International Journal of Information & Network Security (IJINS)
Vol.2, No.1, February 2013, pp. 43~53
ISSN: 2089-3299

Construction Efficiency of the Elliptic Curve Cryptosystem using Code Computing for Amazigh Alphabet

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 Sept 01th, 2012
Revised Sept 26th, 2012
Accepted Oct 22th, 2012

Keyword:

Elliptic Curve Cryptography,
Tifinagh Characters,
Code Computing,
Encryption, Decryption,
Circular Queue.

ABSTRACT

This paper puts forward a safe mechanism of data transmission to tackle the security problem of information which is transmitted in Internet. A new secure scheme based on matrix scrambling using code computing on elliptic curve has been proposed here. We define two operations used to scramble code matrix for Tifinagh characters. Hence, the proposed algorithm combines and conjures up the features of matrix with code computing on elliptic curve of circular queue. It is shown that the high performance of this technique is conditioned by the use of the coded key. Our scheme is secure against most of the current attacking mechanisms. The steps of the implementation of our algorithm are also investigated.

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

Information security has become a critical aspect of 21st century's computing systems. In this era, with the rapid growth of internet, security of information has become a necessity. Due to this, modern day researches are working on different kind of encryption and decryption for transferring data over internet [1]. There have been several techniques developed for encryption/decryption of the information over the years.

In the last decade the application of the elliptic curves in cryptography have been attracting increased attention of many authors [see e.g [2, 3]] because they have opened a wealth possibilities in terms of security. The research indicates that the security of 160 bits's(210bits's) elliptic curve key equals to the security of 1024 bit's (2048 bit's) RSA key[4].

In our previous work [5], we provide an example of the public-key cryptosystem based on ECC mechanism and the implementation of elliptic curve cryptosystem using Tifinagh characters [6]. Further, we provide a new method to secure the output of ECC cryptosystem [7, 8]. In [9], we have constructed a new method of mapping alphanumeric characters to an EC points by using a non-singular matrix. In fact, the transformation of the message into affine points is explained. A transformed character is encrypted by ECC technique. In [10] our idea is based on matrix scrambling technique on elliptic curve.

In this paper, we define novel method of scrambling based on code computing. More precisely, we discusse a new technique of encrypting data based on matrix scrambling method which is based on two operations: code addition and code substraction. These operations utilized to scramble the code matrix. More precisely, the proposed algorithm is a new technique of encryption data which enables good diffusion and is having a unique technique of decrypting it back to the plaintext and is easy to implement using a code substraction operation.

The rest of this paper is organized as follows: we start with some basics notions on elliptic curve over finite field Fp. Section 3 presents an overview about the Amazigh language. In section 4, we shall propose a new secure technique for Tifinagh characters using code computing on elliptic curve. We also explain in detail the implemention of our algorithm. The security analysis of the proposed scheme will be discussed in section 5. Finally, the concluding remarks will be in the last section.

2. BASIC THEORY OF ELLIPTIC CURVE

In this section, we introduce briefly some basics notions connected with elliptic curves. For more details on the theory of elliptic curves, we refer interested reader to [11, 12, 13].

An elliptic curve E over a finite field Fp is defined by the parameters α, $\beta \in F_p$ (α, β satisfy the relation $4\alpha^3+27\beta^2 \neq 0$), consists of the set of points (x, y), satisfying the equation:

$$y^2 = x^3 + \alpha x + \beta \qquad (1)$$

The set of points on E (Fp) also include point, which is the point at infinity and which is the identity element under addition. The addition operator is defined over E (Fp) and it can be seen that E (Fp) forms an abelian group. The addition and doubling of points rule is explained in many references (see e.g [14]).

3. THE AMAZIGH LANGUAGE

The Amazigh alphabet which is called Tifinagh-IRCAM, adopted by the Royal Institute of the Amazigh Culture, was officially recognized by the International Organization of Standardization (ISO) as the basic multilingual plan [15]. Tifinagh is encoded in the Unicode range U+2D30 to U+2D7F. The Figure 1 represents the repertoire of Tifinagh which is recognized and used in Morocco with their correspondents in Latin characters.

