $S^N_{1667,351}$ | $S^N_{1394,544}$ | $S^D_{3023,626}$ | $S^D_{599,1451}$ | $S^D_{599,1298}$ | $S^D_{3347,2937}$ | $S^M_{3299,2422}$ | $S^M_{4217,1156}$ | $S^M_{5299,1400}$ |
|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| NL               | 106              | 106              | 106              | 106              | 106              | 106              | 106              | 106              | 106              |

Security tests, and their results for some of the newly generated S-boxes $S^N_{1667,351}$, $S^N_{1394,544}$, $S^D_{3023,626}$, $S^D_{599,1451}$, $S^D_{599,1298}$, $S^D_{3347,2937}$, $S^M_{3299,2422}$, $S^M_{4217,1156}$ and $S^M_{5299,1400}$ 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 the adversaries. The confusion creation capability of an S-box $S$ over the Galois Field $GF(2^8)$ is measured by its non-linearity $\mathcal{N}(S)$, which is defined below

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

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

An S-box with high NL is capable of generating high confusion in the data. However, it is also shown in [22] that an S-box with high NL may not satisfy other cryptographic properties. The NL of some of the newly constructed S-boxes is listed in Table 5. Note that each listed S-box has NL 106, which is large enough to create high confusion.

4.2 Approximation Attacks

A cryptographically strong S-box must have high resistance against approximation attacks. The 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 $\mathcal{L}(S)$ of coincident input bits with the output bits. The mathematical expression of $\mathcal{L}(S)$ is as follows

$$\mathcal{L}(S) = \frac{1}{2^8} \left\{ \max_{\alpha,\beta} \{ \# \{ x \in GF(2^8) : \alpha \cdot x = \beta \cdot S(x) \} - 2^7 \} \right\},$$

where $\alpha \in GF(2^8)$ and $\beta \in GF(2^8) \{0\}$.

An S-box $S$ is said to be highly resistive against linear approximation attacks if it has low value of $\mathcal{L}(S)$. The LAP of the newly generated S-boxes is listed in Table 6. The average LAP of all of the listed S-boxes is 0.1371 which is very low, and hence the proposed technique 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.,

\[
D(S) = \frac{1}{2^8} \max_{\Delta x, \Delta y} \left\{ \# \{ x \in GF(2^8) : S(x \oplus \Delta x) = S(x) \oplus \Delta y \} \right\},
\]

where \( \Delta x, \Delta y \in GF(2^8) \), and \( \oplus \) is bit-wise addition over \( GF(2) \).

The smaller is the value of DAP, the higher is 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 7. It is evident from Table 7 that the newly generated S-boxes have high resistance against differential attacks.

4.3 Strict Avalanche Criterion (SAC)

The diffusion creation capability of an S-box is calculated by 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 \( S_i \), where \( 1 \leq i \leq 8 \), is computed by calculating an eight dimensional square matrix \( M(S) = [m_{ij}] \) by using each of the eight elements \( \alpha_j \in GF(2^8) \) with only one non-zero bit as

\[
m_{ij} = \frac{1}{2^8} \left( \sum_{x \in GF(2^8)} w \left( S_i(x \oplus \alpha_j) \oplus S_i(x) \right) \right),
\]

where \( w(v) \) denotes the number of non-zero bits in the vector \( v \).

SAC test is fulfilled, if all entries of \( M(S) \) are close to 0.5. The entries of SAC matrix corresponding to each newly generated S-boxes \( S_{1667,351}^N, S_{3299,1451}^D \) and \( S_{3299,2422}^M \) are plotted in a linear order in Figure 2. The average of minimum, and maximum values of \( M(S) \) corresponding to each of the newly generated S-boxes are 0.4115 and 0.6094, respectively. Table 8 clearly shows that the S-boxes generated by the proposed method based on MEC is capable of generating high diffusion in the data.
Table 8: SAC of the newly generated S-boxes

| S-boxes     | SAC(max) | SAC(min) |
|-------------|----------|----------|
| $S_{1667,351}^N$ | 0.5938   | 0.4531   |
| $S_{3299,1451}^D$ | 0.625    | 0.4219   |
| $S_{4229,2422}^M$ | 0.6094   | 0.3906   |

Figure 2: SAC matrix plot for $S_{1667,351}^N$, $S_{3299,1451}^D$ and $S_{4229,2422}^M$
4.4 Bit Independence Criterion (BIC)

BIC is also an important test to measure the diffusion creation strength of an S-box. The main idea of this test is to investigate the dependence of a pair of output bits when an input bit is reversed. The BIC of an S-box \( S \) over \( GF(2^8) \) with \( S_i \) boolean functions is also calculated by computing a square matrix \( N(S) = [n_{ij}] \) of dimension eight as follows

\[
n_{ij} = \frac{1}{2^8} \left( \sum_{x \in GF(2^8)} w \left( S_i(x \oplus \alpha_j) \oplus S_i(x) \oplus S_k(x + \alpha_j) \oplus S_k(x) \right) \right).
\]

Of course \( n_{ii} = 0 \). An S-box is said to be good if all off-diagonal values of its BIC matrix are near to 0.5. The experimental results of this test on the newly generated S-boxes \( S_{1667,351}, S_{1949,544}, S_{3299,1451} \) and \( S_{4229,2422} \) are shown in a linear order in Figure 3. The minimum, and maximum values of BIC matrix \( N(S) \) of each of the newly generated S-boxes are listed in Table 9. It is evident from Figure 3 and Table 9 that the S-boxes generated by the proposed methods are strong enough to generate high diffusion in the data.

