iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** Issue II **Month of publication:** June 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Implementation of ECC Using Knapsack Algorithm

Mythrigowda Y.P[1], Leelavathi G[2]
UTL Technologies Limited ,VTU Extension Center , Banglore

Abstract — Elliptical Curve Cryptography (ECC) provides greater security by means of key exchange among communicating hosts using the Diffie Hellmen Key Exchange algorithm. The proposed work presents a mapping method based on matrix approach along with Knapsack algorithm, which gives high security for the message. The alphabetic message is first mapped on to the points on an elliptic curve and encodes these points using matrix approach with the use of a non-singular matrix. Later encrypt and decrypt those points using knapsack algorithm. To produce the initial message, the matrix obtained from decoding is multiplied with the inverse of non-singular matrix.
Index Terms — knapsack algorithm, elliptical curve cryptography, mapping

I. INTRODUCTION

Security of the information is an important issue in the developing technology. To protect or exchange confidential data, the cryptography plays an important role in the security of the information. Therefore, it is necessary to implement efficient cryptosystems, which can support applications economically feasible. In this context, public key cryptography based on elliptic curves is widely used because it presents higher security per key bit, and their main application is the private key exchange. Additionally, the Elliptic Curve Cryptosystems (ECC) can be used in applications where the computation resources are limited such as smart cards and cellular telephones. The ECC systems are included in the NIST (National Institute of Standards and Technologies) and ANSI (American National Standard Institute) standards, and the principle advantage over other systems of public key like RSA is the size of the parameters, which offers high computational security than RSA in small number of bits only. Cryptography is one of the techniques in security of Information. It basically deals with encryption and decryption of a given data. Depending upon the number of keys used cryptography is distinguishes as private and public key cryptography . Private key cryptography uses single key and public key cryptography uses two keys such as private key and public key. The advantage of public key cryptography is that it is more secure than private key cryptography. ECC is one such method of public key cryptography along with RSA. The key attraction of ECC over RSA is that it offers equal security even for smaller bit size, thus reducing the band width, processing complexity. In ECC, the operations such as point inverse, point addition, point subtraction, scalar multiplication are performed on the points obtained from an elliptic curve. These point operations are useful in performing encryption and decryption operations. In static, though it is a simple technique, the same alphanumeric characters from the different words are always mapped onto the same x-y coordinates of the elliptic curve points. When encrypted, points obtained will also be same. So, an intruder can easily interpret data with trial and error method. Hence the secrecy of data transmission by using this methodology is very low. In dynamic mapping, the alphanumeric characters are mapped dynamically on to the points of EC. Thus it is difficult for an intruder to guess which particular character is mapped to which point on EC. But mapping method using matrix method as in paper guarantees the security for the data. And no intruder can hack it. Since this method avoids the regularity in the resultant encrypted text. Thus strengthens the cryptosystems and provides better performance. We compare our proposed knapsack algorithm with RSA algorithm and show that our algorithm is better due to the high degree of sophistication and complexity involved. It avoids the brute force attack from a hacker by creating confusions.

II. ELLIPTIC CURVES IN CRYPTOGRAPHY

A. Elliptic Curve

In elliptic curve cryptography, a restricted form of elliptic curve defined over a finite field Fp is considered. One particular interest for cryptography is referred to elliptic group mod p, where p is prime number. Eq.1 defines the condition for choosing the elliptic curve.

$$4a^3+27b^2 \pmod{p} \neq 0 \qquad (1)$$

Where „a" and „b" are two nonnegative integers less than p. Then Ep(a, b) indicates the elliptic group mod p whose elements (x, y) are pairs of nonnegative integers less than p. Eq. 2 refers to the general form of elliptic curve.

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

B. Modular Arithmetic

Modular arithmetic is the principal mathematical concept in Cryptography. Here for every operation, modulus is taken w.r.t the prime number. Eg: Prime number considered in this work is 31.

C. ECC Point Operations

1) Point Inverse

If J = (x, y) □ E (Fp), then (x, y) + (x, – y) = ∞. The point (x, – y) □□E (Fp) and is called the inverse of J.

