International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Encryption of Data using Elliptic Curve over Circulant Matrices

Fatima Amounas
R. O. I. Group, Moulay Ismaïl University
Informatics Department
Faculty of Sciences and Technics
Box 509 Errachidia 52000, Morocco

EL Hassan EL Kinani
A. A. Group, Moulay Ismaïl University
Mathematical Department
Faculty of Sciences and Technics
Box 509 Errachidia 52000, Morocco

***Abstract* — In this paper, the properties of circulant matrices are combining with elliptic curve to provide an analogue of ElGamal cryptosystem for encrypting/decrypting process. More precisely, we establish an algorithm to generate data matrix based on elliptic curve, which is randomized by using traversing process. Then, we apply the encryption/decryption technique based on circulant matrices. In the present work the output of ECC algorithm is provided with circulant matrices. Our scheme is secure against most of the current attacking mechanisms. Further, this paper attemps to utilize the properties of circulant matrices in encryption and decryption process with more efficient. The steps of the implementation of our algorithm are also investigated.**

***Keywords* — Elliptic Curve Cryptography, Discrete Logarithm, Data Matrix, Circulant Matrices.**

I. INTRODUCTION

Many cryptographic algorithms have been proposed based on matrices including [1, 2, 3]. In the paper [2], the authors use circulant matrices to compute the trapdoor function. In [1, 2] described the public key cryptography using simple multiplication of matrices over a given commutative ring. Here we have to choose circulant matrix of rank m defined by the proposed algorithm. Then, we extended data Matrix generated such that rank of vectors is a prime. In fact, we propose a new method to transform a point on the elliptic curve to vectors and applying ECC technique with circulant matrices.

Two of the most popular groups used in the discrete logarithm problem are the group of units of a finite field and the group of rational points of an elliptic curve over a finite field. Recently, the group of circulant matrices offers the same security of a finite field of about same size with half the computational cost. In this paper, we denote the group of non-singular circulant matrices of size m by SC_m.

In our previous work, we have presented an example of the public-key cryptosystems based on ECC mechanism [4, 5, 6]. We have also proposed a new technique to secure the output of ECC cryptosystem [7,8]. Further, we have provided a new mapping method based on non-singular matrices [9]. Here, two algorithms are presented for mapping technique and encryption respectively.

The original message is transformed by using mapping method based on traversing operations. Then, we will extend this algorithm for ElGamal cryptosystem with circulant matrices. The proposed method has two levels of authenticated encryption. First, one is based on traversing of data Matrix and second one is applying it with circulant matrices for ECC technique. The proposed method provides high security in this regard.

Here we will formulate and discuss the algorithm in four sections. The first section starts with Definition of the circulant matrices and the discrete logarithm problem over circulant matrices. The second section deals with the pre-processing of data (traversing of the data). In the third section, we propose the ElGamal scheme with data traversing over circulant matrices. In the fourth section, an example is given to illustrate the working of the entire algorithm on the elliptic curve given by the Weirstrass equation: $y^2 = x^3 + x + 13$. The security Analysis of the proposed method is studied in 5. The paper is concluded in section 6.

II. CIRCULANT MATRICES

A. Definition (Circulant matrix C_m)

A (m×m) matrix over a field F is called a circulant matrix, if every row except the first row, is a right circular shift of the row above that. So a circulant matrix is defined by its first row.

A matrix is a two dimensional object, but a circulant matrix behaves like a one dimensional object, given by the first row or the first column.

We will denote a circulant matrix C of size m, with the first row $(a_0, a_1, \ldots, a_{m-1})$, by C = circ $(a_0, a_1, \ldots, a_{m-1})$.
For example: m = 5, a circulant matrix C (5×5) is:

$$C = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ a_4 & a_0 & a_1 & a_2 & a_3 \\ a_3 & a_4 & a_0 & a_1 & a_2 \\ a_2 & a_3 & a_4 & a_0 & a_1 \\ a_1 & a_2 & a_3 & a_4 & a_0 \end{pmatrix}$$

We will denote a SC_m the group of non-singular circulant matrices of size m over F_p.

B. PLD for circulant matrices over finite field

It was shown in [10] that if five conditions are satisfied, then the security of the discrete logarithm problem for circulant matrices of size m over F_p is the same as the discrete logarithm problem in F_p^{m-1}. In fact, the five conditions are:

1. The circulant matrix should have determinant 1.
2. The matrix C should have row-sum 1.
3. The integer m is a prime.
4. The polynomial χ_C /(x-1) is irreducible, where χ_C is the characteristic polynomial of C.
5. p is primitive mod m.