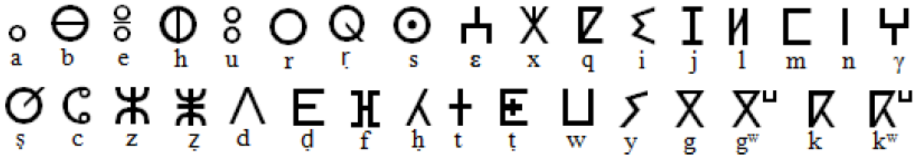
a b e h u r ṛ s ɛ x q i j l m n γ
ṣ c z ẓ d ḍ f ḥ t ṭ w y g gʷ k kʷ

Figure.1 Tifinaghe Characters Adopted by IRCAM with their Correspondents in Latin Characters.

4. MAIN RESULTS

In this section, we provide a new method of encrypting/decrypting data based on elliptic curve using code computing of circular queue. First, we considere an elliptic curve E over the finite field Fp where p is a prime. E is the set of points (x, y) satisfying the following equation E: $y^2 = x^3 + \alpha x + \beta$ where α, β are integer modulo p, satisfying: $4\alpha^3 + 27\beta^2 \neq 0$ mod p, and include an point Ω called point at infinity. Once the defining EC is know, we can select a base point called P and N_1 is order of P.

a. The Proposed Method Description

1) Code Computing on elliptic curve

In this paper, the code computing on elliptic curve is computed by defining two operation for the code 00, 01,10, 11, as shown in Table.1 and Table.2. Code subtraction is the reverse operation of code addition. These operations are utilized to scramble the code matrix.

Table.1. Code Addition operation

+	**00**	**01**	**10**	**11**
00	01	10	11	00
01	10	11	00	01
10	11	00	01	10
11	00	01	10	11

Table.2. Code substraction operation

+	**00**	**01**	**10**	**11**
00	11	10	01	00
01	00	11	10	01
10	01	00	11	10
11	10	01	00	11

Therefore, the coding of points of elliptic curve can be expressed with these codes.

2) Encryption

In this cryptosystem, the plaintext is arranged into code matrix of n×m. Then, its transpose is taken. This results in a matrix of m×n. Input an integer parameter N, as the count of operations, say the time of code addition operation we made to matrix. Random() function is used to generate random positive integer noted k. Therefore, we apply doubling and addition operations to compute kP_B. Its binary form is treated. Deponding on the binary bit from the Least Significant Bit(LSB) to Most Significant Bit (MSB), the choice to select rows or columns is made.

In the case of row, two rows r_1 and r_2 are selected randomly from the code matrix, similarly two random values of columns c_1 and c_2 are selected to determine the range of rows on which transformation has to be performed. To perform transformation on row: deponding the binary bit selected, circular code addition is made. Similarly for column transformation. The entire process is repeated N number of times. For each transformation, a sub key is constructed and recorded in a key file. The sub key is 5 tuple and is given as follows:

Sub_key=(Tr, α_1, α_2, β_1, β_2) with

- Tr: Transformation of row (R) or column (C).
- α_1, α_2: Two rows or columns selected.
- β_1, β_2: min and max values of range for two selected.

In the case of row transformation sub key is recorded as: $R(r_1/r_2/m_1/m_2)$.
In the case of column transformation sub key is recorded as: $C(c_1/c_2/m_1/m_2)$.

The encryption process is shown in figure (Figure 2). In our case, the plaintext is transformed on points of elliptic curve as is the embedding system $M \rightarrow P_M$ and the corresponding sequence is coded by using the code 00, 01, 10 and 11. The obtained sequence is arranged into a Bi-directional circular queue data structure [16]. The process of encryption is done in ten steps as following:

Step 1. Transposing the obtained data structure. Then, she can obtain a code matrix of m ×n noted U = ($u_{i,j}$).

$$U=\begin{pmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,n} \\ u_{2,1} & u_{2,2} & \cdots & u_{2,n} \\ & . & . & \\ & . & . & \\ & . & . & \\ u_{m,1} & u_{m,2} & \cdots & u_{m,n} \end{pmatrix}$$

Step 2. Using Bob's public key P_B, she can create a point K such that: $K = kP_B$ with k is a her own private key (k remains secret).