Given a point J(x1, y1) on an elliptic curve, -J(x1, y1) represents its inverse. The inverse of a given point can be computed using Eq.3.

$$-J(x1, y1) = J(x1, p- y1) \quad (3)$$

2) Point Addition: The Addition operator is defined over E (Fp) and it can be seen that E (Fp) forms an abelian group under addition. The addition operation in E (Fp) is given by Eq.4.

$$J + \infty = \infty + J = J, \square\ J \in E\ (Fp) \quad (4)$$

If J = (x1, y1) Є E (Fp) and K = (x2, y2) Є E (Fp) and J ≠ K, then L = J + K = (x3, y3) Є E (Fp). Given two points on an elliptic curve, J(x1, y1) and K(x2, y2), then the addition of those points results in L(x3, y3) which lies on the same curve. It is computed using Eq. 5, Eq. 6 and Eq. 7 as given in [4] and [5].

$$\lambda= (y2-y1)/(x2-x1) \quad (5) \qquad x3= \lambda^2-x1-x \quad (6)$$

$$y3= \lambda(x1-x3)-y1 \quad (7)$$

3) Point Doubling: If J = (x1, y1) □□E (Fp), then L = 2J = (x3, y3) □□E (Fp). Let J(x1, y1) be a point on the elliptic curve, then point doubling yields L(x3, y3) which lies on that curve. It is computed using Eq.8, Eq.9 and Eq.10 as given in [4] and [5].

$$\lambda = (3x1^2+ a) / (2y1) \quad (8) \qquad x3= \lambda^2-2x1 \quad (9)$$

$$y3=\lambda(x1-x3)-y1 \quad (10)$$

4) Scalar Multiplication: Given a point P(x1, y1) on the curve, to find k* P(x1, y1), where k is any integer, it needs repeated computations of point additions and point doublings. The reason for choosing prime fields is that distinct additive and multiplicative inverses exist for each number i.e. 0 to (P1) in the field of the prime number P.

III. PROPOSED METHOD

A. To obtain points on an elliptic curve

The elliptic curve y2=(x3+x+13) mod 31 is considered in this work. i.e. by choosing a=1, b=13 and p=31in the general form of elliptic curve given in Eg.2. The following steps are used to find out the points on an elliptic curve

Step1: perform y2 mod 31 for y= 0 to 31.

Step 2: For x= 0 to 31, perform y2 =(x3+x+13) mod 31

Step 3: Match the value of y2 mod 31 and y2 =(x3+x+13) mod 31 .

Step 4: If match is true , then the corresponding x and y values becomes a point on an elliptic curve.

Step 5: For any point on an elliptic curve, its inverse will also be present.

For the above curve considered, 34 points can be obtained including point at ∞. Here, the group is said to be cyclic, since the points repeat after 34 points.

The Table 1 gives the set of points on an elliptic curve. Let P be the generator point of the group. Now, the preliminary mapping is performed. I.e. the alphabet in the given message is mapped initially on to the points on an elliptic curve. Thus the alphabet „a" can be mapped as P = (9, 10), „b" can be mapped as 2P = (18, 29), „c" can be mapped as 3P = (23, 19), and so on. Finally the alphabet „z" can be mapped as 26P = (24, 2). Remaining 8 points can be used for mapping special characters or numbers.

Table 1: A set of points on EC

Volume 3, Special Issue-I1, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

(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)	∞	

B. Matrix Mapping Method

In this section, a mapping method based on matrices is described. The alphabetic characters are mapped on to the points on an elliptic curve. Here, both the sender and receiver agree upon few common relationships among them. Some of the parameters are defined as follows:-

E (Fp): The set of points on an elliptic curve. P: Generator point of the curve with order N. S: Set of the mapping points generated by the proposed algorithm. A: Non singular matrix, i.e. |A| ± 1 which has only integer entries. A^{-1}: Inverse of matrix A. l: Senders private key.
k: Receivers private key.

The following steps are given for matrix mapping method:-

Step 1: Transform the alphabetic characters into points on elliptic curve.

[P1(x1,y1),P2(x2,y2),……., Pn(xn,yn)] Let m be the original message of length n. If n is divided by 3, then the points have to be padded with ∞, which represents space.