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Further, in [10] the authors study the discrete logarithm problem in group of nonsingular circulant matrices of size m with determinant 1. It is fairly straightforward to see that one can develop a Diffie-Hellman key exchange protocol or the ElGamal cryptosystem from this discrete logarithm problem.

In this work, we provide the ElGamal cryptosystem based on circulant matrices with a data Matrix generated.

III. Main Results

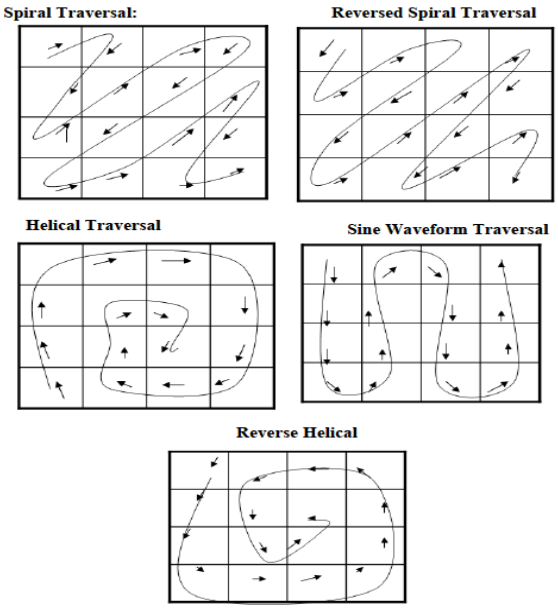
In this study an algorithm for ECC based on matrices will be proposed, which is structurally and functionally divided into two basic parts. The first part deals with the pre-processing of data (traversing of the data). The second part of the algorithm is based on circulant matrices which deal with the key generation and encryption /decryption processes. Now, we discuss the algorithms in greater details to explain its working and features.

A. Pre-processing of Data

This section will deal with the part of the algorithm that deals with the preprocessing of data i.e constructing a (m×m) matrix for the given data to be encrypted if necessary by using padding and this section can be explained in the following stage.

Traversing Data Matrix

This stage involves reading out of the data from the data matrix of order (m×m). This can be achieved in any of the following manners which are depicted through appropriate self-explanatory diagrams:



Since here there are five patterns, so there can be 5! possible sequences, which we denote by T_1, T_2, …, T_{120}. Suppose that the sequence represented above is T_1.

B. Proposed Developments of ECC based on Matrices

The proposed algorithm requires that we generate a data matrix traversal on elliptic curve noted B. The procedure is show in algorithm (1). Then, the result of this procedure is applied in the ECC encryption process.

Algorithm (1) Data traversing

Input: P a base point, N=order (P) and $P_i \in EC$,

Output: B

Step1. Transform the alphanumeric characters into points on elliptic curve (refer to Appendix) as:

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

We consider M the original message of length n.

Step 2. Represent its binary form to stream of digits as well as: 00 ➔0, 01 ➔1, 10 ➔2 and 11 ➔3.

Let m be a number of digits. If n > m then the points have been padded with O which represent space.

This message is decomposed in blocs of length m.

Step 3. Creating the matrix A of (m × m) with entries are the obtained digits (Step 2).

Step 4. Using section (A), spiral, reversed spiral, Helical, sine waveform Reverse helical the matrix A can be traversed with T_1. Then we get the data matrix $B=(b_{i,j})$.

Return B.

Proposed Method Description

Suppose Alice wants to send a message to Bob. They first choose a finite field F_p where p is a prime, an elliptic curve E, defined over that field and a base point P with order N.

- *Initial phase*

1. Plaintext M is transforming into point of elliptic curve noted P_M.
2. Generates a data matrix traversal (section A).
3. Chooses a circulant matrix $C \in SC_m$. The rank of a matrix C is defined in algorithm (1).

- *Encryption*

To encrypt a message M Alice does the following:

Step 1. Bob chooses a random integer 'a' and publishes C^a with $C \in SC_m$.

If $C^a = C$ or $C^a = Id$ (Identity) then return to step1.

Step 2. Alice chooses her own random integer ℓ and Computes C^ℓ and $C^{a\ell}$.

If $C^\ell = C$ or $C^\ell = Id$ (Identity) then return to step2.

Similarly for $C^{a\ell}$.

Step 3. V denotes the first row of C^ℓ. Therefore, the ciphertext is:

$$(D_1, D_2) = (V, BC^{a\ell}).$$

With B is the traversing data matrix of plaintext (Algorithm 1).

Hence, the obtained sequence is transmitted to Bob.

- *Decryption*

To decrypt the message M, Bob gets the Alice's parameters and public key.

Then, Bob does the following:

Step 1. After extract the first part of the pair noted V, create a circulant matrix with the first row V. This matrix represents C^ℓ.

Step 2. Computes $C^{-\ell a}$ from the obtained matrix of step 1.

