# A FAST AND EFFICIENT CRYPTOSYSTEM FOR RESOURCE CONSTRAINED NETWORKS

Nisheeth Saxena

CSE Department - CET Mody University
Lakshmangarh, Sikar, India
nisheeth.somnath@gmail.com

Anil Dahiya

CSE Department - CET Mody University
Lakshmangarh, Sikar, India

**Abstract A paradigm shift is taking place from wired networks to wireless/infrastructure less Ad-Hoc networks, such as Mobile Ad-Hoc Networks (MANET) and Wireless Sensor Networks (WSN). Their computational power is low and bandwidth is limited. Because of their unique characteristics data security becomes a major issue in these resource constrained networks. Elliptic Curve Cryptography (ECC) may provide a solution for the security of Ad-Hoc networks since they need significantly smaller parameters in comparison to cryptosystem such as RSA, DSA etc., therefore involving lightweight computations. In this paper we propose a new cryptosystem based on ECC, which uses non -singular matrix multiplication for point mapping along with Elliptic curve analog of Massey-Omura method for encryption and decryption. Our method being simple, fast and efficient is suitable for resource constrained networks such as MANET and WSN.**

***Keywords:*** Public key cryptography, Elliptic Curve Cryptography, MANET, Non-Singular Matrix, Massey Omura method.

## 1. Introduction:

The use of mobile and wireless devices is increasing day by day. Now a day there is a trend of moving from wired networks to wireless networks, since they are easy to install and need no centralized control system. These networks are constructed on the fly and form a system of wireless mobile nodes that dynamically self-organize themselves in arbitrary and temporary network topologies [Levent and Nitu, (2007)]. These networks are resource constrained having limited bandwidth and can't support heavy computations.

Data security becomes vulnerable, in these networks due to their particular nature and structure, and therefore securing data or messages is a challenging task in such kind of environments. Public key cryptography offers a solution to secure data in Ad-Hoc networks. But public key cryptosystems involve heavy computations so they are not suitable for these networks where processing power is low and bandwidth is limited. Elliptic Curve Cryptography (ECC) may be a better option for data/message security in resource constrained networks, since they use smaller size keys in comparison to popular Public Key Cryptosystems (PKC) available, therefore putting less pressure on the resources.

The use of elliptic curves in public key cryptography was independently proposed by Koblitz, (1987) and Miller, (1986). ECC has attracted attention in recent years due to its ability to use smaller key sizes [Singh and Singh, (2015)], as compared to RSA, but at the same time providing equivalent level of security. It gives better security per bit as compared to RSA. In ECC a 160 bits key, provides the same security as RSA 1024 bits key, reducing the computational power significantly. ECC has been considered suitable for applications such as smart cards, mobile commerce, Ad-Hoc networks etc., due to its less storage requirements and computational cost. The advantage of elliptic curve cryptosystems is the absence of sub exponential time algorithms that could find discrete logarithms in these groups, for attack. The elliptic curve cryptosystems may be regarded as more secure because the analog of Elliptic curve discrete log problem (ECDLP) is at least as hard as the classical Discrete Log Problem(DLP).For further study on Elliptic Curves one can refer to [Stinson, (2005); Katz and Lindel, (2014); Certicom, (2000); Alfred et al., (1996)].

In this paper we have presented an efficient and new method based on Elliptic Curve analog of Massey Omura method (ECAMOM) [Koblitz, (1987)]. First we encode our original message as affine points over Elliptic Curves. This encoding is very simple and one-to-one w.r.t. characters of alphanumeric message and points over Elliptic Curve. Then these mapped points over Elliptic Curve (EC) are converted into matrix form and then are multiplied with the compatible non -singular matrix [Bhatia, (2012]. This is done to refute letter frequency attack, since after matrix multiplication we get random points on Elliptic Curve for message characters. In our method even same characters are mapped on to different points over EC. This effectively hides the letter frequencies in the plaintext message and makes our cryptosystem more secure and efficient. Then the Elliptic Curve Points representation of the message is encrypted at the sender's side and subsequently decrypted at the receiver's side. For encryption and decryption we use EC analog of Massey-Omura method.