Step 3. Input an integer parameter N, which represents no. of rounds of operations to perform. Depending on N, N transformations are applied on the matrix.

Step 4. The binary form of key K (Step 2) provides some sort of strength to the encryption. After choosing k, binary value of K is calculated and placed in a vector B.

Step 5. Let t = Digit(B_i), where 'i' is bit position, t value is either 0 or 1, which provides a way of deciding either to perform row or column transformation. If t = 0, then T_r = R. is performed i.e. row transformation operations are applied on the matrix as given below. If t = 1, then Tr = C i.e. column transformation operations are applied on the matrix as given below (Figure 2).

Step 6. Using code addition operation for the range of two elements selected.

Step 7. Check whether binary sequence in vector t is completed. If it is completed, again start from first digit in the binary sequence of b (LSB →MSB). Repeat steps 5 and 6 for N no of times.

Step 8. Record all the sub keys sequentially in a key file which becomes the key file.
The key file should be maintained secret.

Step 9. Encoding K with codes 00, 01, 10 and 11. Then Applying code addition operation of Column vectors noted Y_i and K as:

$$C_i = Y_i + K \text{ with } i = 1, 2, ...,m$$

Step 10. Compute kP and decode each column of matrix M Therefore, the ciphertext is:

$$C=(kP,C_1,C_2, ..., C_m).$$

Now, the cipher text is sent along with the key file to the receiver.

3. *Decryption*

The decryption process is done by reading the operations in the key file in reverse order and applying code substraction operation on the matrix, which contains cipher text as to get plain text. i-e, the process is done by reversing the operations done in the encryption process. To decrypt the ciphertext according to inverse operations of the encryption steps, code addition operation is replaced by code substraction.

The number of sub_key's equal to the 'N' no of operations. The cipher text is arranged into a matrix of the same order in the encryption as m and n. The steps of the decryption process explained in brief as follows:

Step 1. Extract a first group of 2m bits in the received message and get a cooresponding point noted P_1 = kP. Then he compute K = aP_1 = akP = kP_B with a is his own private key.

Step 2. Separate the remaining sequence in groups of 2m bits noted C_i. After encoding each group with codes, then using code substraction operation to Compute: $Y_i = C_i – K$.
Hence, the results vectors Y_i are stored into code matrix of m×n.

Step 3. The sub keys are decrypted one by one from the last sub key to the first sub key.

Step 4. For each sub key $T_r/ \alpha_1/ \alpha_2/ \beta_1/ \beta_2$ values are obtained whose terms are already explained in the encryption algorithm. Based on Tr value either R or C, code subtraction operation is performed on row or column.

Step 5. The process is done until the key file is completed and at the end of process matrix A contains the required original message i.e. plain text.