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 is the AC, the greater is the security of the S-box against algebraic attacks. The AC of the newly generated S-boxes is computed, and is presented in Table 10. The minimum, and maximum values of AC of the newly generated S-boxes are 253, and 255, respectively, which are very close to the optimal value 255. Thus, the proposed method is able to generate S-boxes with good AC based on MEC.

5 Comparison and Discussion

A comparison of the security efficiency of the proposed S-box design technique with some of the existing techniques [14, 15, 16, 23, 24, 25, 26, 27, 28, 29, 30] is presented in this section by comparing the cryptographic properties of their
Figure 3: BIC matrix plot for $S^N_{1667,351}$, $S^D_{3299,1451}$ and $S^M_{4229,2422}$
Table 11: Comparison of the newly generated S-boxes with some of the existing S-boxes

| S-boxes | NL | LAP | DAP | SAC(Max) | SAC(Min) | BIC(Max) | BIC(Min) | AC |
|---------|----|-----|-----|----------|----------|----------|----------|----|
| Ref. [14] | 103 | 0.1328 | 0.0391 | 0.5703 | 0.4414 | 0.5039 | 0.4961 | 255 |
| Ref. [15] | 102 | 0.1484 | 0.0391 | 0.6094 | 0.375 | 0.5215 | 0.4707 | 254 |
| Ref. [16] | 106 | 0.1406 | 0.0391 | 0.5938 | 0.4375 | 0.5131 | 0.4648 | 251 |
| Ref. [19] | 104 | 0.0391 | 0.0391 | 0.625 | 0.3906 | 0.459 | 0.80 | 9 |
| Ref. [25] | 104 | 0.109 | 0.0469 | 0.5938 | 0.375 | 0.5254 | 0.4688 | 253 |
| Ref. [27] | 112 | 0.062 | 0.0156 | 0.5938 | 0.3984 | 0.4375 | 0.4746 | 255 |
| Ref. [28] | 74 | 0.2109 | 0.0547 | 0.6875 | 0.1094 | 0.504 | 0.480 | 9 |
| Ref. [29] | 103 | 0.1328 | 0.0391 | 0.5703 | 0.453 | 0.5273 | 0.4707 | 255 |
| SN_{1667,351} | 106 | 0.1328 | 0.0391 | 0.5938 | 0.3984 | 0.4375 | 0.4746 | 255 |
| S_{129,2422} | 106 | 0.1328 | 0.0391 | 0.5938 | 0.375 | 0.5254 | 0.4688 | 253 |

S-boxes. The cryptographic properties of the S-boxes used in this comparison are listed in Table 11. Note that the non-linearity (NL) of the S-boxes $S_{1667,351}$, $S_{129,2422}$, and $S_{129,2422}$ is greater than that of the S-boxes in [14, 15, 16, 25, 28, 29, 30], and hence the newly generated S-boxes create better confusion in the data as compared to the later S-boxes. This implies that the proposed technique is capable of generating S-boxes with good NL as compared to some of the other existing techniques. Moreover, the linear approximation probability (LAP) of the newly generated S-boxes is better than the LAP of the S-boxes in [14, 15, 16, 25, 28, 29, 30], while their differential approximation probability (DAP) is at most the DAP of the S-boxes in [14, 15, 16, 25, 28, 29, 30]. Hence, the S-boxes generated by the proposed technique have same or better security against approximation attacks as compared to the other S-boxes. Similarly, the SAC, BIC and AC test results of the newly generated S-boxes are comparable with the S-boxes listed in Table 11. Hence, the proposed S-box generation technique based on MEC is capable of generating cryptographically strong S-boxes as compared to some of the existing S-box construction techniques based on different mathematical structures. Furthermore, the proposed algorithm takes constant time for the generation of an S-box, while the method based on EC in [19] takes $O(p)$ time, where $p$ is the prime of the underlying EC. This implies that the proposed algorithm is fast as compared to the method in [19].

6 Conclusion

In this article, we presented an S-box design technique based on $y$-coordinates of a finite Mordell elliptic curve (MEC) where prime is congruent to 2 modulo 3. The technique uses some special type of total orders on the points of the MEC, and generates an S-box in constant time. Several standard security tests are performed on the S-boxes generated by the proposed method to analyze its cryptographic efficiency. Experimental results show that the newly generated S-boxes are cryptographically strong. Furthermore, a comparison of some of the
newly generated S-boxes with S-boxes generated by some of the existing techniques is also performed. It is evident from the comparison that the proposed method is capable of generating more secure S-boxes as compared to some of the existing S-box design techniques.

