International Journal of Information & Network Security (IJINS)
Vol.1, No.2, June 2012, pp. 54~59
ISSN: 2089-3299

Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography

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

Article Info

Article history:

Received April 30th, 2012
Revised May 11th, 2012
Accepted June 02th, 2012

Keyword:

Elliptic Curve,
Nonsingular Matrix,
Cryptography,
Mapping,
Encryption/Decryption

ABSTRACT

In this paper, we propose a new mapping method based on the proprieties of matrices and the elliptic curve to generate an algorithm that will guarantee the confidentiality of messages. In fact, the alphanumeric characters are mapped onto the points of the elliptic curve in the proposed method by using non-singular matrix. The details of this algorithm with examples are in order. The mapping technique will increase the strength of the elliptic cryptosystem. The proposed method is efficient in its principale and has great potential to be applied to others situations where the exchange of messages is done confidentially.

Corresponding Author:

E.H. El KINANI
Mathematical Department
Moulay Ismaïl University,
Faculty of Sciences and Technics, Box 509 Errachidia, Morocco
E-mail: elkinani_67@yahoo.com

1. INTRODUCTION

It is well known that coding theory is a subject by which the exchange of messages is administered in a confidential and more secured way having a wide application in differents domains. Recently there has been a wide application of inversion of matrices to the problem of exchange of messages in a confidential and a secured way (see e.g [1]). For more details on the theory of matrices, refer to [2]. Furthermore, elliptic curves are fundamental objects in a large part of mathematics they are very interesting because their study involves several fields of mathematics. In 1985, Neal Koblitz [3] and Victor Miller [4] independently proposed using the group of points on an elliptic curve defined over a finite field in discrete logarithm cryptographic systems. The primary advantage that elliptic curve systems have over systems based on the multiplicative group of a finite field (and also over systems based on the intractability of integer factorization) is the absence of a sub exponential-time algorithm (such as those of "index-calculus" type) that could find discrete logarithms in these groups. Consequently, one can use an elliptic curve group that is smaller in size while maintaining the same level of security. The result is smaller key sizes, bandwidth savings, and faster implementations features that are especially attractive for security applications where computational power and integrated circuit space is limited, such as smart cards, personal digital assistants, and wireless devices. Elliptic curve cryptographic protocols for digital signatures, public-key encryption, and key establishment have been standardized by numerous standards organizations including: Institute of Electrical and Electronics Engineers (IEEE 1363), American National Standards Institute (ANSI X9.63), International Standards Organization (ISO/IEC 15946-3), etc.

The vast majority of the standards that use public-key cryptography for encryption and digital signatures use RSA[5]. Recently, the bit length for secure RSA use has increased and this has put a heavier processing load on applications using RSA. Then, a competing system that has emerged is elliptic curve cryptosystem (ECC)[6] and have been attracting increased attention of many authors [7,8], because they have opened a wealth possibilities in terms of security. In our previous works, we provide an example of the public-key cryptosystems based on ECC mechanism [9] and the implementation of elliptic curve cryptosystem using Tifinagh characters [10].

In fact, the transformation of the message into an affine point is explained. A transformed character is encrypted by ECC technique. In the present work, we propose a new mapping method based on matrices and the elliptic curve. In fact, the properties of invertible matrices are combining with elliptic curve to provide a novel mapping method for encrypting/decrypting process. In this algorithm the original message is transformed by using mapping method and coded with nonsingular matrix. Further, the coded message is crypted by ECC technique. The result of decryption process is put in matrix form to be decoded by the recipient by using the inverse of the matrix. In the existing method [11,12], it is easy to decipher using letter frequency attack, because the simple mappings preserve letter frequencies of the plaintext message. But in our proposed method, the same characters are mapped to different points. So, it hides letter frequencies of the plaintext message.

The rest of this paper is organized as follows: we start with brief review of ECC (Elliptic Curve Cryptography) in section 2. Section 3, is devoted to the main results, first we give a new procedure of mapping based on nonsingular matrix and elliptic curve, then the obtained points are encrypted and decrypted by ECC process. Finally, the concluding remarks will be given in the last section.