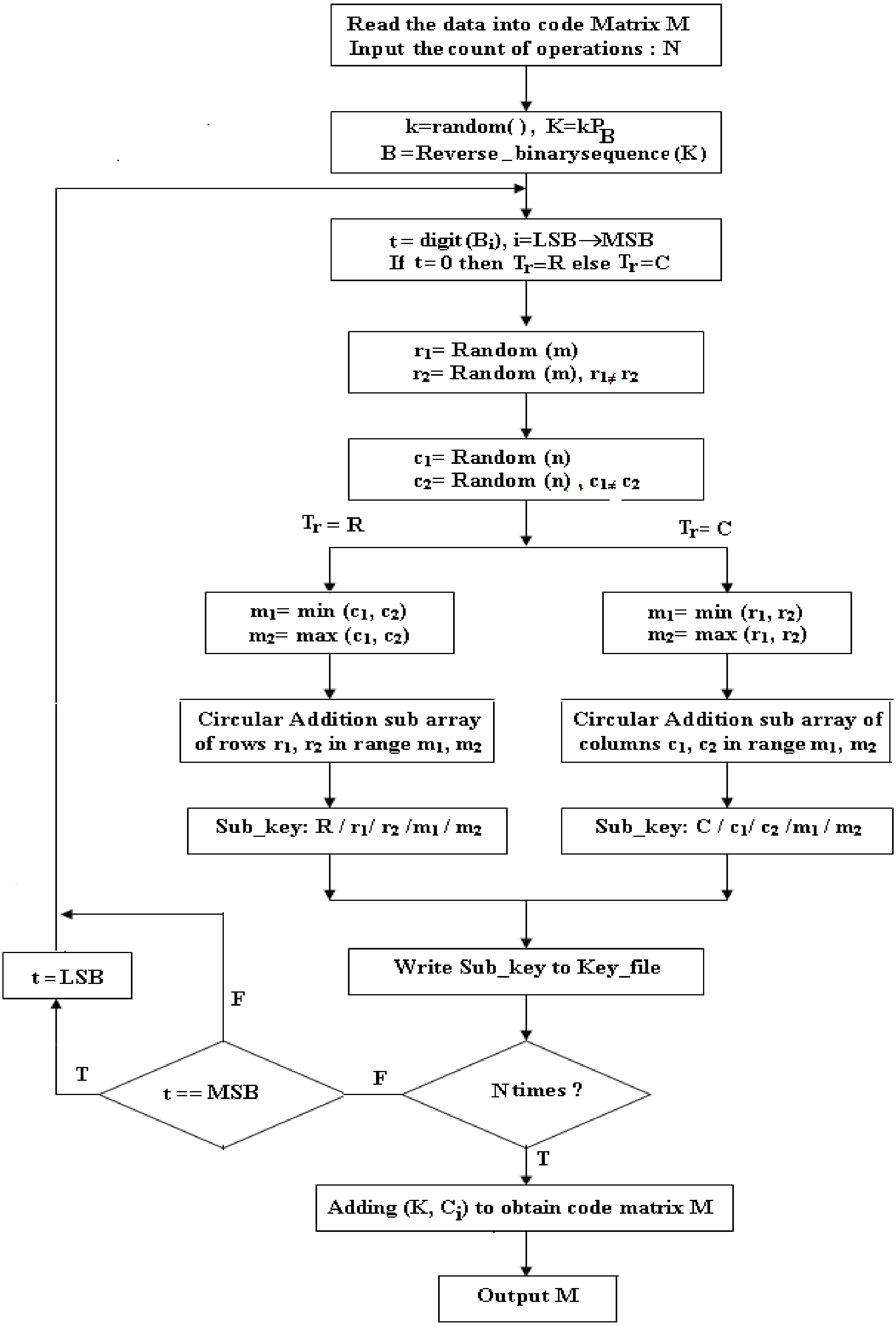
Read the data into code Matrix M
Input the count of operations : N
k=random( ), K=kP_B
B =Reverse_binarysequence (K)
t = digit (Bi), i=LSB→MSB
If t = 0 then Tr=R else Tr=C
r1= Random (m)
r2= Random (m), r1≠ r2
c1= Random (n)
c2= Random (n) , c1≠ c2
Tr = R
Tr= C
m1= min (c1, c2)
m2= max (c1, c2)
m1= min (r1, r2)
m2= max (r1, r2)
Circular Addition sub array of rows r1, r2 in range m1, m2
Circular Addition sub array of columns c1, c2 in range m1, m2
Sub_key: R / r1/ r2 /m1 / m2
Sub_key: C / c1/ c2 /m1 / m2
Write Sub_key to Key_file
t = LSB
F
T
t == MSB
F
N times ?
T
Adding (K, Ci) to obtain code matrix M
Output M

Figure.2 Encryption Algorithm

b. Implementation Details of the Proposed Algorithm

In this section, we show the details of our encryption algorithm by an example. The elliptic curve using here is given by the following equation:

$$y^2 = x^3 + 4x + 20[29]$$

The point on the elliptic curve is shown below in Figure 3.

