Matrix Based Elliptic Curve Cryptography Protocol (MECCP)

Jagannathan M[1] Devaraju B M[2]
[1]M.Tech Scholar [2]Asst. Prof. Dept Of CSE
[1, 2] RNS Institute of Technology Bangalore, Karnataka, India

Abstract--- ECC has gained a lot of focus over a past ten years in literature simply because of its performance. The reason behind this is that ECC when compared with RSA and some other cryptographic algorithm it provides equal security for a smaller key bit size so with this it has less work in processing part. this project, 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 project also attempts 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: ECC, MECCP, MATRIX BASED EEC.

I. Introduction

With the rapid growth of internet, information security in the present era is becoming very important in communication and data storage. Data transferred from one party to another over an insecure channel (e.g., Internet) can be protected by cryptography. The encrypting technologies of traditional and modern cryptography are usually used to avoid the message from being disclosed. Public-key cryptography usually uses complex mathematical computations to scramble the message. There are some popular public-key encryption algorithms, for example, RSA, ElGamal, and ECC. The security of the most public-key encryption algorithms is based on discrete logarithms in finite groups or integer factorization.

In the last decade the application of the elliptic curves in cryptography has been attracting increased attention of many scientists because they have opened wealth possibilities in terms of security. 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[2] 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[3] and Koblitz[4] and it is not easy to understand by attacker.

II. Related Work

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of parameters‟ in ECC is an example of such constants. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties. The mathematical operations of ECC is defined over the elliptic curve

$y^2 = x^3 + ax + b$, -------- (1)

where

$4a^3 + 27b^2 \neq 0$. -------- (2)

Each value of the "a" and "b" gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters „a‟ and „b‟, together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size[1]. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

The Public key infrastructure that is in place today relies on the RSA algorithm, named after the authors who created it. RSA relies on interesting properties of large prime numbers to generate asymmetric keys. However, RSA has been around a long time and is beginning to show some weaknesses, the keys used in RSA are becoming longer and longer to provide the same level of security as they used to.

To basic ECC to ensure higher security some more steps are added and it is mentioned in proposed work.

III. Proposed Work

The proposed system applies some manipulations to the original data using matrices and some of its properties. And then apply the basic algorithm of ECC to the intermediate result obtain to generate result. This result is converted to binary representation and sent to receiver(Bob). This binary representation is received by Bob and exact reverse procedure of proposed encryption process is followed to obtain original data.

Figure 1 shows detailed design of encryption module. The plain text is transformed into points on the elliptic curve. These points are represented in another form, ie., addition of two points by using elliptic curve addition table, and stored in a matrix, M. Choose a non-singular matrix, multiply it with the matrix M and store the result into another matrix B

A. Encryption

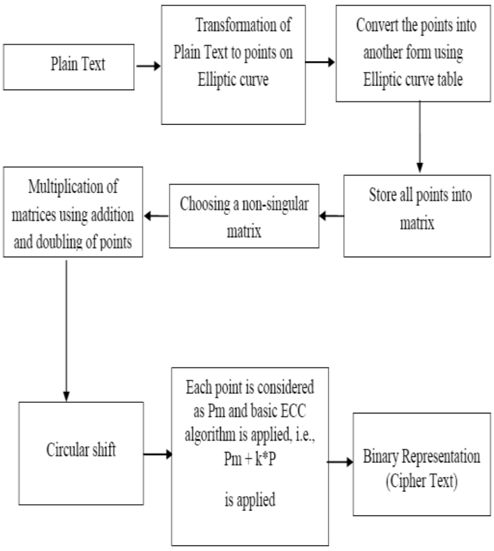
Plain Text
Transformation of Plain Text to points on Elliptic curve
Convert the points into another form using Elliptic curve table
Store all points into matrix
Choosing a non-singular matrix
Multiplication of matrices using addition and doubling of points
Circular shift
Each point is considered as Pm and basic ECC algorithm is applied, i.e., Pm + k*P is applied
Binary Representation (Cipher Text)

Fig. 1: Detailed design of Encryption module

Then perform circular shifts and store the result in matrix D. Then represent the points in the matrix D in binary form. This binary representation is the cipher text.