Step 3. Extracts the remaining sequence and stored into data matrix of (m×m).

Then, compute $(B.C^{a\ell}).C^{-\ell a} = B$.

Step 4. Reverse the process, i.e. reverse the operations done in the encryption process (Algorithm1) to get back data matrix A.

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

We have to find data matrix B_1 such that: B=Reverse_Helical (B_1). It is similar for others operations. The result data matrix represents A.

Step 5. Converts data sequence A to binary form: 0 ➔00, 1 ➔01, 2 ➔10 and 3 ➔11.

Step 6. Transforms the obtained sequence to points on EC, and reverses the embedding to get back the message M.

IV. Implementation Details of our Algorithm

In our case, the elliptic curve E is given by the Weirstrass equation:

$$y^2 = x^3 + x + 13 \bmod 31 \quad (1)$$

The set of all points on elliptic curve is shown below in Fig.1.

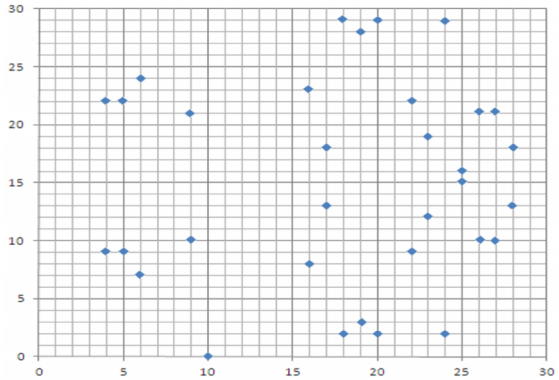


Fig.1. The points on elliptic curve $E_{31}(1,13)$

The above curve contains 34 points with P(9,10) is the point generator. It is the point which represents the letter 'a', as well as 2P represents the letter 'b',..., 34P 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.

Suppose that Alice wants to encrypt and transmit a message M="hello" to Bob, she does the following:

A. Generating of traversing data Matrix

- Transforms the above message into a stream of points as follow:
  {(24, 29), (25, 16), (28,13), (28, 13), (5, 9)}
- Converts its binary form to sequence of digits as well as: 00 ➔0, 01 ➔1, 10 ➔2 and 11 ➔3.
  [3 0 1 3 1 3 0 3 0 0 3 2 0 3 1 3 2 0 3 1 0 2 2 2 1]
- Construct the message matrix A with this stream of numerals as:

$$A = \begin{pmatrix} 3 & 0 & 1 & 3 & 1 \\ 3 & 0 & 3 & 0 & 0 \\ 3 & 2 & 0 & 3 & 1 \\ 3 & 2 & 0 & 3 & 1 \\ 0 & 2 & 2 & 2 & 1 \end{pmatrix}$$

- Using a list L as mentioned in section (A), we obtain data matrix as follow:

$$B = \begin{pmatrix} 3 & 2 & 0 & 3 & 3 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 3 \\ 1 & 2 & 2 & 3 & 3 \\ 3 & 2 & 1 & 0 & 1 \end{pmatrix}$$

B. Crypting/Decrypting

Now the encryption-decryption process is illustrated by using the plaintext "hello" as below:

Hence we shall assume that $\ell = 13$, a = 108 and a circulant matrix C such that:

$$C = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Therefore:

$$C^{\ell} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

and

$$C^{a\ell} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Now, the plaintext "hello" is arranged into data matrix B by applying Algorithm (1) as:

$$B = \begin{pmatrix} 3 & 2 & 0 & 3 & 3 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 3 \\ 1 & 2 & 2 & 3 & 3 \\ 3 & 2 & 1 & 0 & 1 \end{pmatrix}$$

Therefore, encrypted version of the message is:

$$(D_1, D_2) = (V, BC^{a\ell})$$

With D_1 = V denote the first row of C^{ℓ}. D_2 is given as:

$$D_2 = \begin{pmatrix} 3 & 3 & 2 & 0 & 3 \\ 2 & 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 3 & 0 \\ 3 & 1 & 0 & 2 & 3 \\ 1 & 3 & 2 & 1 & 0 \end{pmatrix}$$

The recovery of ciphertext is done as follows:

- Extract the first part D1 and stored into vector V.
  V =(0 0 0 0 1) ➔ C =circ (0, 0, 0, 0, 1).
- Creating a circulant matrix of the first row V. Its denote C^{ℓ}.
- Compute $C^{-\ell a}$ from the result matrix C^{ℓ} as:

$$C^{-\ell a} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

- Arrange the remaining data into matrix of size (m×m) and compute:
  $$D_2.C^{-\ell a} = B.C^{a\ell}.C^{-\ell a} = B.$$
  Then, we have to find data matrix B_1 such that: B=Reverse_Helical (B_1). It is similar for others operations. The result data matrix represents A.
- Decoding each row of A such that: 0➔00, 1➔01, 2➔10 and 3➔11. Then, separate the result sequence in groups, which represents a point P_i on EC.

Now reverses the embedding to get back the message. Thus we retrieve the plaintext "hello".

V. Security Analysis

The proposed cryptosystem provides security in two levels. First level, the random number 'm' and the matrix C are used for encryption of the plaintext block. Each character is coded into point on elliptic curve and stored into matrix A of (m×m). The obtained matrix is randomized by using traversing process. the second level, the security is based on the difficulty of the discrete logarithm problem in group of circulant matrices, i.e. we give the output of ElGamal cryptosystem with a circulant matrix. Here, the proposed method is compared to Hill cipher [11,12] to find out our algorithm performance.

The main limitation with Hill Cipher is that if sufficient elements of plain text and Cipher text are obtained, the key can be retrieved. Thus the Hill Cipher prone to known Plain text attack. In the proposed scheme, the same character is mapped into different blocks. Further, it is also difficult to guess which particular character is mapped to which point on the Elliptic Curve.

Thus the given model is free from plain text attack and free from chosen Cipher text attack. Also, the good choice of circulant matrix avoids the regularity in the resultant cipher text.

VI. Conclusion

This paper proposes a circulant matrix based asymmetric algorithm using elliptic curve. Whose strength is based on the solving of PLD for circulant matrices over finite field. More precisely, we establish an algorithm to generate a data matrix using traversing process. The transformation of point into data matrix is a new innovation of this paper. Then, we provide ElGamal cryptosystem based on circulant matrices. Further, the steps of the implementation of our cryptosystem on the elliptic curve E: $y^2 = x^3 + x + 13$ are explained. We like to point out that the use of traversing process and circulant matrices will provide better performance in this regard.

Finally, the proposed cryptosystem can be enhanced further by using more complex techniques in data matrix as well as using the genetic functions in a more detailed and complicated way.

Appendix

Point	Symbol	Corresponding code
(9,10)	a	0100101010
(18, 29)	b	1001011101
(23, 19)	c	1011110011
(4, 22)	d	0010010110
(25, 16)	e	1100110000
(17, 18)	f	1000110010
(6, 24)	g	0010011000
(24, 29)	h	1100011101
(16, 8)	i	1000001000
(20, 2)	j	1010000010
(22, 22)	k	1011010110
(28, 13)	l	1110001101
(27, 10)	m	1101101010
(26, 21)	n	1101010101
(5, 9)	o	0010101001
(19, 3)	p	1001100011
(10, 0)	q	0101000000
(19, 28)	r	1001111100
(5, 22)	s	0010110110
(26, 10)	t	1101001010
(27, 21)	u	1101110101
(28, 18)	v	1110010010
(22, 9)	w	1011001001
(20,29)	x	1010011101
(16,23)	y	1000010111
(24,2)	z	1100000010
(6,7)	!	0011000111
(17,13)	,	1000101101
(25,15)	;	1100101111
(4,9)	:	0010001001
(23,12)	(	1011101100
(18,2)	)	1001000010
(9,21)	?	0100110101
O	Space	0000000001

Table1. A set of points on EC, corresponding codes and the corresponding alphabetical symbol

Acknowledgment

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

References

[1] Mukesh Kumar Singh, Public key cryptography with matrices, Proceeding for 2004 IEEE workshop on Information Assurance, 2004.

[2] Toelplitz and circulant Matrices: A review, Robert M.Gray, Information System Laboratory, Department of Electrical Engineering, Stanford University, California 94305 http://www.stanford.edu/~gray/toeplitz.pdf.

[3] Joan-Josep, Francisco Ferrandez, Jose-Francisco Vicent, Antonio Zamora, A nonlinear elliptic curve cryptosystem based on matrices, Mathematic of computation volume 174, 150-164, 2006.

[4] 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.

[5] 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.

[6] F.Amounas and E.H. El Kinani, An elliptic curve cryptography based on matrix scrambling method, Proceedings of the JNS2, IEEE Xplore, 31-35, 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] Mahalanobis Ayan. The discrete logarithm problem in the group of nonsingular circulant matrices. Groups Complex. Cryptol. 2, No.1, pp: 83-89, 2010.
[11] Hill LS, Concerning Certain Linear Transformation Apparatus of cryptography, American Mathematical Monthly, 38, pp: 135-154, 1931.
[12] Krishna A.V.N, A.Vinaya Babu: A Modified Hill Cipher Algorithm for Encryption of Data in Data Transmission, Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No. 3(14) pp: 78-83, 2007.

AUTHOR'S PROFILE

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