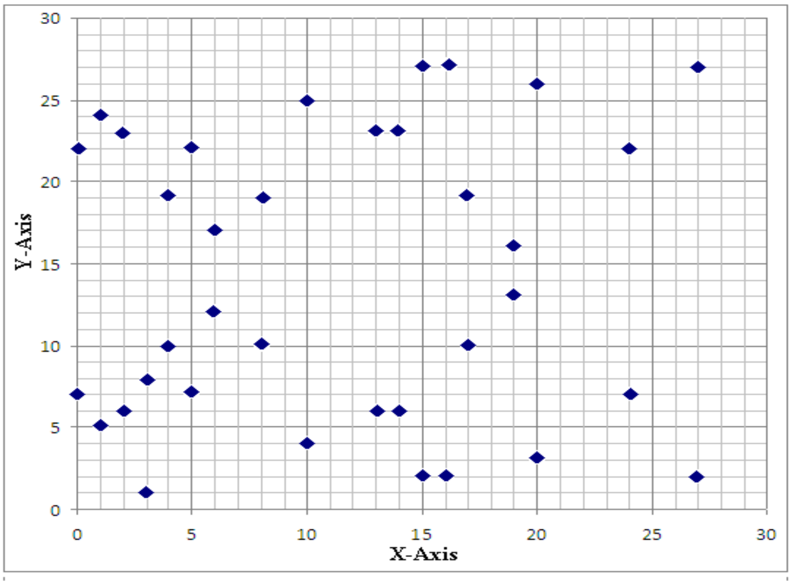

Figure 3. Set of points on elliptic curve $E_{29}(4,20)$

The base point P is selected as (1,5). Here the choosing curve contains 37 points with P is the point generator. In our case we use the Tifinagh characters (Tifinagh IRCAM) with some of the other symbols like ';', '(', ')' and space for illustration purpose only.
In our case we have k = 13, a = 29 , P_B=(8,19)

4.2.1) Case study of the Encryption Process

Suppose that Alice wants to encrypt and transmit a message M=" ⵜⴰⵏⵎⵉⵔⵜ" to Bob, first she converts all the text characters of the message into the points on the elliptic curve using the agreed upon code table given in table 3.

ⴰ (1, 5)	ⴱ (4, 19)	ⴼ (20, 3)	ⵟ (15, 27)	ⵄ (6, 12)
ⵔ (17, 19)	ⵕ (24, 22)	ⵙ (8, 10)	ⵀ (14, 23)	ⵅ (13, 23)
ⵚ (10, 25)	ⵉ (19, 13)	ⵊ (16, 27)	ⵍ (5, 22)	ⵎ (3, 1)
ⵏ (0, 22)	ⵖ (27, 2)	ⵇ (2, 23)	ⵛ (2, 6)	ⵥ (27, 27)
ⵣ (0, 7)	ⴷ (3, 8)	ⴻ (5, 7)	ⵃ (16, 2)	ⵡ (19, 16)
ⵜ (10, 4)	ⴹ (13, 6)	ⵓ (14, 6)	ⵢ (8, 19)	ⴳ (24, 7)
ⴳⵯ (17, 10)	ⴽ (6, 17)	ⴽⵯ (15, 2)	; (20, 26)	((4, 10)
) (1, 24)	Ω Space			

Table 3. Tifinaghe Characters and the coorresponding points on EC.

Let us set m = 5, n = 7, N = 6, B = 0110100011. In vector B only 10 digits of the binary sequence is considered in the example. After the plaintext is set into code matrix U, the layout of the matrix is shown as:

01	00	00	00	10	10	01
01	00	00	01	01	00	01
00	10	01	10	10	11	00
01	01	01	00	11	00	01
00	01	10	01	01	11	00

Layout of the Plaintext

After N operations and based on binary values in B, sub keys recorded in the key file is given as followed:

C /1/2/1/3, C /5/1/0/3, R /2/3/0/6,
R /1/4/0/4, R /0/1/1/3, C /2/4/1/4

Then, she does the following:

- Alice tranform the plaintext into points on elliptic curve and the corresponding sequence is coded with 00, 01, 10 and 11.