The paper is organized in following manner: Section 2 gives a brief description of Elliptic Curve Cryptography and the modular arithmetic involved; in section 3, we have explained our proposed method based on Elliptic Curve analog of Massey Omura method; in section 4 we have presented our implementation procedure and results, and finally concluding remarks are given section 5.

## 2. Elliptic Curves and Cryptography

An elliptic curve $E_k$ over the set of real numbers ℝ (for a finite field *K*) is defined by a Weierstrass equation of the form:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 - - - - - - - - - (1)$$

The Eq.(1) can be simplified by linear change of variables whenever characteristic of field K≠2, 3 [Koblitz, (1987); Arita (2000)].

The change of variables may be as follows:

$$(x, y) \leftrightarrow (x - \frac{a_2}{3}, y - \frac{a_1x + a_3}{2})$$

Then Eq. (1) becomes:

$$y^2 + a_1xy + a_3y = x^3 + ax + b - - - - - - - - - - - - - - - (2)$$

Where$a = \frac{1}{9a_2^2} + a_4$ and$b = \frac{2}{27a_2^3} - \frac{1}{3a_2a_4a_6}$ such that *a, b*∈*K.*

If we set $a_1$=0, $a_3$=0,then Eq.(2) can be simplified further as:

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

with condition $4a^3 + 27b^2 \neq 0$ and a point at infinity ***O***. Alternatively Eq. (3) is the simplified form of an elliptic curve $E_K$ over a filed *K*, which has the set of solutions $(\mathrm{x}, \mathrm{y}) \in \mathrm{K} \times \mathrm{K}$together with the point at infinity ***O***, which is a special point.

If $\mathrm{K} = \mathrm{GF}(\mathrm{q}),\ \mathrm{q} = \mathrm{p}^\mathrm{n}$, where *p* and *q*are very large prime numbers and *n* is a positive integer, then the points of elliptic curve $E_K$ form a finite abelian group. Here point addition is the group operation. Here *GF* is Galois field, which is finite and cyclic.

Now we can define elliptic curve *E* over finite field $GF(p)$ (when *n=1*) as:

$$y^2 = x^3 + ax + b\ \ (mod\ p)$$

s.t.$4a^3 + 27b^2 \neq 0\ \ (mod\ p)$and*a, b*∈*GF(p).*

The addition of points of elliptic curve *E* [Lange and Ruppert,(1987)] satisfies the following rules:

- *O*+*O*=*O* (*O* is the identity element, the point at infinity)
- *P*+*O*=*P* ∀*P*=*(x, y)*∈ *E.*
- If *P=(x,y)*,then negative of point *P* i.e. –*P*is :*Q=(x,-y)* and *P*+*Q*=*O* ; *P*,*Q* ∈ *E.*
- Let *P* and *Q* be two distinct points over E, such that $P=(x_1, y_1)$ and $Q=(x_2, y_2)$ and $x_1 \neq x_2$, then addition is given as:

$$\mathrm{P} + \mathrm{Q} = \mathrm{R} \quad ; \quad \mathrm{R} = (\mathrm{x}_3, \mathrm{y}_3)$$

Where, $x_3 = \lambda^2 - x_1 - x_2$;$y_3 = \lambda(x_1 - x_3) - y_1$ and $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$

- Let P and Q are similar points i.e. $P = Q$ ; $x_1 \neq x_2$
  Then
  $$P + Q = 2P = R = (x_3, y_3)$$
  Where,
  $$x_3 = \lambda^2 - 2x_1 \ ; \quad y_3 = \lambda(x_1 - x_3) - y_1 \text{ and} \lambda = \frac{3x_1^2 + a}{2y_1}$$
- Scalar point multiplication: We can compute the multiple of a point P, i.e. $\beta *$P is the same manner as to exponentiate $a^\beta$. We apply doubling and addition, which takes time *O(log β).*