Step 2: Create the matrix of 3*r with entries as points on EC. Here, take r =n/3 and s = 2n/3. The matrix M is given as

$$\begin{bmatrix} & & \\ & & \\ & & \end{bmatrix} \qquad \begin{matrix} P1 & P2 \ldots & P_r \\ P_r+1 & P_r+2 \ldots & P_S \\ P_S+1 & P_S+2 \ldots & P_n \end{matrix}$$

Step 3: A non singular matrix of 3*3 such that |A| ±1 is selected. Using addition and doubling of points, find Q = AM. Where, matrix A is given as

$$\begin{bmatrix} a11 & a12 & a13 \\ a21 & a22 & a23 \\ a31 & a32 & a33 \end{bmatrix}$$

Step 4: The result is set of points S.
S = [Q1(x1,y1), Q2(x2,y2),……., Qn(xn,yn)]

C. Knapsack Algorithm

(Encryption = TRUE) then
Q+Ia(KbP)= (x2,y2)
IaP= (x1,y1)
S[x1] = Knapsack value (x1);
S[y1] = Knapsack value (y1);
S[x2] = Knapsack value (x2);
Send (Bob, Cm=((S[x1], S[y1]), (S[x2], S[y2])));

(Decryption = TRUE) then
x1 = Inverse Knapsack value (S[x1]);
y1 = Inverse Knapsack value (S[y1]);

Volume 3, Special Issue-I1, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

x2 = Inverse Knapsack value (S[x2]);
y2 = Inverse Knapsack value (S[y2]);
IaP = (x1,y1);
Q+Ia(KbP)-KbIaP= (x2,y2);

D. Implementation Of Our Proposed Algorithm

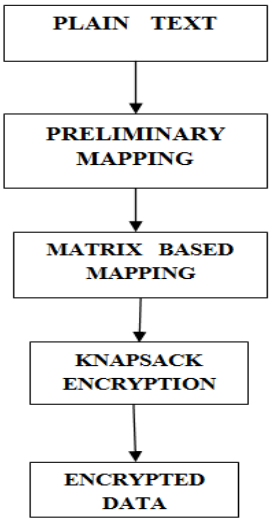


Figure 1 : Encryption Block Diagram

Figure 1 shows the Encryption Block Diagram .Input is a plain text that can be converted into binary data. In that plain text each letter is mapped as points on elliptical curve. In mapping ,Then storing all the points in the matrix form. Choose one non singular matrix. Multiply two matrix using addition and doubling. Apply knapsack algorithm result in binary representation of cipher text.

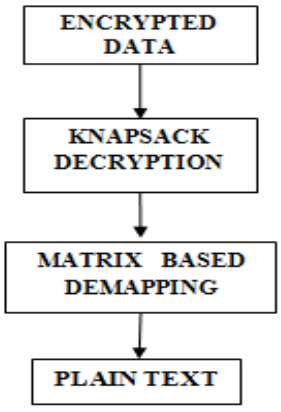


Figure 2 : Decryption Block Diagram

Figure 2 shows the Decryption Block Diagram Encrypted cipher text can be decrypted by using knapsack decryption algorithm Choosing a inverse of non singular matrix Multiplication of two matrix using addition and doubling of points. Transform the points on elliptic curve to text. Then output will be the plain text.