ⵜⴰⵏⵎⵉⵔⵜ ⇒ (10,4), (1,5), (0,22), (3,1), (19,13), (17,19), (10,4)

- Creating the code matrix of m×n noted U. Hence, the process of disordering or scrambling the matrix elements based on sub keys is explained as following:

01	00	00	00	10	10	01
01	00	00	01	01	00	01
00	10	01	10	10	11	00
01	01	01	00	11	00	01
00	01	10	01	01	11	00

Plaintext

01	00	00	00	10	10	01
01	11	10	01	01	00	01
00	00	11	10	10	11	00
01	01	00	00	11	00	01
00	01	10	01	01	11	00

C/1/2/1/3

01	00	00	00	10	11	01
01	00	10	01	01	00	01
00	10	11	10	10	00	00
01	10	00	00	11	00	01
00	01	10	01	01	11	00

C/5/1/0/3

01	00	00	00	10	11	01
01	00	10	01	01	00	01
11	10	10	01	11	01	00
00	11	01	00	00	10	10
00	01	10	01	01	11	00

R/2/3/0/6

01	00	00	00	10	11	01
10	11	00	11	00	00	01
11	10	10	01	11	01	00
00	11	01	00	00	10	10
10	00	00	11	00	11	00

R/1/4/0/4

01	01	01	10	10	11	01
10	00	00	00	00	00	01
11	10	10	01	11	01	00
00	11	01	00	00	10	10
10	00	00	11	00	11	00

R/0/1/1/3

01	01	01	10	10	11	01
10	00	11	00	00	00	01
11	10	00	01	00	01	00
00	11	10	00	01	10	10
10	00	00	11	01	11	00

C/2/4/1/4

- After encoding K with codes 00, 01, 10 and 11, we obtain [11 00 01 01 10]. Applying code addition operation to compute $C_i = Y_i + K$ with i = 1, 2, ..., m. Therefore,

01	01	01	10	10	11	01
11	01	00	01	01	01	10
01	00	10	11	10	11	10
10	01	00	10	11	00	00
01	11	11	10	00	10	11

- After decode each C_i and calculate kP, the cipher text is given as following:

1000011011010101101011011101000101011001001011101110100100101100000 01111110001011
Now, the cipher text is sent along with the key file to the receiver.

4.2.2) Case study of the Decryption Process

When Bob received the above series of bits, he does a steps as following:

- Extract a first group of 2m bits in the received message and get a cooresponding point noted $P_1 = kP = (16, 27)$. Bob compute: $K = aP_1 = akP = (24, 22)$ with 'a' is his own private key. Hence, the coded key K is represented by [11 00 01 01 10].
- Separate the remaining sequence in groups of 2m bits. Each group is coded with 00, 01, 10 and 11, noted C_i. The layout of the cipher text after placing in matrix A of order m and n, which have vectors C_i is given as followed:

01	01	01	10	10	11	01
11	01	00	01	01	01	10
01	00	10	11	10	11	10
10	01	00	10	11	00	00
01	11	11	10	00	10	11

- Using the code subtraction, to compute $Y_i = C_i - K$ with i = 1, 2, ..., m. Then, we get the code matrix as:

01	01	01	10	10	11	01
10	00	11	00	00	00	01
11	10	00	01	00	01	00
00	11	10	00	01	10	10
10	00	00	11	01	11	00

- The next stage of decryption is done by reading the sub keys in key file in reverse order and sub keys in reverse order is given as:

C /2/4/1/4, R /0/1/1/3, R /1/4/0/4
R /2/3/0/6, C /5/1/0/3, C /1/2/1/3

- The remaining steps of the decryption are given as follows:

01	01	01	10	10	11	01
10	00	11	00	00	00	01
11	10	00	01	00	01	00
00	11	10	00	01	10	10
10	00	00	11	01	11	00

Ciphertext

01	01	01	10	10	11	01
10	00	00	00	00	00	01
11	10	10	01	11	01	00
00	11	01	00	00	10	10
10	00	00	11	00	11	00

C/2/4/1/4

01	00	00	00	10	11	01
10	11	00	11	00	00	01
11	10	10	01	11	01	00
00	11	01	00	00	10	10
10	00	00	11	00	11	00

R/0/1/1/3

01	00	00	00	10	11	01
01	00	10	01	01	00	01
11	10	10	01	11	01	00
00	11	01	00	00	10	10
00	01	10	01	01	11	00

R/1/4/0/4

01	00	00	00	10	11	01
01	00	10	01	01	00	01
00	10	11	10	10	00	00
01	10	00	00	11	00	01
00	01	10	01	01	11	00