  For example *13*P* can be calculated as:$13 * P = (P + 2(2(P + 2P)))$

  We can write m in the binary representation:

$$\beta = d_0 + 2.d_1 + 2^2d_2 + - - - - + 2^rd_r$$

Where $d_0, d_1, - - - - d_r \in \{0,1\}$ and

$$\beta * P = d_0P + 2d_1 P + 2^2d_2P + - - - + 2^rd_rP$$

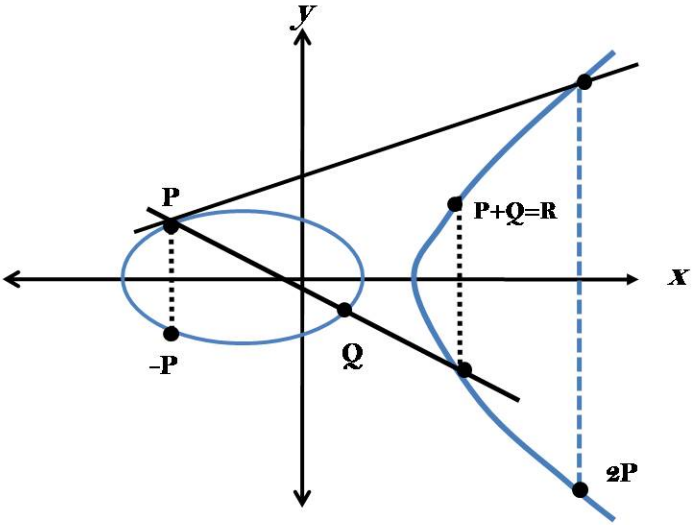

Fig. 1. Representation of different Points operations over Elliptic Curve.

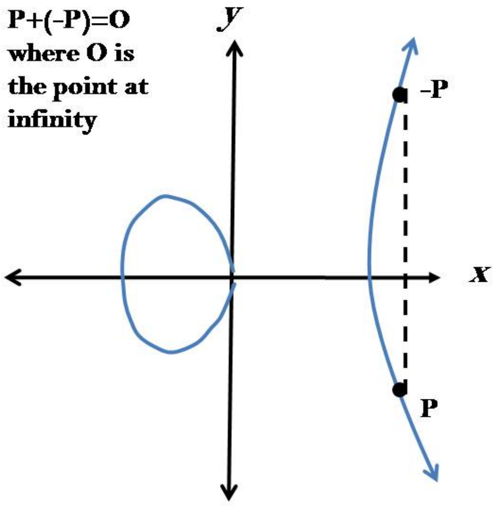

Fig.2. Addition of a point *P* with its negative point –*P*

The numbers of points over EC, E over *GF* $(p^n)$ are given as:

$$\# E = p^n + 1 - t \quad ; \quad with \qquad |t| \leq \quad 2\sqrt{p^n}$$

Where, ***t*** is called the trace of Elliptic Curve - E.

Let G be a point on an elliptic curve E. Then order of point G is the smallest integer x, such that

*x.G=O*. If order of a point is equal to the order of E, then that point is called the base point or generator point of the Elliptic curve-E. Suppose if two points *P* and *Q* are given on E, such that *P=y.Q*, then finding multiple *y* is believed to be a difficult problem and is known as elliptic curve discrete logarithm problem (*ECDLP*). All cryptosystems based on Elliptic Curves rest their security on this, infeasible to solve, problem. Anomalous EC over *GF(p)* are those whose trace *t=1*, i.e. they have exactly '*p*' points over them.

For super singular EC the trace '*t*' is given as : $t = \pm\sqrt{i.p^n}$ ; $i = 0,1,2,3,4.$

When, *i=0* and *t=0*, the order of EC - E over $GF(p^n)$ will be$p^n + 1$and over *GF(p)*, it will be exactly *p+1*. Except anomalous and super singular ECs, the fastest known algorithm to solve discrete logarithm problem (DLP) takes time $O(\sqrt{p^n})$ which is exponential in nature.

### 3. Description of Proposed Method and its Correctness:

In our proposed cryptosystem the public parameters are as follows:

**E:** An elliptic curve over GF(q),where $q = p^n$ , and p and q being very large primes. If n=1, we can take our finite field as GF(p).