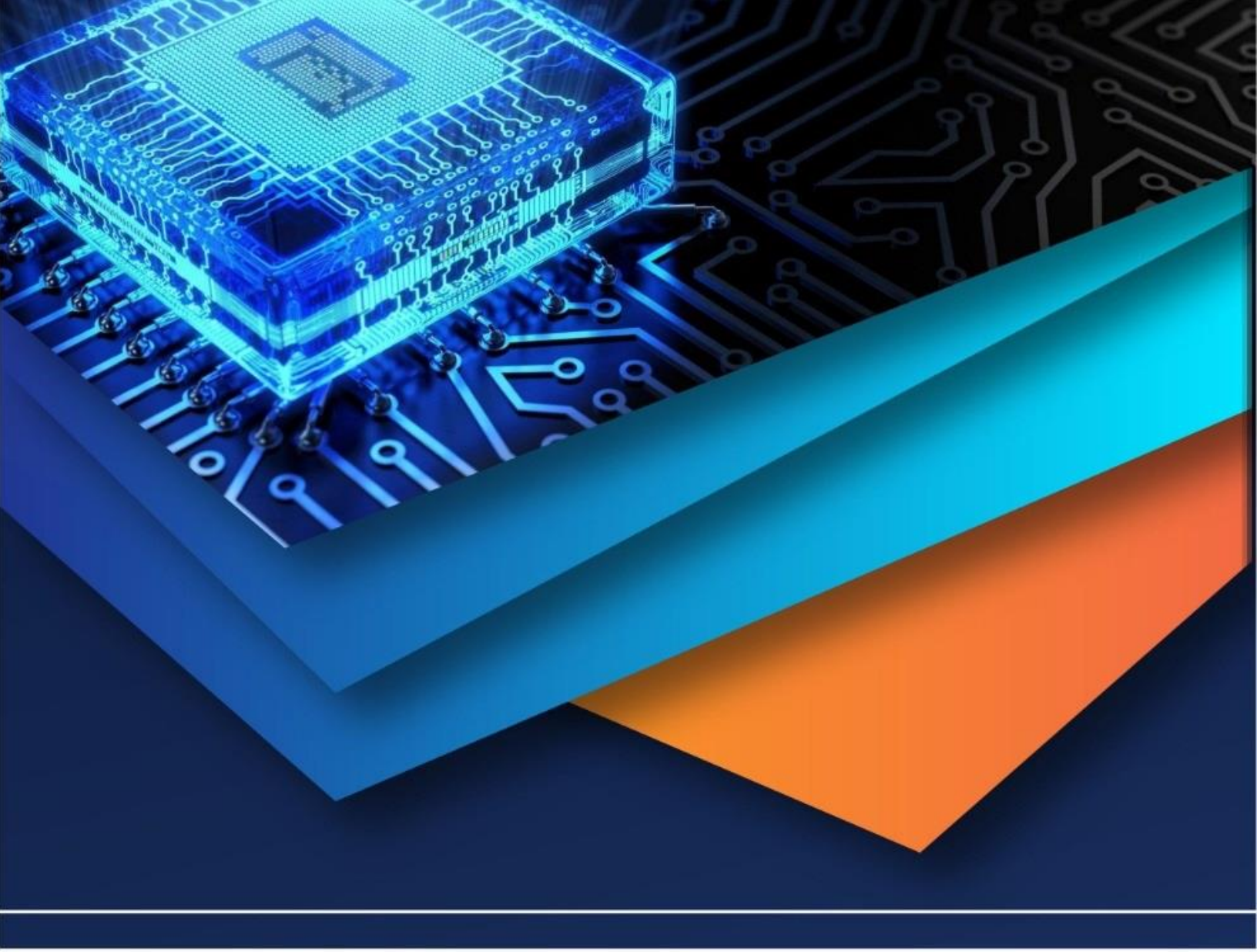
IV. CONCLUSION

In this work , implemented a matrix mapping methodology and knapsack algorithm. In matrix mapping method transfer all

alphabetic character into points on elliptic curve is explained. Encryption and decryption of mapping points is employed by knapsack algorithm .In this paper mapping method is difficult to guess the words by it does not show any regularity and knapsack algorithm avoids brute force attack by creating confusions .The language used to code these modules is Verilog. The modules are integrated to obtain matrix mapping ,Knapsack encryption, knapsack ECC decryption and de mapping. The software used to simulate the modules is Modelsim6.1c. For synthesis, XILINX software is used. .

REFERENCES

[1] Geetha G, Padmaja Jain ," Implementation of Matrix based Mapping Method Using Elliptic Curve Cryptography ",International Journal of Computer Applications Technology and Research Volume 3– Issue 5, 312 - 317, 2014
[2] Jitendra Sharma and Prashant Shukla ,**"** ECC Cipher Processor Based On Knapsack Algorithm", National Conference on Emerging Trends in Electrical, Instrumentation &Communication Engineering Vol.3, No.2, 2013 [3] O.Srinivasa Rao, Prof. S. Pallam Setty, "Efficient Mapping methods for Elliptic Curve Cryptosystems ," International Journal of Engineering Science and Technology, 2010.
[4] F. Amounas and E.H. El Kinani, " Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography," Internation al Journal of Information & Network Security (IJINS), Vol.1, No.2, June 2012, pp. 54~59, ISSN:2089- 3299.
[5] William Stallings, "Cryptography and network security principles and practice"Prentice Hall,5th Edition, 2011
[6]Darrel R. Hankerson, A. Menezes and A. Vanstone, "Guide to Elliptic Curve Cryptography" Springer, 2004
[7]G.Chen,G.Bai,and H.Chen," A High-performance elliptic curve cryptographic processors for general curves over GF(p) based on a systolic arithmetic unit," IEEE Transactions on Circuits System- II: Express Briefs,vol.54,no.5,pp.412-416,May 2007
[9] http://www.certicom.com/index.php/ecc-tutorial



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY