A Novel Way of Encrypting Text and Images using Elliptic Curve Cryptography

Ch. Udaya Bhaskar, A. Krishna Mohan

***Abstract*: ECC became one of the most widely used security standards due to it's ability for providing more security for smaller key lengths when compared to other algorithms like RSA. Like RSA and other Algorithms ECC can't be understood easily. This paper focuses on the fundamentals behind the working principle of ECC. This paper also proposes a deterministic method for mapping bytes to points on elliptic curve and illustrates the working of ECC encryption on text as well as image.**

***Index Terms*: Elliptic curve, Elliptic curve cryptography, Encryption, and Decryption.**

I. INTRODUCTION

ECC is a public key cryptography technique. It was developed basing on the concepts of algebraic structure of elliptic curves over finite fields. The reason for wide spread use of ECC is it's strength compared to other public key cryptosystems for smaller key lengths.

Public key cryptosystems like RSA[1], DHK[2], and DSA[3] were based on modular exponentiation concepts which are easily understandable. But, the concepts behind elliptic curve cryptography are difficult to understand.

This paper explains the mystery behind ECC in detail. A technique for mapping bytes to points on elliptic curves is proposed. Encryption and decryption of text as well as image is illustrated.

II. ELLIPTIC CURVES OVER REAL NUMBERS

An Elliptic curve can be defined over any domain like real numbers, rational numbers, and complex numbers e.t.c.

Elliptic curves are cubic equations like,

$$y^2 + axy + by = x^3 + cx^2 + dy + 2 \quad (1)$$

where a, b, c, d, e are real numbers and x, y take on real values.

Normally equation like,

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

with a point at infinity or zero point represented by O is used to describe elliptic curves.

Such a curve is denoted by E (a,b) and described by all the points(x,y) that satisfy the curve.

Following figures show E(-1,1) and E(-2,0)

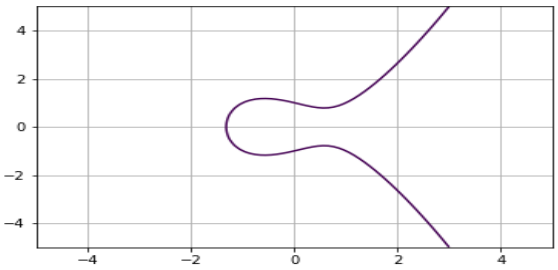

Fig. 1. Elliptic Curve of E(-1,1)

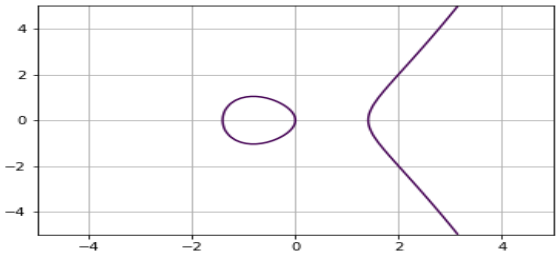

Fig. 2. Elliptic Curve of E(-2,0)

An abelian group with an operation addition denoted by the symbol + can be defined over E(a,b), if a,b satisfies the following equation.

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

The following rules are defined for addition over elliptic curve based on the rule that the sum of three points on an elliptic curve lie on a straight line, their sum is O.

1. Additive identity is O.
2. The negative of a point P=(x1,y1) is-P= (x1, -y1)
3. The sum of Two points P,Q with different x coordinates can be found by draw a straight line between them and finding the third point of intersection on the curve R.

   P+Q=-R
4. Doubling a point P can be by simply drawing a tangent line to find the other point of intersection on the curve Q .

   Then P + P = 2P = -Q .

Revised Manuscript Received on April 06, 2019.

Ch. Udaya Bhaskar, Research scholar, Computer science and Engineering, JNTUK, Kakinada, India.

Dr. A. Krishna Mohan, Professor, Computer Science and Engineering, JNTUK, Kakinada, India.

III. ELLIPTIC CURVES OVER FINITE FIELDS

ECC makes use of Elliptic curves where its variables and coefficients take on values from finite fields. There are two kinds of families of elliptic curves over finite fields.

1. prime curve over Zp :The variables and coefficients take on values only from the set [0, p-1] and all operations are performed modulo p .
2. Binary curve defined over GF(2^m):The variables and coefficients take on values in GF(2^m) and all operations aree performed over GF(2^m).

In this paper we limit our discussion to curves over Zp only. An elliptic curve over Zp is same as (2) with the values restricted to Zp and seems like,

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \quad (4)$$

The curve E(a,b) consists of all points (x,y) satisfying above equation along with point at infinity i.e. O.
The following figure shows the points on the curve Z_{89} with a=-1 and b=0.

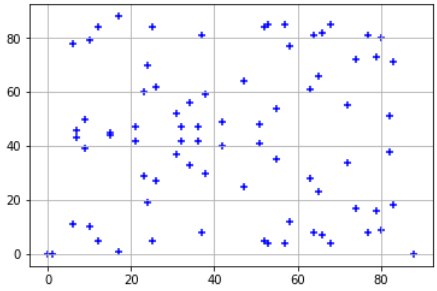

Fig. 3. Points on the curve E_{89} (1,0)

An abelian group can be defined for elliptic curves over Zp in the same way as it is defined for elliptic curves over real numbers.

A. Addition of two points over prime curves Zp

Let the sum of two point P(x_1,y_1) and Q(x_2,y_2) be R(x_3,y_3). Then R can be computed as,

$$x_3 = \nabla^2 - x_1 - x_2$$
$$y_3 = \nabla(x_1 - x_3) - y_1$$

Where

$$\nabla = \frac{y_2 - y_1}{x_2 - x_1} \text{ if P } \neq \text{Q otherwise } \frac{3x_1^2 + a}{2y_1}$$

B. Multiple of a Point

Apart from addition, multiplication of a point P on the curve with a scalar plays a vital role in ECC.,

Suppose P(x,y) is a point, then nP is equivalent to,

$$nP = P + P + ... + P \text{ (n times)}$$

This requires n-1 additions and not efficient when n is large.

The same result can be achived with th ehelp of the following algorithm which makes use of the binary equivalent of n and doubling and adding of point.

1. Let $b_n\, b_{n-1}\, b_{n-2}\ldots\ldots\ldots b_0$ is the binary equivalent of n
2. Scalar_result=0
3. Point=P
4. Repeat for bits of n from LSB to MSB
   if b_i =1 then
      scalar_result=scalar_result+P
   else
      scalar_result=2*scalar_result
5. Return scalar_result

C. Number of Points on the curve

This is represented by N and is known as order of the curve. Finding N plays a vital role in ECC.

To find what is N trying out all the possibilities between 0 and p-1 is not an efficient technique for large p. There is an efficient algorithm known as scoof's algorithm [4] for doing this.

The cardinality of the curve E_{89}(-1,0) is 80.

D. Generator, order, and Subgroups over Elliptic Curve

Every point on the elliptic curve has one property known as order. Order of a point P on the curve is defined as the least positive integer n (because for any point NP=O) such that nP=O.

If the order of a point P is n then 1P, 2P, 3P, 4P....(n-1)P are different points and form a cyclic subgroup. P is known as generator of this group with order n.

For example on the curve E_{89}(-1,0) the order of point P(68,5) is 5.

One important property of the order of a sub group is it divides the order of the parent group. So to find out the order of a point P, it is better first to compute divisors of N and then try them in ascending order on P.

Order plays an important role in ECC. Particularly prime orders. .

IV. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

The following sections explain the ECC with a deterministic mapping of bytes to points on EC.

A. ECC Parameters and their Computations

ECC is described by the following parameters.

1. p, a, and b of EC
2. N order of EC
3. Generator point G of cyclic subgroup with large prime order
4. h the co factor of the cyclic group generated by G

.The computation of G and need for co factor is explained as under.

For finding G, co factor of the sub group is needed. This is represented by h and is defined by the following equation

h= Order of the curve/ order of G i.e. N/n (5)

According to Lagrange's Theorem [5] h is an integer

For any point on the P on the Elliptic curve, the following equation holds,

$$NP = O \tag{6}$$

Equation (5) can be rewritten as,

$$n(hP) = O \tag{7}$$

From the above equation it is clear that if n is prime, then the point G=hP generates a subgroup of order n (except when G=hP=0).

The following Algorithm [6] can be used to find G.

1. Find N of the elliptic curve
2. Choose a prime order n for the subgroup such that N/n=0.
3. Find the cofactor h as N/n
4. Pick a point P randomly on the curve
5. Calculate *G* as hP.
6. If *G* is O, then
   go back to step 4.
   else
   return G

B. Encryption

For the purpose of encryption the sender chooses a private key $n_s < n$ and computes its public key as

$$P_s = n_s \times G$$

Similarly, the receiver also chooses a private key $n_r < n$ and public key as

$$P_r = n_r \times G$$

Now, sender selects a random number k < n and encrypts a point P as

$$C = \{ kG, P + kP_r \}$$

The cipher text is a set of two points.

C. Decryption

The receiver decrypts Cipher text, C, to extract plain Text, P, by multiplying the first point in C with nr and then subtracting the result from the second point.

$$\begin{aligned} & P + k \times P_r - n_r \times KG \\ & = P + k \times P_r - k(n_r \times G) \\ & = P + k \times P_r - k \times P_r \\ & = P \end{aligned}$$

D. Strength of ECC

The ECC strength lies in scalar multiplication which is very similar to discrete logarithm problem [7]

In ECC given a Point P and a positive integer n, finding nP is easy. But, given P and nP finding n is very difficult.

V. PROPOSED METHOD OF MAPPING BYTE TO A POINT ON ELLIPTIC CURVE

ECC works only with points. So the primary step in encryption is to convert given plain text to points on EC.

There are many probabilistic methods that map digital blocks to points on EC. Our method is an extension to the method [8]. Initially we choose G such that it's order is at least 257. We map byte values from 0 to 255 to 1G to 256G.

For example, for the curve $E_{5171}(-1,0)$ the following table shows mapping between byte values and Points with G =(3502,2660) whose order is 431>257.

Table I. Map table

Byte Value	Point	Mapped point on curve
0	1G	(3502, 2660)
1	2G	(1491, 2461)
2	3G	(1651, 3571)
3	4G	(4176, 1756)
255	256G	(398, 3474)

.

VI. IMPLEMENTATION OF THE PROPOSED METHOD

A. Encryption

The following figure shows the encryption mechanism.

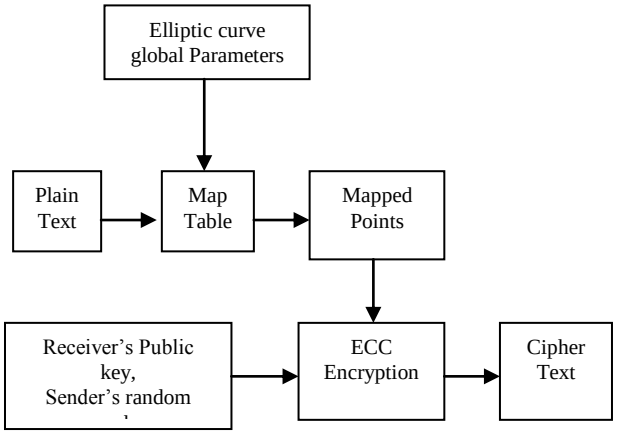

Fig. 4. Overview of Encryption

Various steps involved in Encryption are,

1. Choose EC Global Parameters
2. Compute the mapping table using proposed method.
3. Map the Plain text to Points on EC
4. Use Senders randomly chosen parameter and Receivers Public key to encrypt the points using ECC Encryption

B. Decryption

The following figure shows the decryption mechanism

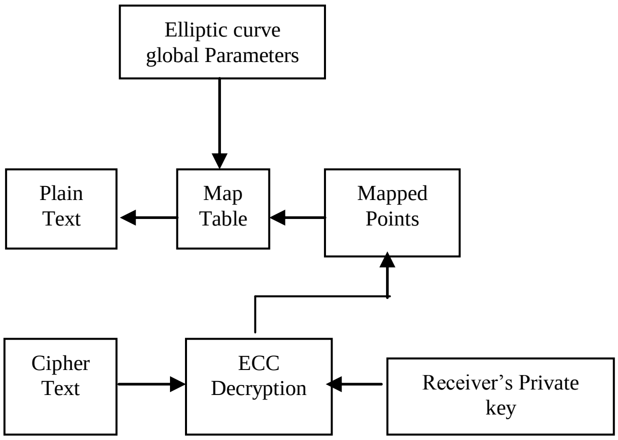

Fig. 5 Overview of Decryption

Various steps involved in Decryption are ,

1. Using ECC Decryption Algorithm to decrypt the cipher text using it's private key.
2. Compute the mapping table using the proposed technique.
3. Convert the points to plaintext using the mappings in the map table.

C. Simulation

For the purpose of simulation of ECC on text as well as image we have considered the Elliptic Curve $E_{5171}(-1,0)$ with G=(3502, 2660) with order n=431.

The following are the computed values on sender and receiver sides.

Sender: private key: 155
public key: (3262, 4368)
k: 199

Receiver: private key: 342
public key: (376, 2470)

The following figures depicts the results.
Contents of file considered for encryption.

this is the working of ecc by a new way to map text to points on elliptic curves.

Fig. 6. Original file

Mapped Points

(1308, 2605), (4694, 1830), (4755, 2646), (2368, 5072), (5033, 2819), (4755, 2646), (2368, 5072), (5033, 2819), (1308, 2605), (4694, 1830), (4941, 2906), (5033, 2819), (3370, 4568), (2492, 3496), (2282, 2431), (1041, 2726), (4755, 2646), (4160, 1049), (2428, 4710), (5033, 2819), (2492, 3496), (419, 3613), (5033, 2819), (4941, 2906), (263, 4812), (263, 4812), (5033, 2819), (734, 3869), (3939, 3127), (5033, 2819), (1839, 1945), (5033, 2819), (4160, 1049), (4941, 2906), (3370, 4568), (5033, 2819), (3370, 4568), (1839, 1945), (3939, 3127), (5033, 2819), (1308, 2605), (2492, 3496), (5033, 2819), (1759, 2638), (1839, 1945), (4473, 3284), (5033, 2819), (1308, 2605), (4941, 2906), (4961, 1976), (1308, 2605), (5033, 2819), (1308, 2605), (2492, 3496), (5033, 2819), (4473, 3284), (2492, 3496), (4755, 2646), (4160, 1049), (1308, 2605), (2368, 5072), (5033, 2819), (2492, 3496), (4160, 1049), (5033, 2819), (4941, 2906), (4849, 364), (4849, 364), (4755, 2646), (4473, 3284), (1308, 2605), (4755, 2646), (263, 4812), (5033, 2819), (263, 4812), (1820, 168), (2282, 2431), (2456, 1011), (4941, 2906), (2368, 5072), (1254, 4935)

Fig. 7. Mapped points

Encrypted points:
Encrypted with kG= (4649, 511)

(2790, 4193), (1933, 3690), (305, 465), (22, 191), (244, 2729), (305, 465), (22, 191), (244, 2729), (2790, 4193), (1933, 3690), (3273, 4679), (244, 2729), (3567, 1044), (4290, 3597), (2222, 66), (4511, 3217), (305, 465), (1868, 3547), (3601, 490), (244, 2729), (4290, 3597), (1730, 3101), (244, 2729), (3273, 4679), (2151, 4413), (2151, 4413), (244, 2729), (1893, 1677), (4684, 4324), (244, 2729), (3478, 3688), (244, 2729), (1868, 3547), (3273, 4679), (3567, 1044), (244, 2729), (3567, 1044), (3478, 3688), (4684, 4324), (244, 2729), (2790, 4193), (4290, 3597), (244, 2729), (2301, 658), (3478, 3688), (3706, 746), (244, 2729), (2790, 4193), (3273, 4679), (4306, 2293), (2790, 4193), (244, 2729), (2790, 4193), (4290, 3597), (244, 2729), (3706, 746), (4290, 3597), (305, 465), (1868, 3547), (2790, 4193), (22, 191), (244, 2729), (4290, 3597), (1868, 3547), (244, 2729), (3273, 4679), (4522, 4126), (4522, 4126), (305, 465), (3706, 746), (2790, 4193), (305, 465), (2151, 4413), (244, 2729), (2151, 4413), (4091, 4687), (2222, 66), (3190, 3892), (3273, 4679), (22, 191), (244, 2442)

Fig. 8. Encrypted Points

Contents of the file after decryption:

this is the working of ecc by a new way to map text to points on elliptic curves.

Fig. 9. Decrypted file

Image considered for encryption

Fig. 9. Original Image

Mapped Points:

(2582, 4642), (461, 2900), (2582, 4642), (614, 1012), (3502, 2660), (1253, 4045), (2222, 66), (1868, 3547), (3477, 1516), (1868, 3547), (3502, 2660), (1491, 2461), (1491, 2461), (3502, 2660), (3502, 2660), (1491, 2461), (3502, 2660), (1491, 2461), (3502, 2660), (3502, 2660), (2582, 4642), (4485, 1323), (3502, 2660), (4520, 4489), (3502, 2660), (1294, 2118), (244, 2442), (3708, 891), (2575, 3363), (2575, 3363), (2575, 3363), (1647, 3726), (2575, 3363), (2575, 3363), (2575, 3363), (2331, 1865), (2331, 1865), (2331, 1865), (2331, 1865), (1402, 3211), (4289, 4646), (2575, 3363), (2331,1865),(2331,1865),(2405,377),(2405,2377),(2405,2377),(2331,1865),(2405,2377),……... (4677, 4972), (668, 3164), (668, 3164), (3502, 2660), (2283, 852), (2283, 852), (1651, 3571), (668, 3164), (5033, 2819), (3220, 3202), (2283, 852), (4677, 4972), (668, 3164), (668, 3164), (3502, 2660), (2283, 852), (2283, 852), (1651, 3571), (668, 3164), (5033, 2819), (3220, 3202), (2283, 852), (4677, 4972), (668, 3164), (668, 3164), (3502, 2660), (2283, 852), (2283, 852), (1651, 3571), (668, 3164), (5033, 2819), (3220, 3202), (2283, 852), (4677, 4972), (668, 3164), (668, 3164), (3502, 2660), (2283, 852), (2283, 852), (1651, 3571), (668, 3164), (5033, 2819), (3220, 3202), (2283, 852), (4677, 4972), (2582, 4642), (4151, 3676)

Fig. 10. Mapped points

Encrypted points:
Encrypted with kG= (4649, 511)

(4800, 5105), (4151, 3676), (4800, 5105), (532, 1298), (3502, 2660), (2293, 1348), (22, 191), (4290, 3597), (2222, 66), (4290, 3597), (3502, 2660), (1651, 3571), (1651, 3571), (3502, 2660), (3502, 2660), (1651, 3571), (3502, 2660), (1651, 3571), (3502, 2660), (3502, 2660), (4800, 5105), (561, 715), (3502, 2660), (304, 4955), (3502, 2660), (4998, 1207), (3708, 891), (3220, 3202), (1647, 3726), (1647, 3726), (1647, 3726), (1866, 4640), (1647, 3726), (1647, 3726), (1647, 3726), (2405, 2377), (2405, 2377), (2405, 2377), (2405, 2377), (65, 2833), (1402, 3211), (1402, 3211), (2405, 2377), (2405, 2377), (2405, 2377), (2405, 2377), (2405, 2377), (2405, 2377), (2405, 2377), (1402, 3211), (1647, 3726), (2405, 2377), (2405, 2377), (4289, 4646), (4289, 4646), (4289, 4646), (2405, 2377), (4289, 4646),(2405,2377),(65,2833),(930,5128),...
....(2778, 4916), (4176, 1756), (3069, 686), (1420, 4264), (1294, 2118), (638, 1766), (593, 4503), (3069, 686), (3069, 686), (3502, 2660), (638, 1766), (638, 1766), (4176, 1756), (3069, 686), (1420, 4264), (1294, 2118), (638, 1766), (593, 4503), (3069, 686), (3069, 686), (3502, 2660), (638, 1766), (638, 1766), (4176, 1756), (3069, 686), (1420, 4264), (1294, 2118), (638, 1766), (593, 4503), (3069, 686), (3069, 686), (3502, 2660), (638, 1766), (638, 1766), (4176, 1756), (3069, 686), (1420, 4264), (1294, 2118), (638, 1766), (593, 4503), (3069, 686), (3069, 686), (3502, 2660), (638, 1766), (638, 1766), (4176, 1756), (3069, 686), (1420, 4264), (1294, 2118), (638, 1766), (593, 4503), (4800, 5105), (2829, 258)

Fig. 11. Encrypted points

Decrypted Image:

Fig. 12. Decrypted Image

VII. CONCLUSION

ECC is a faster encryption technique when compared to other techniques in the same group. It can also be used for key exchange and digital signatures.

In this paper we explained the math behind working of ECC and proposed a technique for mapping bytes to point on ECC. The technique we proposed in this paper allows for encryption of 8 bits at a time only. Enthusiasts may extend this technique to encrypt more number of bits at a time.

REFERENCES

1. Chia Long Wu, Chen Hao Hu. Modular Arithmetic Analyses for RSA Cryptosystem. Proc. of 2014 International Symposium on Computer,Consume and Control, IEEE Press,10-12 June 2014: 816-819.
2. Dong young Roh, Sang Geun Hahn.On the bit security of the weak Diffie–Hellman problem. Information Processing Letters, Volume 110, Issues 18-19, 15 September 2010, Pages 799-802.
3. Lin YOU, Yong-xuan SANG. Effective generalized equations of secure hyperelliptic curve digital signature algorithms. The Journal of China Universities of Posts and Telecommunications, Vol.17(2),2010:100-108
4. R. Schoof: Counting Points on Elliptic Curves over Finite Fields Journal de Theorie des Nombres. de Bordeaux 7 (1995), 219-254
5. Richard L. Roth Mathematics Magazine Vol. 74, No. 2 (Apr., 2001), pp. 99-108
6. http://andrea.corbellini.name/2015/05/23/elliptic-curvecryptography-finite- fields-and-discrete-logarithms
7. Robert Granger, Thorsten Kleinjung1, and Jens Zumbragel. Breaking `128-Bit Secure' Supersingular Binary Curves (or how to solve discrete logarithms in F24•1223 and F212•367). arXiv:1402.3668 [cs,Math], February 15, 2014.
8. Omar Reyad, Text Message encoding based on Elliptic curve and Mapping Methodology, Inf. Sci. Lett. 7, No. 1, 7-11 (2018)

AUTHORS PROFILE

Ch. Udaya Bhaskar, is now an Associate professor in the C.S.E. Department of Aditya Engineering College. He is Currently working towards Ph.d in Information security at JNTUK.. His research interests include Cloud computing and Machine learning.

Dr. A. Krishna Mohan Second is now a Professor in the Department of C.S.E ., UCEK, JNTUK, Kakinada.
He has a vast teaching and research experience. He has a good number of publications in reputed journals. His research interests include Data mining, Big data, and Information security.