2. CRYPTOGRAPHY WITH ELIPTIC CURVE

In elliptic curve cryptography, we are concerned with a restricted form of elliptic curve that is defined over a finite field noted F_p. One particular interest for cryptography is what is referred to as the elliptic group mod p, where p is a prime number. This is defined as follows, choose two nonnegative integers, α and β, less than p that satisfy:

$$4\alpha^3 + 27\beta^2 \pmod p \neq 0 \qquad (1)$$

Then $E_p(\alpha, \beta)$ denotes the elliptic group mod p whose elements (x, y) are pairs of nonnegative integers less than p satisfying:

$$y^2 = (x^3 + \alpha x + \beta) \bmod p, \qquad (2)$$

together with the point at infinity Ω.

The addition operator is defined over $E(F_p)$ and it can be seen that $E(F_p)$ forms an abelian group. The addition and doubling of points rule is explained in many references (see e.g [13]).

2.1. ECC Encryption and Decryption

Several approaches to encryption/decryption using elliptic curves have been analyzed. This paper describes one of them: Elgamal cryptosystem [14]. The first task in this system is to encode the plaintext message m to be sent as an x-y point P_m. It is the point P_m that will be encrypted as a cipher text and subsequently decrypted. First recall that the Elgamal cryptosystem consist in the following steps:

Suppose here that we have some elliptic curve E defined over a finite field Fp and that E and a point $P \in E$ are publicly known, as is the embedding system $m \rightarrow P_m$, which imbed plain text on an elliptic curve E. Then, when Alice wants to communicate secretly with Bob, they proceed thus:

Step 1. Bob chooses a random integer a, and publishes the point aP (while a remains secret).
Step 2. Alice chooses her own random integer l and sends the pair of points $(lP, P_i + l(aP))$ to Bob (while a remains secret).
Step 3. To decrypt the message, Bob calculates $a(lP)$ from the first part of the pair, then subtracts it from the second part to obtain $P_i + l(aP) - a(lP) = P_i + laP - laP = P_i$, and then reverses the embedding to get back the message.

More precisely, an example of Elgamal encryption cryptosystem based into an elliptic curve is given in [11].

3. MAIN RESULTS

3.1. Description of the proposed Method

In this section, we will provide a new mapping method based on matrices and elliptic curve. The alphanumeric characters are mapped on to the points of the elliptic curve in the following method. The proposed method requires both the sender of the message and the receiver of the message to know the following relationships:

E(Fp): the set of points on elliptic curve.
P: base point with order N.
C: the set of all alphabets and ponctions marks.
S: the set of the mapping points generated by the proposed algorithm.
A: the encoded matrix is constructed in such a way that: A is nonsingular and has only integer entries.
A^{-1}: Matrix inverse of A. In our case, we select the entries of A in such a manner that: $|A|= \pm 1$ (for simplicity).

We define the mapping F: C $\rightarrow$S, as specified rule of correspondence between sets of symbols which are composed message and a set of points on elliptic curve.
Suppose that we have some elliptic curve E defined over a finite field F_p and that E and a point $P \in E$ are publicly known, as is the embedding system m $\rightarrow P_m$, which imbed the original message on an elliptic curve E.

3.1.1. Mapping Methodolgy

Step 1. Transform the alphanumeric characters into points on elliptic curve.

$$[P_1(x_1, y_1), P_2(x_2, y_2), P_3(x_3, y_3), \ldots , P_n(x_n, y_n)]$$

We consider m the original message of length n. If n is not divided by 3, then the points have been padded with Ω which represent space.
Step 2. Creating the matrix of 3×r with entries are points on EC (Step 1):

$$M= \begin{pmatrix} P_1 & P_2 & P_3 & \ldots & P_r \\ P_{r+1} & P_{r+2} & P_{r+3} & \ldots & P_s \\ P_{s+1} & P_{s+2} & P_{s+3} & \ldots & P_n \end{pmatrix}$$

with r = n/3 and s = 2n/3
Step 3. Choosing a non singular matrix of 3×3 such that $|A| = \pm 1$. Then, using addition and doubling of points to compute: **Q = AM**
With

$$A= \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Step 4. The result set of points is:

$$S = [Q_1(x_1, y_1),Q_2(x_2, y_2), ..., Q_n(x_n, y_n)].$$

Once the mapping of the all-alphanumeric characters onto the curve is completed, these points are crypted by using elliptic curve encryption technique which are transmitted through an insecure channel. The message is retrieved from the encoded data by using the elliptic curve decryption technique and the inverse of matrix.

3.2. Illustration and results

In our case we choose an elliptic curve given by the following equation:

$$y^2 = x^3 + x + 13[31] \qquad (3)$$

The table below (Table 1) gives a set of points on the elliptic curve. In our case, the choosing curve contains 34 points, then if P is the generator point of the group. It is the point which represents the letter 'a', as well as 2P represents the letter 'b',..., 34P represents space.

Table 1. A set of points on EC

(9, 10)	(18, 29)	(23, 19)	(4, 22)	(25, 16)
(17,18)	(6, 24)	(24, 29)	(16, 8)	(20, 2)
(22, 22)	(28, 13)	(27, 10)	(26, 21)	(5, 9)
(19, 3)	(10, 0)	(19, 28)	(5, 22)	(26, 10)
(27,21)	(28, 18)	(22, 9)	(20, 29)	(16, 23)
(24, 2)	(6, 7)	(17, 13)	(25, 15)	(4, 9)
(23, 12)	(18, 2)	(9, 21)	Ω	

Here, we choose a nonsingular matrix as follow:

$$A=\begin{pmatrix} -1 & 5 & -1 \\ -2 & 11 & 7 \\ 1 & -5 & 2 \end{pmatrix}$$

Then,

$$A^{-1}=\begin{pmatrix} -57 & 5 & -46 \\ -11 & 1 & -9 \\ 1 & 0 & 1 \end{pmatrix}$$

Here in our case Alice wishes to send a message "cryptography" to Bob. So, we have P = (9, 10), a = 41, and l = 13. Then, we convert the above message into a stream of points as follows:
{ (23, 19), (19, 28), (16, 23), (19, 3), (26, 10), (5, 9), (6, 24), (19, 28), (9, 10), (19, 3), (24, 29), (16, 23)}

The results of the mapping, encrypted, decrypted points is shown in Table2. Their graphically representations are shown in Figure 1, Figure 2 and Figure 3..

Table 2. Mapping, encrypted and decrypted points for "cryptography".

Character	Point Pi	Mapping Points	Encrypted Points	Decrypted Points (Qi)
c	(23,19)	(17, 3)	((27, 10),(10, 0))	(17, 3)
r	(19,28)	(6, 24)	((27, 10),(4, 9))	(6, 24)
y	(16, 23)	(18, 29)	((27, 10),(16, 23))	(18, 29)
p	(19, 3)	(5, 9)	((27, 10),(4, 22))	(5, 9)
t	(26, 10)	(10, 0)	((27, 10),(18, 29))	(10, 0)
o	(5, 9)	(6, 24)	((27, 10),(4, 9))	(6, 24)
g	(6, 24)	(5, 9)	((27, 10),(4, 22))	(5, 9)
r	(19, 28)	(9, 10)	((27, 10),(20, 29))	(9, 10)
a	(9, 10)	(6, 24)	((27, 10),(4, 9))	(6, 24)
p	(19, 3)	(16, 8)	((27, 10),(18, 2))	(16, 8)
h	(24, 29)	(17, 18)	((27, 10),(25, 15))	(17, 18)
y	(16, 23)	(20, 2)	((27, 10)),(9,21))	(20, 2)

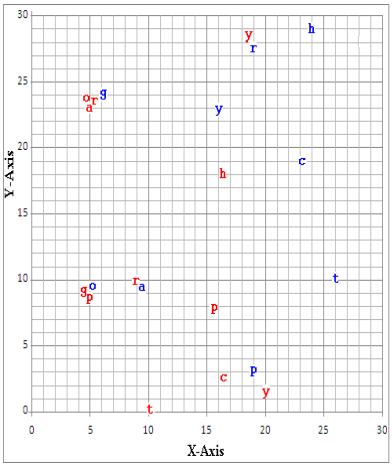

Figure 1. Mapping

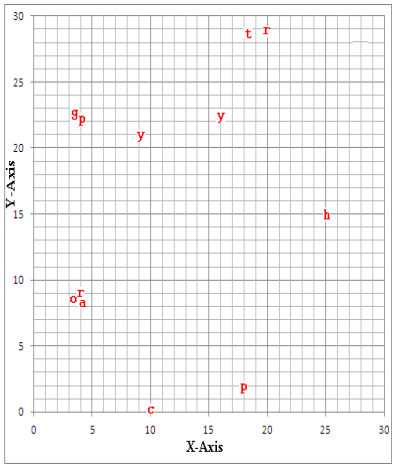

Figure 2. Encrypted

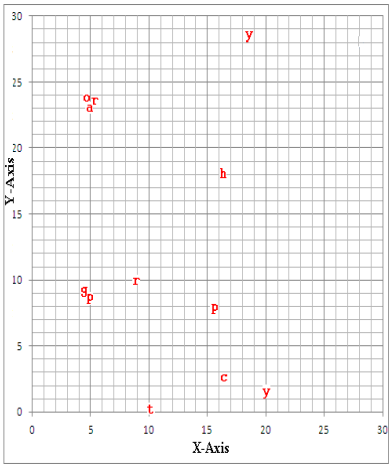

Figure 3. Decrypted

After decryption, the obtained points are stored into matrix Q of 3 × 4. This encoded matrix is again decoded using the inverse of A as:

$$M= A^{-1}Q=\begin{pmatrix} -57 & 5 & -46 \\ -11 & 1 & -9 \\ 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} Q_1 & Q_2 & Q_3 & Q_4 \\ Q_5 & Q_6 & Q_7 & Q_8 \\ Q_9 & Q_{10} & Q_{11} & Q_{12} \end{pmatrix}$$

Then, reverses the embedding to get back the message "cryptography".

Results of this mapping method for another string is shown in Table 3. The graphically representations of this string are shown in Figure 4, Figure 5 and Figure 6.

Table 3. Mapping, encrypted and decrypted points for "decryption".

Character	Point Pi	Mapping Points	Encrypted Points	Decrypted Points (Qi)
d	(4, 22)	(4, 22)	((27, 10),(6,7))	(4, 22)
e	(25, 16)	(6, 7)	((27, 10),(19,3))	(6, 4)
c	(23, 19)	(25, 15)	((27, 10),(19,28))	(25, 15)
r	(19, 28)	(6, 7)	((27, 10),(19,3))	(6, 7)
y	(16, 23)	(18, 2)	((27, 10),(27,21))	(18, 2)
p	(19, 3)	(24, 2)	((27, 10),(5,9))	(24, 2)
t	(26,10)	(20, 2)	((27, 10),(9,21))	(20, 2)
i	(16, 8)	(25, 15)	((27, 10),(19,28))	(25, 15)
o	(5, 9)	(22, 22)	((27, 10),(0,1))	(22, 22)
n	(26, 21)	(27, 21)	((27, 10),(20,2))	(27, 21)
Space	Ω	(25, 16)	((27,10),(17,13))	(25, 16)
Space	Ω	(6, 24)	((27, 10),(4,9))	(6, 24)

From the below tables (Table 2, Table 3), we observe that the common letters ‘c’, ‘r’, ‘y’, ‘p’, ‘t’ and ‘o’ are mapped onto the different x-y coordinates of the curve as illustrated in the figures. Then, for an intruder it would be very difficult to guess on which points the alphanumeric characters are mapped. Further, it is also difficult to guess which particular character is mapped to which point on the elliptic curve. Also, the good choice of non singular matrix and elliptic curve avoid the regularity in the resultant ciphertext. From the below table we observe that the point P_i can not derive from the mapping point Q_i, because ECDLP is difficult. It is thus concluded that the proposed mapping method can strengthens the elliptic curve cryptosystem.

