*International Journal of Engineering Inventions*
*ISSN: 2278-7461, www.ijeijournal.com*
*Volume 1, Issue 9 (November2012) PP: 49-54*

# An Efficient Elliptic Curve Cryptography protocol Based on Matrices

F. Amounas[1] and E.H. El Kinani[2],
[1]*R.O.I Group, Informatics Department Moulay Ismaïl University, Faculty of Sciences and Technics Errachidia, Morocco*
[2]*A.A Group, Mathematical Department Moulay Ismaïl University, Faculty of Sciences and Technics Errachidia, Morocco*

**Abstract:—**In the last decade the Elliptic Curve Cryptography (ECC) was gained a lot of attention in the literature due to their performance. In fact, the principal attraction of ECC compared to RSA (Rivest-Shamir-Adleman) is that it offers equal security for a smaller bit size, thereby reducing processing overhead. In this paper, we present a novel mapping of text message into multiple points on Elliptic Curve by using addition table. Then, we describe a new method for encryption and decryption based on matrices. Further, this paper also attemps to utilize the properties of invertible matrices in encryption and decryption process with more flexible and efficient. The proposed method enhances the security of ECC with multi fold encryption.

**Keywords:—**Elliptic Curve Cryptography, Addition Table, Encryption, Shifting Technique, Non-singular Matrix, Decryption.

## I. INTRODUCTION

Most of the existing public key cryptosystems are based on the number theory, providing high stability against attacks by using a large key space. Elliptic Curve Cryptography (ECC) is a newer approach, and considered as a good technique with low key size for the user. In fact, in ECC a 160-bit key provides the same security as compared to the traditional crypto system RSA [1] with a 1024-bit key. Therefore, ECC offers considerably greater security for a given key size. Further, there are extremely efficient, compact hardware implementations are available for ECC exponentiation operations, offering potential reductions in implementation footprint even beyond those due to the smaller key length alone. ECC is not only emerged as an attractive public key crypto-system for mobile/wireless environments but also provides bandwidth savings. The use of elliptic curve in cryptography was proposed firstly by Miller [2] and Koblitz [3] and it is not easy to understand by attacker.

In our previous works, we have provided an example of the public-key cryptosystem based on ECC mechanism [4] and the implementation of elliptic curve cryptosystem using Tifinagh characters [5]. In fact, the transformation of the message into affine points is explained. A transformed character is encrypted by ECC technique. Further, we have provided some methods based ECC [6, 7, 8, 9]. Our approach here is different from our previous work [9] due to the use of addition table of the points on elliptic curve. More precisely, in this paper we have discussed about the encryption for cryptography with elliptical curves $E(F_p)$ and an attempt has been made to represent plaintext with points on EC with the help of an addition table a new encryption technique based on matrix is provided.

The remainder of this paper is arranged as follows: we briefly review some basic notions connected with elliptic curve in section 2. Section 3, is devoted to the description of the methodology for encryption of plaintext based on matrices with addition table. In section 4, we explain the implementation of the proposed method with an example. In section 5, we give our results analysis followed by our conclusion.

## II. MATHEMATICAL BACKGROUND OF ELLIPTIC CURVE ARITHMETIC

In this section, we recall briefly the notion of elliptic curve (EC), for more details, we refer interested reader to[10].

An elliptic curve E over finite field $F_p$ in its standard form is described by:

$$y^2 = x^3 + ax + b\ [p], \qquad (1)$$

where $a, b \in F_p$, and $4a^3 + 27b^2 \neq 0 \pmod p$, then the elliptic curve is noted by $E_p(a, b)$.

An elliptic curve over $F_p$ consists of all points (x, y) where $x,y \in F_p$ such that it satisfies equation (1) together with the point at infinity, noted $\Omega$.

The addition of points follows specific rules indicated below:

(1) $\Omega + \Omega = \Omega$.

(2) $P + \Omega = P$ for all values of $P = (x, y) \in E$.
Namely, E has $\Omega$ as its identity element.

(3) $P + Q = \Omega$ for all values of $P= (x, y) \in E$ and $Q=(x, -y) \in E$.
In other words, the inverse of (x, y) is simply (x, - y).