R/2/3/0/6

01	00	00	00	10	10	01
01	11	10	01	01	00	01
00	00	11	10	10	11	00
01	01	00	00	11	00	01
00	01	10	01	01	11	00

C/5/1/0/3

01	00	00	00	10	10	01
01	00	00	01	01	00	01
00	10	01	10	10	11	00
01	01	01	00	11	00	01
00	01	10	01	01	11	00

C/1/2/1/3

- After transposing of the result matrix, we get a code matrix of n × m. Then, extract and decode it to obtain the sequence as:
  010000001010010100000101000100100110101100010100011000100011001011100
- Separate the sequence in group of 2m bits.

After decoding each group, and reverse the imbedding, he can obtain the plaintext =" ⵜⴰⵏⵎⵉⵔⵜ ".

5. SECURITY ANALYSIS

Since the encrypted message, the public key and the domain parameters [17] of elliptic curve are open to the public. The attackers may attempt to compute the private key from the publickey in order to decrypt the encrypted message. The security of the proposed scheme therefore relies on the coded sequence can be obtained from the knowledge of codes 00, 01, 10, 11 and the coded key. The only possibility of coding sequence arises when the attacker has the knowledge of the private key k of Alice. We have shown this attack is not possible in our proposed scheme, because ECDLP (Elliptic Curve Digital Signature Algorithm) to obtain Alice private key k is difficult. Also, the good choice of elliptic curve gives a better binary sequence. Then, the code computing on elliptic curve is combining with transposing to scramble the matrix in both directions row wise and column wise efficiently. So, the proposed scheme is more robust against most of the current attacking.

6. CONCLUSION

In this paper, the use of code computing firstly, secondly code addition operation with an point on elliptic curve (K), avoid the regularity in the resultant ciphertext which is transformed from plaintext matrix and hence improves the difficulty of decrypting. This paper indicates that the original message are completely scrambled by these operations. Therefore, our algorithm is a good candidate for the security of text and image. Finally, the steps of the implementation of this algorithm are explained.

REFERENCES

[1] Stallings, W. Cryptography and Network Security, (2003) Prentice Hall, 3rd Edition.

[2] V. S. Miller. Use of Elliptic Curves in Cryptography. *Advances in Cryptology CRYPTO'85*, pp. 417-426, 1986.

[3] N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, Vol. 48, No. 177, pp. 203-209, 1987.

[4] Zhu Yufei, Zhang Yajuan. Introduction to elliptic curve cryptosystem. Beijing: *Science press*, 10, 130 (in chinese), 2006.

[5] 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.

[6] 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.

[7] F.Amounas and E.H. El Kinani, ECC Encryption and Decryption with a Data Sequence, *Applied Mathematical Sciences*, Vol. 6, no. 101, 5039- 5047, 2012.

[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)*, Vol.1, No.3, pp. 216-222, 2012.

[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)*, Vol.1, No.2, pp. 54-59, 2012.

[10] F.Amounas and E.H. El Kinani, An Elliptic Curve Cryptography Based on Matrix Scrambling Method, *Proceedings of the JNS2*, pp 31-35, 2012.

[11] J. W. S. Cassels. Lectures on Elliptic Curves. (1991) Cambridge University Press.

[12] A. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, Vol. 61, No. 203, pp. 29-68, 1993.

[13] M. Saeki. Elliptic curve cryptosystems. M.Sc. thesis, School of Computer Science, McGill University, 1996.

[14] H. Lange and W. Ruppert, Addition laws on elliptic curves in arbitrary characteristics, *Journal of Algebra* , Vol.107(1),106-116, 1987.

[15] L. Zenkouar, L'écriture Amazighe Tifinaghe et Unicode, in Etudes et documents berbres. Paris (France). n 22, , pp. 175-192, 2004.

[16] W.W.Yan Weimin, Data Structure. (1996) Tsinghua University Press, Beijing.

[17] Cheng, Z., Simple tutorial on elliptic curve cryptosystem, ver.0.1 (2003), *School of Computing Science*, Mdx University London 2003 Conference.

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