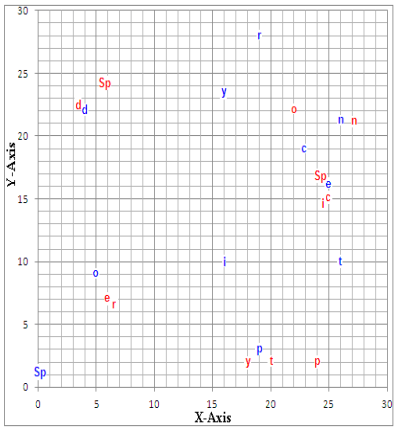

Figure 4. Mapping

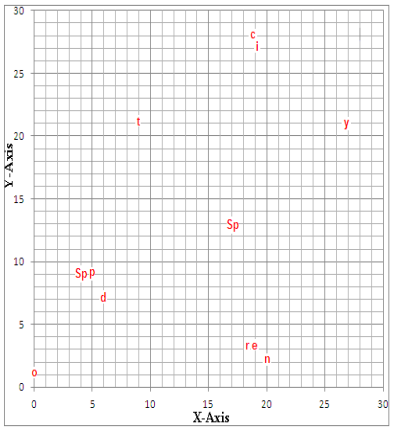

Figure 5. Encrypted

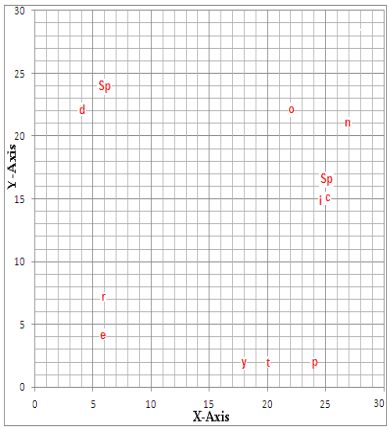

Figure 6. Decrypted

4. CONCLUSION

In this paper, we have constructed a new method of mapping alphanumeric characters to an EC points by using a non-singular matrix. The mapping points are encrypted and decrypted using ECC technique. Our results indicate that the mapping method avoids the regularity in the resultant cipher text which is transformed from plaintext matrix and hence improves the difficulty of decrypting. i.e, for an intruder it would be very difficult to guess on which points the alpha-numeric characters are mapped. It is thus concluded that the proposed mapping method can strengthens the system, guarantee the confidentiality of messages and provide better performance in this regard.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the paper.

REFERENCES

[1] B. Vellaikannan, V. Mohan and V. Gnanaraj, "The Role of Eigen Values and Eigen Vectors in Coding Theory", *European Journal of Scientific Research*, Vol.59 No.1, pp.85-92, 2011.
[2] Vatsa B.S, Suchi Vatsa, "Theory of Matrices, " Third edition, New Age international , India 2010.
[3] N. Koblitz. "Elliptic Curve Cryptosystems, " *Mathematics of Computation*, Vol. 48, No. 177, pp. 203-209, 1987.
[4] V. S. Miller. "Use of Elliptic Curves in Cryptography, " *Advances in Cryptology CRYPTO85*, pp. 417-426, 1986.
[5] R.L. Rivest, A. Shamir, and L.M. Adleman, Method for Obtaining Digital Signatures and Public-key Cryptosystems ", Communications of the ACM,Volume 21, pp 120-126, 1978.
[6] S. Arita, "Weil descent of elliptic curves over finite fields of characteristic three", Advances in Cryptology-Asiacrypt 2000, *Lecture Notes in Computer Science*, Vol.1976, *Springer-Verlag*, 248-259, 2000.
[7] Brian King, "Mapping an Arbitrary Message to an Elliptic Curve when Defined over GF(2^n) ", *International Journal of Network Security*, Vol.8, No.2, pp.169-176, 2009.
[8] Megha Kolhekar, Anita Jadhav, "Implementation of elliptic curve cryptography on text and image", *International Journal of Enterprise Computing and Business Systems,* Vol. 1, Issue 2, 2011.
[9] F.Amounas, E.H. El Kinani and A. Chillali, "An application of discrete algorithms in asymmetric cryptography", *International Mathematical Forum*, Vol. 6, No. 49, pp.2409-2418, 2011.
[10] F.Amounas and E.H. El Kinani, "Cryptography with Elliptic Curve Using Tifinagh Characters", *Journal of Mathematics and System Science* Vol.2, No.2, pp.139-144, 2012.
[11] S. Maria Celestin Vigila , K. Muneeswaran "Implementation of Text based Cryptosystem using Elliptic Curve Cryptography", *IEEE*, pp. 82-85, 2009.
[12] Padma Bh, D.Chandravathi, P.Prapoorna Roja, "Encoding and Decoding of a message in the Implementation of Elliptic Curve Cryptography uing Koblitz Method", *International Journal on Computer Science and Engineering*, pp. 1904-1907, 2010.
[13] H. Lange and W. Ruppert, "Addition laws on elliptic curves in arbitrary characteristics, " *Journal of Algebra*, Vol.107(1), pp.106-116, 1987.
[14] T.Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms". *IEEE, Transactions on Information Theory*, Vol.31, pp.473- 481, 1985.

BIOGRAPHY OF AUTHORS

EL HASSAN EL KINANI received the Ph.D in mathematical physics in 1999 from Mohamed V University Rabat Morocco. He is full professor at department of mathematics in Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco. He is interested in classical and quantum cryptography.

E-mail: elkinani_67@yahoo.com

FATIMA AMOUNAS received the DESS (diploma of high special study) degree in informatic in 2002 from Sidi Mohamed Ben Abdellah University, Faculty of Sciences Dhar El Mehrez, Fès Morocco. She is currently a Ph.D student in University Moulay Ismaïl, Faculty of Sciences and Technics, Errachidia, Morocco. Her research interests include elliptic curve and cryptography.

E-mail: F_amounas@yahoo.fr