References

[1] Shannon, C. E. (1949). Communications theory of secrecy systems. Bell Labs Technical Journal, 20, 656–715.

[2] Thomas, J., and Knudsen, L. R. (1997). The interpolation attack on block ciphers. International workshop on fast software encryption (FSE), Fast Software Encryption (pp. 28–40).

[3] Courtois, N. T., and Josef, P. (2002). Cryptanalysis of block ciphers with over defined systems of equations. ASIACRYPT 2002 LNCS, 2501, 267–287.

[4] Murphy, S., and Robshaw, M. J. (2002). Essential algebraic structure within the AES. Proceedings of the 22th annual international cryptology (pp. 1–16). Berlin: Springer.

[5] Rosenthal, J. (2003). A polynomial description of the Rijndael advanced encryption standard. Journal of Algebra and its Applications, 2, 223–236.

[6] Azam, N. A., A Novel Fuzzy Encryption Technique Based on Multiple Right Translated AES Gray S-Boxes and Phase Embedding, Security and Communication Networks Volume 2017, Article ID 5790189, 9 pages, https://doi.org/10.1155/2017/5790189.

[7] Hussain, I., Azam, N. A., and Shah, T. (2014). Stego optical encryption based on chaotic S-box transformation. Optics and Laser Technology, 61, 50–56.

[8] Rahnama, B., Y. Kran, R. Dara, Countering AES Static S-Box Attack, SIN '13, November 26 - 28 2013, Aksaray, Turkey Copyright 2013 ACM 978-1-4503-2498-4/13/1115.00. http://dx.doi.org/10.1145/2523514.2523541

[9] Liu, J., Wai, B., Cheng, X., and 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).

[10] Cui, L., and Cao, Y. (2007). A new S-box structure named affine power-affine. International Journal of Innovative Computing, Information and Control, 3, 751–759.

[11] Tran, M. T., Bui, D. K., and Doung, A. D. (2008). Gray S-box for advanced encryption standard. International Conference on Computational Intelligence and Security, 1, 253–258.
[12] Khan, M., and Azam, N. A. (2014). Right translated AES Gray S-box. Security and Network Communication. https://doi.org/10.1002/sec.1110.

[13] Khan, M., and 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.

[14] Guoping, T., Xiaofeng, L., and Yong, C. (2005). A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons and Fractals, 23, 413–419.

[15] Guo, C. (2008). A novel heuristic method for obtaining S-boxes. Chaos, Solitons and Fractals, 36, 1028–1036.

[16] Neural, Y. W., Li, Y., Min, L., and Sihong, S. (2010) A method for designing S-box based on chaotic neuralnetwork. In 2010 Sixth international conference on natural computation (ICNC).

[17] Miller, V. (1986). Uses of elliptic curves in cryptography. Advances in Cryptology, 85, 417–426.

[18] Jung, H. C., Seongtaek, C., and Choonsik, P. (1999). S-boxes with controllable nonlinearity, EUROCRYPT ’99. LNCS, 1592, 286–294.

[19] Hayat, U., Azam N. A., and Asif, M. (2018) A Method of Generating 8 × 8 Substitution Boxes Based on Elliptic Curves, Wireless Personal Communications. 101: 439–451

[20] Brown, D. R. L. (2009). SEC 1: Elliptic curve cryptography. Mossossaiga: Certicom Corp.

[21] Washington, L. C. (2008) Number Theory: Elliptic Curves and Cryptography, vol. 50 of Discrete Mathematics and Its Applications. Chapman and Hall/CRC, 2nd ed.

[22] Willi, M., and Othmar, S. (1990). Nonlinearity criteria for cryptographic functions. Advances in Cryptology-EUROCRYPT ’89 LNCS, 434, 549–562.

[23] Shi, X. Y., Xiao, H., You, X. C., and Lam, K. Y. (1997). A method for obtaining cryptographically strong 8 x 8 S-boxes. International Conference on Information Network and Application, 2, 689–693.

[24] Jakimoski, G., and Kocarev, L. (2001). Chaos and cryptography: block encryption ciphers. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48, 163–170.

[25] Kim, J., and Phan, R. C. W. (2009). Advanced differential-style cryptanalysis of the NSA’s skipjack block cipher. Cryptologia, 33, 246–270.

[26] Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., and 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.

15
[27] Daemen, J., and Rijmen, V. (2002) The Design of Rijndael-AES: The Advanced Encryption Standard, Springer, Berlin, Germany.

[28] Gautam, A., Gaba, G. S., Miglani, R., and Pasricha, R. (2015) Application of Chaotic Functions for Construction of Strong Substitution Boxes, Indian Journal of Science and Technology, vol. 8, no. 28, pp. 1-5.

[29] Chen, G., Chen, Y., and Liao, X. (2007) An extended method for obtaining S-boxes based on three-dimensional chaotic baker maps, Chaos, Solitons and Fractals, vol. 31, no. 3, pp. 571-579.

[30] Tang, G., Liao, X., and Chen, Y. (2005) A novel method for designing S-boxes based on chaotic maps, Chaos, Solitons and Fractals, vol. 23, no. 2, pp. 413-419.