(4) Adding two distinct points:

For all $P = (x_1, y_1) \in E$ and $Q = (x_2, y_2) \in E$ with $x_1 \neq x_2$,
$P+Q = (x_3, y_3)$ is defined as:

$$\begin{cases} x_3 = \alpha^2 - x_1 - x_2 \\ y_3 = \alpha(x_1 - x_3) - y_1 \end{cases} \quad \text{where} \quad \alpha = (y_2 - y_1)/(x_2 - x_1)$$

(5) Doubling a point:

For any $P = (x_1, y_1) \in E$ with $y_1 \neq 0$, $2P = (x_2, y_2)$ is defined as:

$$\begin{cases} x_2 = \alpha^2 - 2x_1 \\ y_2 = \alpha(x_1 - x_2) - y_1 \end{cases} \quad \text{where} \quad \alpha = (3x_1^2 + a)/2y_1$$

## III. MAIN RESULT

*A. Proposed Method Description*

In this section, we introduce new cryptography protocol based on algebraic description for addition operation over finite field $F_p$. More precisely, the proposed algorithm requires that we generate addition table which contain all possible points with coordinates between 0 … p-1. It is known that each addition two points represents third point in curve i.e $P(x,y) + Q(x,y)=R(x,y)$.

Further, the point R(x,y) have many choices but addition different points P(x,y) and Q(x,y) gives unique point R(x,y). This feature makes the protocol more efficient.

*1) Generate Addition table for EC*

- Choose an elliptic curve E defined over finite field $F_p$. Let P is a point generator and n is order of P.
- Generate table addition (n×n) by using the rules for addition over $E_p(a, b)$.

**Table 1.** The table addition of points on EC

| + | $\mathbf{Q}_0$ | $\mathbf{Q}_1$ | … | $\mathbf{Q}_{n-1}$ |
|---|---|---|---|---|
| $\mathbf{P}_0$ | $R_{0,0}$ | $R_{0,1}$ | … | $P_{0,n-1}$ |
| $\mathbf{P}_1$ | $R_{1,0}$ | $R_{1,1}$ | … | $P_{1,n-1}$ |
| | ... | ... | … | |
| $\mathbf{P}_{n-2}$ | $R_{n-2,0}$ | $R_{n-2,1}$ | … | $R_{n-2,n-1}$ |
| $\mathbf{P}_{n-1}$ | $R_{n-1,0}$ | $R_{n-1,1}$ | … | $R_{n-1,n-1}$ |

Each point is represented by two different point $R_{i,j} = P_i + Q_j$ . There many forms that represent a point R. This feature helps to send the same characters but with another form.

For example: The below table shows the results of addition over $E_7$ (3, 2).

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| (2,3) | (5,4) | Ω | (5,3) | (0,4) | (2,4) | (4,6) | (4,1) | (0,3) |
| (5,4) | (4,6) | (0,3) | (2,4) | Ω | (0,4) | (4,1) | **(5,3)** | (2,3) |
| Ω | (0,3) | (2,4) | (4,6) | **(5,3)** | (4,1) | (2,3) | (5,4) | (0,4) |
| **(5,3)** | (2,4) | (4,6) | (0,3) | (5,4) | (2,3) | (0,4) | Ω | (4,1) |
| (0,4) | Ω | **(5,3)** | (5,4) | (4,1) | (4,6) | (0,3) | (2,3) | (2,4) |
| (2,4) | (0,4) | (4,1) | (2,3) | (4,6) | (5,4) | Ω | (0,3) | (5,3) |
| (4,6) | (4,1) | (2,3) | (0,4) | (0,3) | Ω | **(5,3)** | (2,4) | (5,4) |
| (4,1) | **(5,3)** | (5,4) | Ω | (2,3) | (0,3) | (2,4) | (0,4) | (4,6) |
| (0,3) | (2,3) | (0,4) | (4,1) | (2,4) | (5,3) | (5,4) | (4,6) | Ω |

There is many forms that represent unique point (5,3), i.e

(5,3)= (2,4) + (0,4); (5,3)= (4,1) + (0,3); ...

- Use an appropriate data structure to store the text to be encrypted.
- Read the table in row-major form and find the corresponding point of character stored in that position.
- Note the row and column points.
- Assign these values to the same character in all positions it appears.

*2) Encryption process*

Alice wants to send a message M to Bob. She converts the message with equivalent points in EC.

1. Transforms the plaintext into points on elliptic curve $R_i$, i=1, 2, …, r.
2. Converts the points R(x, y) in another form using Table 1. So, each point is represented by two points.
3. All points are stored into matrix of (r×2) as follows:

$$M= \begin{pmatrix} P_1 & Q_1 \\ P_2 & Q_2 \\ . & . \\ . & . \\ . & . \\ P_r & Q_r \end{pmatrix}$$

4. Choosing a non-singular matrix of $(2\times2)$ such that $|A|=\pm1$.

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

5. Using addition and doubling of points to compute: B=MA. For example: the first element of B is computed as: $a_{11}P_1 + a_{21}Q_1$.

6. Circularly shifting each row of B by one element to the right. Next, circularly shifting downward columns of matrix B. The result matrix is noted D.

Converts the data points into binary form and call it C.

*3) Decryption process*

After receiving the cipher text C, it may be decrypted by the receiver using the following steps:

*Step 1*. First separate x-coordinate and y-coordinate of points $D_i$ from C.

*Step 2*. Convert a sequence to decimal form.

*Step 3*. Obtain $D_i$ from two values and stored point $D_i=(x_1, y_1)$ into matrix of $(r\times2)$.

*Step 4*. Circular upward shift is followed by circular left shift the elements of D. The result matrix is noted B.

*Step 5*. Compute $M = BA^{-1}$ to obtain a points $P_i$ and $Q_i$.

*Step 6*. Compute $R_i = P_i + Q_i$ for each row of M. Then reverse the embedding to recover the plaintext.

## IV. IMPLEMENTATION OF THE PROPOSED ALGORITHM

In this section we implemented an example that shows the proposed algorithm using the elliptic curve defined by the following equation:

$$y^2 = x^3 - x + 16[29] \qquad (2)$$

The base point P is selected as (5, 7). Here, the choosing curve has 31 points with P is the point generator.

The set of all points on elliptic curve $E_{29}$ (-1, 16) are:

{ Ω, (5, 7), (28, 4), (18, 1), (22, 12), (6, 20), (13, 5), (2, 14), (21, 11), (23, 3), (10, 7), (14, 22), (16, 23), (7, 27), (1, 4), (0, 4), (0, 25), (1, 25), (7, 2), (16, 6), (14, 7), (10, 22), (23, 26), (21, 18), (2, 15), (13, 24), (6, 9), (22, 17), (18, 28), (28, 25) (5, 22) }

The points on the elliptic curve over $E_{29}$ (-1, 16) is shown below in Fig. 1.

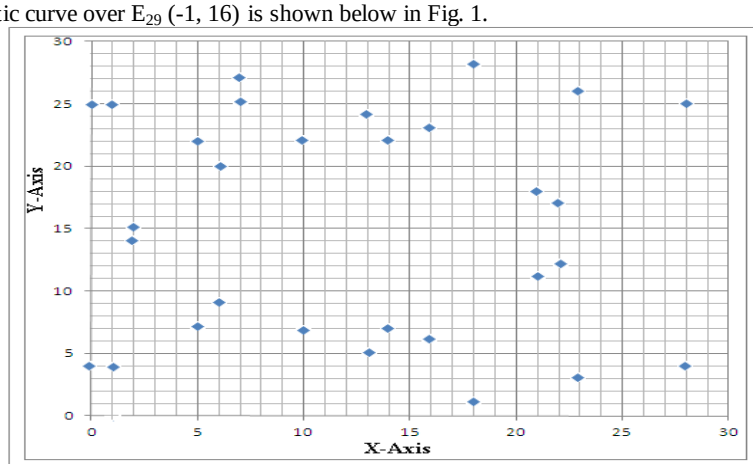


***Figure 1.*** *The elliptic curve $E_{29}$ (-1, 16)*

Here, all text characters are converted into points on elliptic curve. P is the point which represents the letter 'a', as well as 2P represents the letter 'b',..., (31P) represents space. In our case we use the letters 'a' to 'z' with some of the other symbols like ';', ', ', '.', ' ?' and space for illustration purpose only.

*A. Case Study of the Encryption Process*

To encrypt the message "cipher", the encoding process convert this message to points:
(18,1), (23,3), (0,25), (21,11), (6,20), (7, 2)
In this stage, we use another form for represent each point using addition table.
There many forms that represent unique (18,1) i.e:
(18,1)= (0,25) + (7,2) or (18,1)=(23,26) + (16,23), …
In our case, we select (18,1)=(0,25) + (7, 2).
Similarly we have:
(23,3)=(13,24) + (0,4)
(0,25)=(16,6) + (18,28)
(21,11)=(5,22) + (23,3)
(6,20)=(5,7) + (22,12)
(7,2)=(2,15) + (13,24)
Now we rearrange these points into a matrix M (Row wise / Column wise). We use row wise. For our case, we have:

$$M=\begin{pmatrix} (0,25) & (7,2) \\ (13,24) & (0,4) \\ (16,6) & (18,28) \\ (5,22) & (23,3) \\ (5,7) & (22,12) \\ (2,15) & (13,24) \end{pmatrix}$$

Next, Then we perform the product B=MA, where A is an arbitrary nonsingular matrix with $|A| = \pm 1$.
In our case, we choose A as:

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$$

Then,

$$B = MA = \begin{pmatrix} (0,25) & (7,2) \\ (13,24) & (0,4) \\ (16,6) & (18,28) \\ (5,22) & (23,3) \\ (5,7) & (22,12) \\ (2,15) & (13,24) \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} (10,22) & (21,11) \\ (2,15) & (21,11) \\ (7,27) & (10,7) \\ (1,25) & (6,9) \\ (23,3) & (7,27) \\ (16,23) & (13,5) \end{pmatrix}$$

Circular right shift is followed by circular downward shift the elements of matrix. The result matrix is noted D as follow:

$$D=\begin{pmatrix}(13,5) & (16,23)\\ (21,11) & (10,22)\\ (21,11) & (2,15)\\ (10,7) & (7,27)\\ (6,9) & (1,25)\\ (7,27) & (23,3)\end{pmatrix}$$

Then, the cipher text C is given as following:
01101001011000010111101010101101010101101010101011000100111101010001110011111101100110010010000111001
00111110111011100011

*B. Case Study of the Decryption Process*
After receiving the cipher text C by the receiver, he will decrypt it using the following steps:
*Step 1*. Separate C into groups of m bits. In our case m=10.
*Step 2*. Extract the x-coordinate and the y-coordinate of points $D_i$ from results of step1. Then convert them to decimal.
*Step 3*. Obtain points $D_i$ with coordinates indicated in step 2. Then stored data points in matrix of (6×2).
*Step 4*. Circular upward shift is followed by circular left shift the elements of matrix D. The result matrix B is given as:

$$B=\begin{pmatrix}(10,22) & (21,11)\\ (2,15) & (21,11)\\ (7,27) & (10,7)\\ (1,25) & (6,9)\\ (23,3) & (7,27)\\ (16,23) & (13,5)\end{pmatrix}$$

Step 5. The encoded message M is again decoded using the inverse of A.

$$M=BA^{-1}=\begin{pmatrix}(10,22) & (21,11)\\ (2,15) & (21,11)\\ (7,27) & (10,7)\\ (1,25) & (6,9)\\ (23,3) & (7,27)\\ (16,23) & (13,5)\end{pmatrix}\begin{pmatrix}3 & -1\\ -2 & 1\end{pmatrix}$$

$$=\begin{pmatrix}(0,25) & (7,2)\\ (13,24) & (0,4)\\ (16,6) & (18,28)\\ (5,22) & (23,3)\\ (5,7) & (22,12)\\ (2,15) & (13,24)\end{pmatrix}$$

Step 6. For each row, adding data points. The obtained stream of points is given as:
(18,1), (23,3), (0,25), (21,11), (6,20), (7,2)
Now reverses the embedding to get back the message. Thus we retrieve the plaintext "cipher".

## V. RESULT ANALYSIS

In this paper, we have mapped each alphabet into two points on elliptic curve using addition table. Then, we ciphered the results points by using a non-singular matrix of (2×2). Here, we analysed with existing public key algorithm to find out our algorithm performance.

*- Encryption analysis*

Our encryption technique is very authoritative and straight forward. In this algorithm, there are many forms to represents an point on elliptic curve. The algorithm is based on the (2×2) square matrix. Therefore we can select nonsingular

matrix noted A with |A|=±1. When compare to other algorithm, the RSA algorithm calculates each and every text variable for encryption. The ElGamal algorithm produces two different cipher texts for single encryption. In our algorithm we can make set of points in single encryption. The following figure (Fig. 2) clearly indicates about encryption methods of various algorithms.

- *Decryption analysis*

Our decryption process is complex without the private key. All the plaintext are decrypted using inverse matrix as a key, Therefore it provides security from the unauthorized entities and susceptible. Comparing to other algorithm, the RSA algorithm decrypt the cipher text one by one. The ElGamal algorithm receives the two cipher text and calculating decryption once. In our algorithm, we receive set of blocks and decrypt in single step. The following Figure (Fig. 3) clearly indicates about decryption methods of various algorithms.

