Research Inventy: International Journal Of Engineering And Science
Vol.5, Issue 6 (June 2015), PP 06-12
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Elliptic Curves as Tool for Public Key Cryptography

[1] Srinivas Madhira, [2]Sammulal Porika
[1] (*Research Scholar, Department of CSE, JNTUH, Hyderabad, Telangana, India.,*
[2](*Assistant Professor, Department of CSE, JNTUHCEJ, Jagityal, Telangana.,*

ABSTRACT - *Cryptography is the technique of transforming an intelligible message into unintelligible format so that the message can't be read or understood by an unauthorized person during its transmission over the public networks. A number of cryptographic techniques have been developed over the centuries. With technological advancement, new techniques have been evolved significantly. Public key cryptography offers a great security for transmitting data over the public networks such as Internet. The popular public key cryptosystems like RSA and Diffie- Hellman are becoming slowly disappearing because of requirement of large number of bits in the encryption and decryption keys. Elliptic Curve Cryptograph (ECC) is emerging as an alternative to the existing public key cryptosystems. This paper describes the idea of Elliptic Curve Cryptography (ECC) and its implementation through two dimensional (2D) geometry for data encryption and decryption. This paper discusses the implementation of ECC over prime field. Much attention has been given on the mathematics of elliptic curves starting from their derivations.*

Keywords – *decryption, discrete Logarithm, Elliptic Curve (EC), Elliptic Curve Cryptography (ECC), encryption, private-key, public-key.*

I. Introduction

Elliptic Curve Cryptography (ECC) is completely a newer approach, and considered as an excellent technique in the history of cryptography. ECC was discovered in 1985 by Neil Koblitz and Victor Miller [4]. It is an asymmetric key cryptosystem. It is possible to generate public and private keys with elliptic curves. The existing popular cryptosystems like RSA [1] requires large length keys which increase the computational burden on the processor as a result of it, the cryptosystem becomes slow. Use of large size keys in RSA cryptosystem is essential in order to thwarts bruteforce attack [3]. The great feature of ECC is that with lower key size, it has a hard exponential time challenge for an opponent to break into the system [4] [5][6][7]. In ECC, a 160-bit key offers the same level of security as compared to the security offered by popular public key cryptosystem RSA [1] with a 1024-bit key and Diffie-Hellman crypto system [2]. Thus, ECC provides great security with smaller key sizes reducing the computational overhead on the processor and resulting in faster encryption/decryption operations [5]. ECC is used to implement a variety of public key cryptosystems for encryption/decryption, key exchange and digital signature applications [7]. Elliptic curve cryptography uses complex mathematical operations and is not easy to understand like other pubic key cryptosystems [4] [5]. Hence, it is not easy to break the cryptosystem. The choice of elliptic curve is dependent on its domain parameters, the finite field, elliptic curve algorithms and as well as elliptic curve arithmetic [5]. The selection of these parameters decides the security of ECC. ECC makes use of elliptic curves defined over a finite field [6]. A finite field restricts the variable and coefficients to its elements. Elliptic Curves are not ellipses, and they are named because of the nature of equation that generates the elliptic curve appears to be same as ellipses. For cryptographic processes it is necessary that the elliptic curves be defined over a finite field, typically a prime finite field, so that the decryption process is carried out within the range of the elements. Otherwise, it will not be possible to apply the cryptographic process [6]. In this paper, we have focused on the derivations of the elliptical curves, operations on elliptic curves and how they are used in encryption and decryption applications.

II. What is Elliptic Curve?

An elliptic curve E, over a finite field R, of real numbers is defined by a cubic equation

$$y^2 + a_1xy + a_3 y = x^3 + a_2x^2 + a_4x + a_6$$

Here a_1, a_2, a_3, a_4 and a_6 are real numbers belong to R, x and y takes values from the finite field of real numbers. Two families of elliptic curves are widely used in cryptographic applications: Prime curves defined over Z_P and binary curves defined over $GF(2^m)$ [7]. For a prime curve over Z_P , we use a cubic equation in which the variables and the coefficients all take values from the set of integers from 0 through (p-1) and the calculations are performed with respect to modulo p.