Decryption

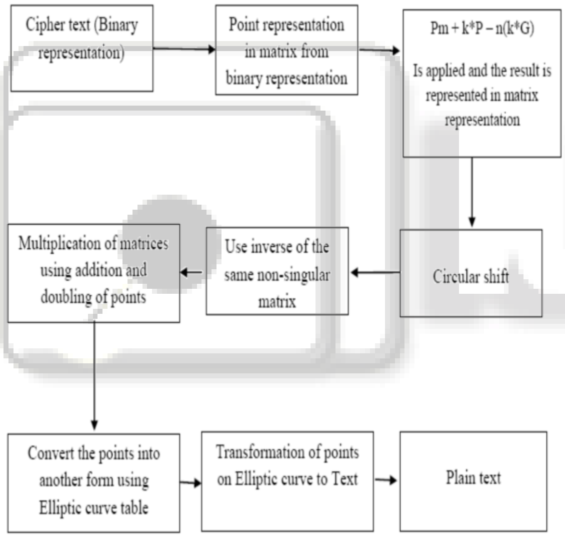
Cipher text (Binary representation)
Point representation in matrix from binary representation
Pm + k*P – n(k*G) Is applied and the result is represented in matrix representation
Circular shift
Use inverse of the same non-singular matrix
Multiplication of matrices using addition and doubling of points
Convert the points into another form using Elliptic curve table
Transformation of points on Elliptic curve to Text
Plain text

Fig. 2 : Detailed design of Decryption module

Figure 2 shows detailed design of decryption module. The cipher text obtained in binary representation is converted into points and stored in the matrix B. Perform circular shifts to this matrix, B. Then multiply the matrix B with the inverse of the same non-singular matrix using addition and doubling of points and store the result in a matrix, M. The add the two points in each row of the matrix to obtain single point per row. Then transform these points into text to obtain the original plain text.

IV. IMPLEMENTATION

A. Double and Add method

Let P(x1, y1) and Q(x2, y2) be elements of the ECC. Then P + Q = (x3, y3), where

$$X_3=\lambda^2-x_1-x_2$$

$$Y_3=\lambda(x_1-x_3)-y_1 \qquad \text{and}$$

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1} & \text{If } P \neq Q\\[2ex] \dfrac{3x_1^2+a}{2y_1} & \text{IF } P = Q\end{cases}$$

Generate Addition table for EC

1. Choose an elliptic curve E defined over finite field Fp. Let P is a point generator and n is order of P.
2. Generate table addition (n n) by using the rules for addition over Ep(a, b).

+	Q_0	Q_1	...	Q_{n-1}
P_0	$R_{0,0}$	$R_{0,1}$	...	$P_{0,n-1}$
P_1	$R_{1,0}$	$R_{1,1}$	...	$P_{1,n-1}$
	...	...	...	
P_{n-2}	$R_{n-2,0}$	$R_{n-2,1}$	...	$R_{n-2,n-1}$
P_{n-1}	$R_{n-1,0}$	$R_{n-1,1}$	...	$R_{n-1,n-1}$

Table 1: The table addition of points on EC

Each point is represented by two different point Ri,j = Pi + Qj . There many forms that represent a point R. This feature helpsto send the same characters but with another form.

B. Encryption

1. Tranforms the plaintext into points on elliptic curve Ri, i=1,2,….,r.

2. Converts the points R(x,y) in another form using addition table. So, each point is represented by two points.

3. All points are stored into matrix of (rx2) 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 (2x2) such that |A|=±1.

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

5. Using addition and doubling of points to compute: B=MA.

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

7. Pm + k*P is applied to each point in matrix and stored in matrix.

8. Converts the data points into binary form and call it C, cipher text.

C. Decryption

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

1. First separate x-coordinate and y-coordinate of points Di from C.
2. Convert a sequence to decimal form.
3. Obtain Di from two values and stored point Di=(x1, y 1) into matrix of (r x 2).
4. Pm + k*P – n(k*G) Is applied and the result is represented in matrix representation.
5. Circular upward shift is followed by circular left shift the elements of D. The result matrix is noted B.
6. Compute M = BA-1 to obtain a points Pi and Qi.

Compute Ri = Pi + Qi for each row of M. Then reverse the embedding to recover the plaintext.

V. CONCLUSION

This paper presents and implements 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. This transformed character of the message is encrypted by the proposed encrypted technique. Decryption of encrypted message is itself quite a formidable task, unless we have knowledge about the private key "n_B", the secret integer "k" and the affine point Pm.

ACKNOWLEDGEMENT

We would like to thank Director Dr. H N Shivashankar, Principal Dr. M K Venkatesha and Dr. G T Raju, Professor and Head, Dept of Computer Science and engineering, RNSIT, for constant and pursing this paper.

REFERENCES

[1] F.Amounas and E.H. El Kinani, "An Efficient Elliptic Curve Cryptography protocol Based on Matrices",2012, vol 1,PP:49-54

[2] 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.

[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.