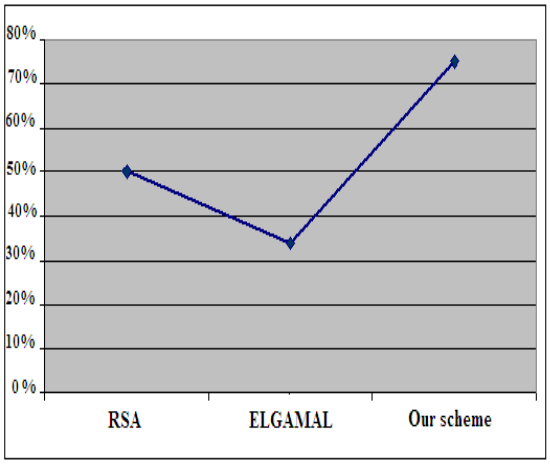


***Figure 2.*** *Comparison performance of Encryption.*

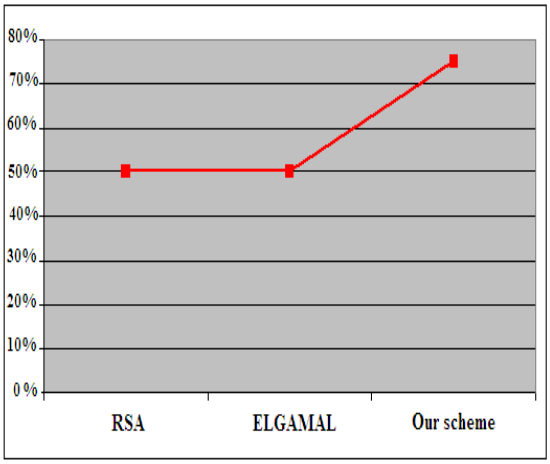


***Figure 3.*** *Comparison performance of Decryption.*

## VI. CONCLUSION

This paper presented a method to embed the message into the multiple point form and then using non-singular matrix for encryption. In the proposed method, the same character of message is mapped to different points by using addition table of the curve points. Therefore, the proposed method strengthens the cryptosystem, i.e., for a given intruder it would be very difficult to guess on which points the message characters are mapped and it hides letter frequencies of the plaintext message. The test realized on the algorithm showed their robustness and their efficiency. Finally, we like to point out that the use of non-singular matrix will provide better performance in this regard.

## REFERENCES

1. Rivest R., Schamir A. and Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21, pp. 120-126,.
2. Miller V. Use of elliptic curves in cryptography. Advances in Cryptography-Crypto 85. LNCS 218, Springer Verlag, 1986, pp.417-426.
3. Koblitz N., Menezes A.J., and Vanstone S.A. The state of elliptic curve cryptography. Design, Codes and Cryptography, 2000, Vol 19, Issue 2-3, pp.173-193.
4. F.Amounas, E.H. El Kinani and A. Chillali, An application of discrete algorithms in asymmetric cryptography, International Mathematical Forum, 2011, Vol. 6, no. 49, pp. 2409-2418.
5. F.Amounas and E.H. El Kinani, Cryptography with Elliptic Curve Using Tifinagh Characters, Journal of Mathematics and System Science, 2012, Vol.2, No.2, pp.139-144.
6. F.Amounas and E.H. El Kinani, ECC Encryption and Decryption with a Data Sequence, Applied Mathematical Sciences, 2012, Vol. 6, no. 101, pp. 5039- 5047.
7. F.Amounas and E.H. El Kinani, An elliptic curve cryptography based on matrix scrambling method, Proceedings of the JNS2, IEEE Xplore, 2012, pp. 31-35.
8. F.Amounas and E.H. El Kinani, Elliptic Curve Digital Signature Algorithm Using Boolean Permutation based ECC, International Journal of Information & Network Security (IJINS), 2012, Vol.1, No.3, pp. 216-222.
9. F.Amounas and E.H. El Kinani, Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography, International Journal of Information & Network Security (IJINS), 2012, Vol.1, No.2, pp. 54-59.
10. Darrel R. Hankerson, Scott A. Vanstone, and Alfred J. Menezes. "Guide to Elliptic Curve Cryptography". Springer, 2004.