In this paper, for the purpose of the encryption and decryption using elliptic curves, it is sufficient to consider the equation of the form

$$y^2 = x^3 + ax + b \qquad (1)$$

which is defined over a finite field of prime numbers Z_P, where 'p' is a large prime number [4]. The variables x and y, the constants a and b takes the values from the finite field Z_P. For the given values of a and b the plot consists of positive and negative values of y for each value of x. Thus, this curve is symmetric about the x-axis. For the polynomial,

$$x^3 + ax + b$$

the discriminant can be given as

$$D = - (4a^3 + 27b^2) \qquad (2)$$

This discriminant must not become zero for an elliptic curve polynomial $x^3 + ax + b$ to possess three distinct roots [4]. If the discriminant is zero, that would imply that two or more roots have coalesced, giving the curves in singular form. It is not safe to use singular curves for cryptography as they are easy to crack. Due to this reason we generally take non-singular curves for data encryption [4].

III. Elliptic Curve Arithmetic

3.1 Group Laws of E(Z_P)

Let EP(a, b) be an elliptic curve defined over the Z_P, there is a chord-and-tangent rule for adding two points in E(Z_P), to give the third point. Together with this addition operation, the set of points of E_P(a, b) forms an abelian group with ∞ , the point at infinity O as identity elements [4][7].

3.2 Geometric Rules of Addition for Adding Two Points on An Elliptic Curve over Z_P

Let Z_p be the set of finite integers, where p is a large prime number. In Fig. 1. Given two points P = (x_1, y_1) and Q = (x_2, y_2) on an elliptic curve E(a,b) defined over Z_P, we have to compute the point P + Q.

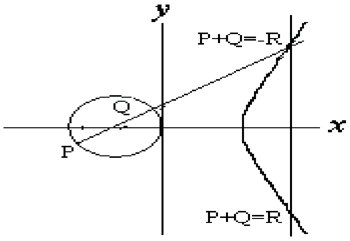

Fig.1. Elliptic Curve for $y^2 = x^3 – x$

Draw a straight line through points P and Q on elliptic curve. Next, find the third intersection of the line with the elliptic curve and denote this point of intersection by R. Then, it can be evident that P + Q is equal to the mirror image of R about the x-axis. In other words, if points P, Q and -R are the three intersections of the straight line with the elliptic curve, then

$$P + Q = - R \qquad (3)$$

The algebraic relationship between these three points of intersection can be examined as follows. The equation of the straight line that runs through two points P(x_1, y_1) and Q(x_2, y_2) is in the form of

$$y = \alpha x + \beta \pmod p \qquad (4)$$

where, α is the slope of the straight line and can be expressed as

$$\alpha = (y_1 - y_2) / (x_1 - x_2) \pmod p \qquad (5)$$

For a point (x, y), to lie at the intersection of the straight line and the elliptic curve E(a,b), the following equality should hold

(6)

$$(\alpha x + \beta)^2 = x^3 + ax + b \pmod p$$

Since, $y = \alpha x + \beta \pmod p$ is the straight line through the points P and Q and the equation of the elliptic curve is

$$y^2 = x^3 + ax + b$$

for there to be three points of intersection between the straight line and the elliptic curve, the cubic form in equation (6) must have three roots. We have known two of these roots, since they must be x_1 and x_2, corresponding to the points P and Q respectively. Being a cubic equation, equation (6) has at most three roots and the remaining root x_3 is the x-coordinate of the third point R. Further, equation (6) represents a monic polynomial in x. By the use of the property that sum of the roots of the monic polynomial must equal to the negative of the coefficient of the second highest power and expressing equation (6) with the rearrangements of terms as

$$x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + (b - \beta^2) = 0 \qquad (7)$$

Then, we have

$$x_1 + x_2 + x_3 = \alpha^2$$

The x-coordinate of R is then given by

$$x_3 = \alpha^2 - x_1 - x_2 \pmod p \qquad (8)$$

Since the point (x_3, y_3) must be on the straight line

$$y = \alpha x + \beta (\mathrm{mod}\ p)$$

we can write y_3 as

$$y_3 = \alpha x^3 + \beta (\mathrm{mod}\ p) \qquad (9)$$

Since, the point (x_1, y_1) is also on the straight line

$$y = \alpha x + \beta (\mathrm{mod}\ p)$$

we can write y_1 as

$$y_1 = \alpha x_1 + \beta \pmod p$$

$$\beta = y_1 - \alpha x_1 \qquad (10)$$

from equations (9) and (10), we can write y_3 as

$$y_3 = \alpha (x_3 - x_1) + y_1 (\mathrm{mod}\ p) \qquad (11)$$

Further, since the y-coordinate of the reflection -R is negative of the y-coordinate of the point R on the intersecting straight line, using the relation (3) we can write equation (11) as

$$y_3 = \alpha (x_1 - x_3) - y_1 \pmod p \qquad (12)$$

We can summarize that ordinarily a straight line intersects an elliptical curve at three points and if the co-ordinates of the first two points are known then the co-ordinates of the third point can easily be obtained from the equations (8) and (12).

3.3 Doubling the point on the elliptic curve

Let $P(x_1, y_1)$ be the point on the elliptic curve E(a, b), here we need to calculate 2P. In order to calculate 2P, we draw the tangent at $P(x_1, y_1)$ on elliptic curve E(a, b), the tangent intersects the EC at a point –R, which is the mirror image of point R (x_3, y_3) on EC about x-axis as shown in fig.2.

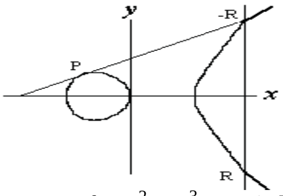

Fig.2. Elliptic Curve for $y^2 = x^3 - x$, (where 2P = -R)

The slope of the tangent at a point (x_1, y_1) is obtained by differentiating both sides of the curve equation (2), that is

$$2y_1 (dy/dx) = 3x_1^2 + a$$

Therefore, we can write the following expression for the slope of the tangent at point P:

$$\alpha = (3x_1^2 + a)/ 2y_1 \pmod p \tag{13}$$

Since, the tangent at P is the limiting case of drawing a line through P and Q as Q approaches P, two of the three roots of the following equation

$$(\alpha x + \beta)^2 = x^3 + ax + b \pmod p$$

must coalesce into the same point, say x_1 and the third root, say x_3 that may be different. Consequently, as above we get

$$x_3 = \alpha^2 - 2x_1 \pmod p \tag{14}$$

Since, the point R must also lie on the straight line $y = \alpha x + \beta$, it can be written as

$$y_3 = \alpha x_3 + \beta \tag{15}$$

Since, point P is also on the tangent (straight line) $y = \alpha x + \beta$, it can be written as

$$y_1 = \alpha x_1 + \beta$$

by rearranging the words, it can be written as

$$\beta = y_1 - \alpha x_1 \tag{16}$$

Substituting equation (16) in equation (15) yields

$$y_3 = \alpha x_3 + (y_1 - \alpha x_1)$$

$$y_3 = \alpha (x_3 - x_1) + y_1 \tag{17}$$

If we take the condition 2P = -R, then we have

$$y_3 = \alpha (x_1 - x_3) - y_1 \pmod p \tag{18}$$

Thus, for a given point P(x_1, y_1) on EC, its double or 2P can be obtained from equations (14) and (18).

3.4 Multiplication of P(x, y) with an integer K on Elliptic Curve

Let P(x, y) be any point on the elliptic curve E(a, b) defined over Z_P. Then, the operation of multiplication of the point P with an integer K is defined as the repeated addition of P, K times i.e.

$$K*P = P + P+\ldots\ldots\ldots\ldots\ldots\ldots..K \text{ times} \tag{19}$$

3.5 Negative of a point P(x, y) on Elliptic curve

Let P(x, y) be any point on the elliptic curve E(a, b) defined over Z_P. Then, the negative of the point P(x, y) is represented as –P(x, -y) which also lies on the EC. The sum of a point with its negative point is ∞ i.e.

$$P+(-P)=\infty \tag{20}$$

3.6 Identity Element on Elliptic curve

Let E(a, b) is an elliptic curve defined over Z_P, $P(x_1, y_1)$ and $Q(x_2, y_2)$ be the points on elliptic curve, then, identity element O of elliptic curve E(a, b) is defined as