**G:** The base point or generator point of Elliptic Curve E, where order of G is x, such that x is the smallest integer satisfying $x.G = O \; and \; x = \#|E|$.
**S:** The set of symbols or alphabets, it can include all printable characters.
**M:**Matrix representing the characters of plaintext message as linear mapping points over Elliptic Curve.
In our proposed cryptosystem private parameters are as follows:
**A:**A non-singular square matrix of size $d_1 \times d_1$ having integer entries and determinant of *A*, $|A| = \pm\alpha$ , where $\alpha$ is any integer. *A* is shared by only Alice and Bob.
**Q:**Matrix representing random distribution of plaintext message characters over EC,obtained after applying non - singular matrix multiplication over matrix *M*.
All operations are done in modular arithmetic (*mod p*) .
Let f**:** A mapping from S to M i.e. f: S → M.Steps of our algorithm are as follows:

1. Transform the characters/symbols of the plaintext message ‘*m*’ into points over Elliptic Curve [King, (2009)].Transform the characters (symbols) of the plaintext message ‘*m*’ into points over EC:

   $P_1$, $P_2$, -------$P_l$; where l is length of message ‘*m*’. Every symbol of ‘m’ is linearly mapped to a point of EC-E.We choose a generator G or a base point of the EC.We perform linear mapping of characters of message ‘*m*’as shown in the following Table 1.

Table 1: Linear mapping of symbols to points of EC

| S.No. | Character/Symbol of Plaintext message ‘m’ | Corresponding point over Elliptic Curve |
|---|---|---|
| 1. | ‘a’ | G |
| 2. | ‘b’ | 2*G |
| 3. | ‘c’ | 3*G |
| … | … | … |
| 26. | | 26*G |
| 27. | ‘0’ | 27*G |
| 28. | ‘1’ | 28*G |
| and so on. | | |

Any number of symbols can be mapped in this way by appropriately choosing the finite cyclic field *GF(p).*

2. Create a matrix *M* of dimension $d_1 \times d_2$ so that all points $P_1$, $P_2$, ------- $P_l$ become the entries of *M*, i.e.

$$M=\begin{bmatrix} a_{11} & a_{12} & .... & a_{1d_2} \\ a_{21} & a_{22} & .... & a_{1d_2} \\ : & : & .... & : \\ a_{d_1 1} & a_{d_1 2} & .... & a_{d_1 d_2} \end{bmatrix}$$

3. Choose a non-singular matrix *A* of dimension $d_1 \times d_1$, whose determinant i.e. $|A| = \pm\alpha$ where α is an integer.
4. Calculate *Q=A.M (mod p).* The dimension of resultant matrix *Q* containing random points of EC is $d_1 \times d_2$. The set points of EC in matrix Q can be represented as :
   *Q’ = {$Q_1$, $Q_2$, --------}*

$$Q = \begin{bmatrix} Q_{11} & Q_{12} & .... & Q_{1d_2} \\ Q_{21} & Q_{22} & .... & Q_{1d_2} \\ : & : & .... & : \\ Q_{d_1 1} & Q_{d_1 2} & .... & Q_{d_1 d_2} \end{bmatrix}$$

5. On matrix *Q* we apply EC analog of Massey Omura method to get the encrypted message in the form of points over EC. The description of Massey Omura method is given afterwards.
6. To get back the original message after decryption Receiver calculates:

$A^{-1}.Q = A^{-1}.A.M = M$ ; where$A^{-1}$*(mod p)*is the inverse matrix of *A (mod p).*

Actually$A^{-1}$. *A = I (mod p)*(Identity matrix).

7. From M we can obtain the plaintext message ‘*m*’ by inversing the linear mapping,which is easy.
8. Stop.

The ECAMOM can be described asfollows:

Let $N$=$|E|$. Suppose Alice, the sender, wants to send a message '$m$' to Bob, the receiver. Let $m_i$ represents the $i^{th}$ character of '$m$' represented by point $P_{m_i}$ over the EC.

Steps of ECAMOM Encryption/Decryption procedure are as follows:

(i) Alice chooses a random integer number, $r_A \in [1, \mathrm{N}-1]$ ; such that $\gcd(r_A, N) = 1$.
She also calculates:$s_A = r_A^{-1}\ (mod\ \ N)$.She keeps $r_A$ and $s_A$ secret.
She sends ( $r_A * \mathrm{P}_{\mathrm{m_i}}$) to Bob.

(ii) Bob chooses a random integer number, $\mathrm{r_B} \in [1, \mathrm{N}-1]$and$\gcd(r_B, N) = 1$.
Bob also calculates:$s_B = r_B^{-1}\ (mod\ \ N)$. He keeps $r_B$ and $s_B$ secret.
Bob sends back to Alice : $r_B\left(r_A * \mathrm{P}_{\mathrm{m_i}}\right)$.

(iii) Alice calculates :$s_A * \left(r_B.\left(r_A * \mathrm{P}_{\mathrm{m_i}}\right)\right)$ and again sends to Bob.

(iv) Finally Bob calculates :$s_B * \quad s_A * \left(r_B.\left(r_A * \mathrm{P}_{\mathrm{m_i}}\right)\right)$*(mod N)* and obtains $P_{m_i}$.

**Correctness and Security**: The procedure is correct since:

$$s_B\left(s_A\left(r_B\left(r_A.P_{m_i}\right)\right)\right) = s_B.s_A.r_B.r_A.P_{m_i} = r_A.s_A.r_B.s_B.P_{m_i} = P_{m_i}$$

The method is secure,since if an intruder wants to know the plaintext message then she has to find either $r_A\ \ or\ r_B$ from( $r_A * \mathrm{P}_{\mathrm{m_i}}$) or $r_B\left(r_A * \mathrm{P}_{\mathrm{m_i}}\right)$ or ( $r_B * \mathrm{P}_{\mathrm{m_i}}$),which is Elliptic Curve Discrete logarithm Problem and is intractable.

The block diagram of our proposed method is shown in figure 3:

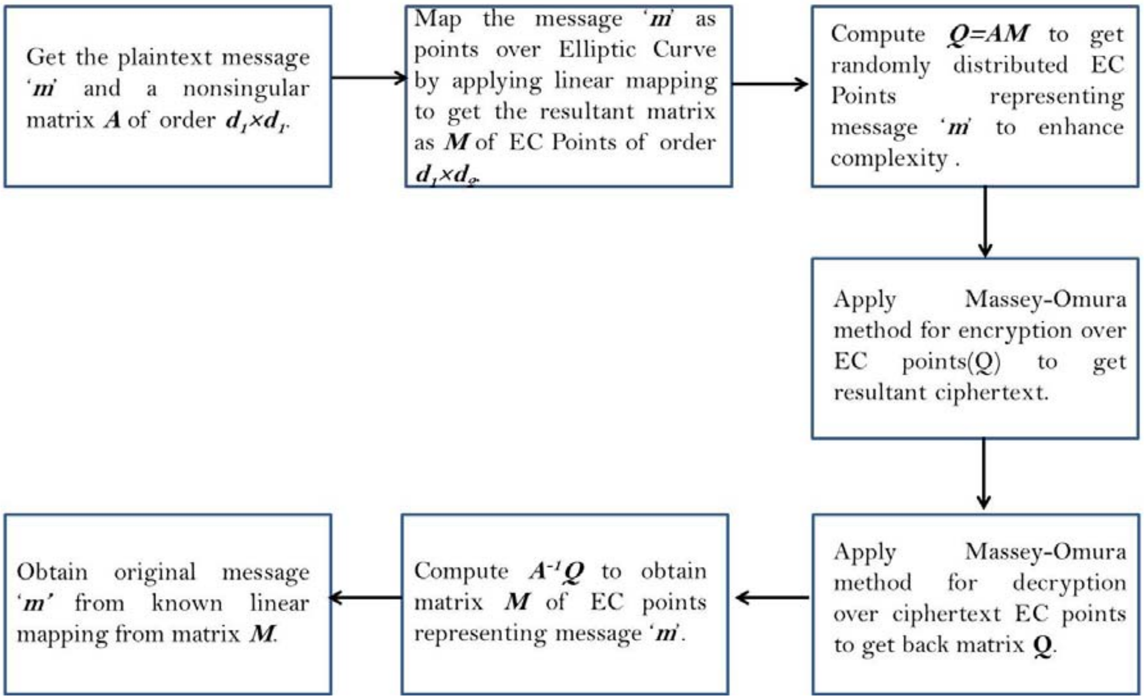
Get the plaintext message '*m*' and a nonsingular matrix *A* of order *d₁×d₁*.
Map the message '*m*' as points over Elliptic Curve by applying linear mapping to get the resultant matrix as *M* of EC Points of order *d₁×d₂*.
Compute *Q=AM* to get randomly distributed EC Points representing message '*m*' to enhance complexity .
Apply Massey-Omura method for encryption over EC points(Q) to get resultant ciphertext.
Apply Massey-Omura method for decryption over ciphertext EC points to get back matrix **Q**.
Compute *A⁻¹Q* to obtain matrix *M* of EC points representing message '*m*'.
Obtain original message '*m*' from known linear mapping from matrix *M*.

Fig. 3.The block diagram of our proposed method

## 4. Implementation of Proposed Method and Results

In out method we selected an EC given as follows:

$$y^2 = x^3 + 2x + 11\ (mod\ 41)$$

Here EC parameters are: *a=2*, *b=11* and *p=41*. Where $4\mathrm{a}^3 + 27\mathrm{b}^2 \bmod \mathrm{p} = 4\ \times\ 2^3 +\ 27 \times 11^2\ (\mathrm{mod}\ 41) = 19 \neq 0$. Therefore we can choose this parameters.Here we have chosen as our plaintext message '$m$' as: 'attacktoday'. '$m$' is padded with an extra character '$z$' to make compatibility in matrix multiplication.We have used Matlab version 2013a for the simulation of our results.

We select a non - singular square matrix *A(mod 41)*of dimension 3 x 3 for simplicity, although non - singular matrices of any dimension can be chosen.

$$\mathrm{A} \quad = \quad \begin{bmatrix} 40 & 5 & 40 \\ 39 & 11 & 7 \\ 1 & 36 & 2 \end{bmatrix}\ (mod\ 41)\ \ ; Det(A) = 40(mod\ 41)$$

Inverse of A is :

$$A^{-1}= \begin{bmatrix} 25 & 5 & 36 \\ 30 & 1 & 32 \\ 1 & 0 & 1 \end{bmatrix} (mod\ 41)$$

$$A.A^{-1} = I\ (\ mod\ 41)$$– Identity matrix as expected.

The points over this EC as well as base points are given in the tables 2 and 3 respectively.

The rest of the calculations involved in our method are shown in detail in Tables 4 and 5.

Table 2. Set of points over our Elliptic Curve (Total number of points over Elliptic Curve = 46)

| | | | | |
|---|---|---|---|---|
| [2 , 8] | [2 , 33] | [4 , 1] | [4 , 40] | [5 , 8] |
| [5 , 33] | [7 , 9] | [7 , 32] | [9 , 15] | [9 , 26] |
| [12 , 0] | [13 , 15] | [13 , 26] | [14 , 6] | [14 , 35] |
| [16 , 11] | [16 , 30] | [18 , 4] | [18 , 37] | [19 , 15] |
| [19 , 26] | [22 , 17] | [22 , 24] | [24 , 5] | [24 , 36] |
| [26 , 3] | [26 , 38] | [28 , 17] | [28 , 24] | [31 , 4] |
| [31 , 37] | [32 , 17] | [32 , 24] | [33 , 4] | [33 , 37] |
| [34 , 8] | [34 , 33] | [36 , 9] | [36 , 32] | [37 , 12] |
| [37 , 29] | [39 , 9] | [39 , 32] | [40 , 7] | [40 , 34] |
| [Inf,Inf]=***O*** | - | - | - | - |

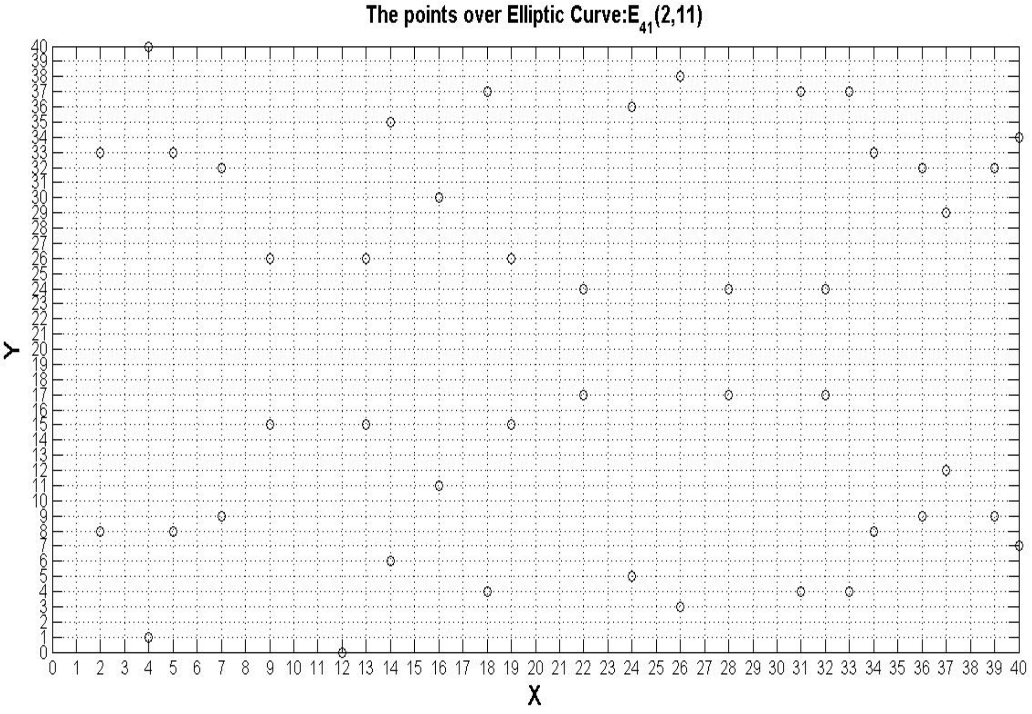

Fig.4. Graphical representation of points over Elliptic Curve.

Table 3: Set of base/ generator points over Elliptic Curve (Total number of generator points = 22, Order =46 )

| | | | | |
|---|---|---|---|---|
| [5 , 8] | [5 , 33] | [9 , 15] | [9 , 26] | [18 , 4] |
| [18 , 37] | [19 , 15] | [19 , 26] | [24 , 5] | [24 , 36] |
| [26 , 3] | [26 , 38] | [31 , 4] | [31 , 37] | [34 , 8] |
| [34 , 33] | [36 , 9] | [36 , 32] | [39 , 9] | [39 , 32] |
| [40 , 7] | [40 , 34] | - | - | - |

Table 4. Elliptic curve point calculation for matrices M and Q.

| S.No.- | Plaintext message – 'm'Characters/Symbols | Alphabetical order | Points on EC after Linear mapping; Base point G=[5 8] Entries of Matrix-M | Points of EC after non – singular matrix Multiplication Entries of Matrix- Q=AM |
|---|---|---|---|---|
| 1. | a | 1 | [5 ,8] | [19 , 26] |
| 2. | t | 20 | [16 ,11] | [36 , 32] |
| 3. | t | 20 | [16 ,11] | [22 , 24] |
| 4. | a | 1 | [5 ,8] | [31 , 37] |
| 5. | c | 3 | [18 ,37] | [33 , 4] |
| 6. | k | 11 | [26 ,38] | [2 , 33] |
| 7. | t | 20 | [16 ,11] | [36 , 9] |
| 8. | o | 15 | [19 ,15] | [37 , 12] |
| 9. | d | 4 | [14 ,35] | [36 , 9] |
| 10. | a | 1 | [5 ,8] | [14 , 35] |
| 11. | y | 25 | [36 ,9] | [33 , 4] |
| 12. | z | 26 | [16 ,30] | [31 , 4] |

Table 5. Results for ECC analog of Massey Omura Encryption /Decryption

Parameters (Alice): $r_A = 17\ (mod\ 41), r_A^{-1} = 29\ (mod\ 41)$
Parameters (Bob): $r_B = 5\ (mod\ 41), r_B^{-1} = 33\ (mod\ 41)$

| S.No. | Mappin g Points- $P_{m_i}$ | Alice : $(r_A \mathrm{P}_{\mathrm{m_i}})$ Encryption | Bob : $r_B(r_A \mathrm{P}_{\mathrm{m_i}})$ Encryption | Alice : $r_A^{-1} * (r_B(r_A \mathrm{P}_{\mathrm{m_i}}))$ Encryption | Bob : $r_B^{-1} r_A^{-1} * (r_B(r_A \mathrm{P}_{\mathrm{m_i}}))$ $=P_{m_i}$ Decryption | Decrypted Points$P_{m_i}$ After matrix inversion= $A^{-1}Q = M$ | Corresponding Characters -after decryption |
|---|---|---|---|---|---|---|---|
| 1 | [19 , 26] | [36,32] | [5 , 8] | [9 , 26] | [19 , 26] | [5 , 8] | a |
| 2 | [36 , 32] | [26 ,3 ] | [9 , 26] | [34 , 33] | [36 , 32] | [16,11] | t |
| 3 | [22 , 24] | [33, 4] | [14 , 6] | [32 , 17] | [22 , 24] | [16,11] | t |
| 4 | [31 , 37] | [40 ,7] | [19 , 15] | [36 , 9] | [31 , 37] | [5 , 8] | a |
| 5 | [33 , 4] | [13,26] | [32 , 17] | [4 , 40] | [33 , 4] | [18 , 37] | c |
| 6 | [2 , 33] | [16 ,30] | [28 , 24] | [22 , 17] | [2 , 33] | [26 , 38] | k |
| 7 | [36 , 9] | [26,38] | [9 , 15] | [34 , 8] | [36 , 9] | [16 , 11] | t |
| 8 | [37 , 12] | [7,9] | [33 , 4] | [13 , 26] | [37 , 12] | [19 , 15] | o |
| 9 | [36 , 9] | [26,38] | [9 , 15] | [34 , 8] | [36 , 9] | [14 , 35] | d |
| 10 | [14 , 35] | [32,24] | [2 , 8] | [16 , 11] | [14 , 35] | [5 , 8] | a |
| 11 | [33 , 4] | [13,26] | [32 , 17] | [4 , 40] | [33 , 4] | [36 , 9] | y |
| 12 | [31 , 4] | [40,34] | [19 , 26] | [36 , 32] | [31 , 4] | [16 , 30] | z |

## 5. Conclusions:

In this paper we have proposed a new method suitable for securing plaintext message in resource constrained Ad Hoc environments such as MANET and WSN. In this method we have used Elliptic curve analog of Massey Omura method for encryption and decryption of plaintext. The plaintext message is mapped over the points of Elliptic curve by using non-singular square matrix multiplication. In our method regularity in resultant ciphertext is avoided due to non-singular matrix multiplication. It hides the frequency pattern in the plaintext and it becomes very difficult for an attacker to launch letter frequency count attack. This makes the decryption process difficult for the attacker and hence enhancing the security of our cryptographic method. It can be concluded that our method is simple, fast and efficient and guarantees the security of messages in resource constrained environment.

## References:

[1] Alfred J. Menezes; Paul C. van Oorschot and Scott A. Vanstone (1996). Handbook of AppliedCryptography, CRC Press.

[2] Arita S. (2000), 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.

[3] Certicom (2000). Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September, Available at http://www.secg.org/download/aid-386/sec2_final.pdf

[4] Katz Jonathan; YehudaLindel, (2014). Introduction to Modern Cryptography, Second Edition, November 6, by Chapman and Hall/CRC ISBN 9781466570269.

[5] King Brian (2009). Mapping an Arbitrary Message to an Elliptic Curve when Defined over GF(2n), International Journal of Network Security, Vol.8, No.2, pp.169-176.

[6] Koblitz N. (1987). Elliptic Curve Cryptosystems, "Mathematics of Computation, Vol. 48, No. 177, pp. 203-209.

[7] Levent Ertauland; Nitu J. Chavan (2007). Elliptic Curve Cryptography based Threshold Cryptography (ECC-TC) Implementation for MANETs. IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.4, April.

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

[9] Bhatia Rajendra (1997), Matrix Analysis, Graduate text in Mathematics, Springer.

[10] Miller.V. S. (1986). Use of Elliptic Curves in Cryptography, Advances in Cryptology CRYPTO85, pp. 417-426.

[11] Stinson Douglas R. (2005). Cryptography: Theory and Practice, Third Edition, Chapman and Hall/CRC ISBN 9781584885085

[12] Singh L. Dolendro; K. Manglem Singh (2015). Implementation of Text Encryption using Elliptic curve cryptography. Science Direct, Eleventh International Multi Conference on Information Processing-2015(IMCIP-2015).