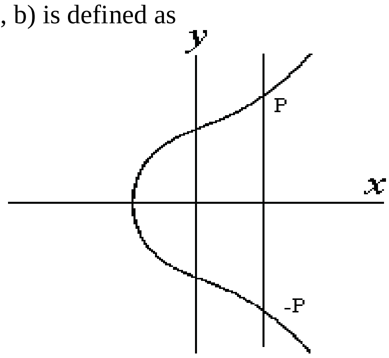

Fig.3. Elliptic Curve for y2 = x3 + x+1

(i) If $x_1 = x_2$ and $y_1 \neq y_2$, then P + Q = O
(ii) If P = Q and y_1= 0, then P + Q = O

IV. Encryption and Decryption using elliptic curves

Elliptic curves are widely used in implementing variety of public key cryptosystems including encryption/decryption, key exchange and digital signature cryptosystems. The section 4.1 focuses on the encryption process and section 4.2 focuses on decryption process.

4.1. Encryption using Elliptic curves

In ECC, we start with a Base Point (B_P) and an affine point A_P (x, y). A Base Point is the smallest co-ordinate on the elliptic curve, satisfying the elliptic curve equation. An affine point A_P may or may not be the Base Point, if it is not base point it should be close to the base point B_P.

To perform encryption, take first character from plain text, find out the ASCII code of that character and use it as an integer. Multiply pre-selected affine point (A_P) with the integer (ASCII code of the character) that gives another affine point on the EC, thus, plain text character is converted into another affine point (ciphet text) on EC. That is, assume that the ASCII value of some plain text character is p, A_P is an affine point on elliptic curve E(a, b), then we need to determine A_{PL} as follows

$$A_{PL}= p*A_P \tag{21}$$

Where, the newly calculated A_{PL} is another affine point on EC. The multiplication is achieved by applying repeated addition strategies of ECC techniques. Then as per ECC algorithm, we have to add the newly obtained point A_{PL} to $k*PU_B$, where k is a randomly generated large secret integer and PU_B is the public key of receiver (User B). The addition yields another affine point ($A_{PL}+ k*PU_B$) of the EC. This is the second part of the encrypted message to be sent. The first part constitutes the product of secret integer k and Base Point B_P, i.e. k*BP. Thus, the encrypted message to be sent to the receiver is

$$(k*B_P, A_{PL}+k*PU_B) \tag{22}$$

These are two sets of co-ordinates on the EC which are considered to the cipher characters for first plain text character. This process is repeated for each plain text character and a pair of cipher text characters are generated for each plain text character and they are transmitted to the destination.

4.2. Decryption using Elliptic curves

To perform decryption, the receiver applies its private key, PR_B, on the first part of the points received from the source i.e. first part of quation (22) , i.e., $k*B_P$

$$k*B_P*PR_B \qquad (23)$$

Since,

$$PU_B=B_P * PR_B, \qquad (24)$$

the equation (23) becomes

$$k* PU_B \qquad (25)$$

Now, by subtracting the equation (25) from the second part of the received message (second part of equation 22), which gives the A_{PL}.

Once A_{PL} is obtained, from equation (21), it is possible retrieve the ASCII value stored in the affine point. From this ASCII value, the plain text character can be obtained.

V. Strength of ECC

The security due to ECC relies on the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP). Let P and Q be two points on an elliptic curve such that k*P = Q, where k is a scalar. Given P and k, it is computationally easy to calculate the point Q on elliptic curve. But, given P and Q, it is computationally difficult to calculate the value of k. If k is sufficiently large, it becomes infeasible to calculate k. k is called the discrete logarithm of Q to the base P. Hence, the main operation involved in ECC is computation of product of an integer with a point on EC i.e. multiplication of a scalar k with any point P on the EC to obtain another point Q on the EC.

VI. Conclusion

In this paper, we have provided a detailed overview of elliptic curve cryptography along with the derivation of equations over the finite prime field. The strength of the ECC has been discussed in comparison with popular public key cryptosystems. A method of encryption and decryption using ECC has also been discussed. Moreover, ECC can be used to develop varieties of public key cryptosystems. Today, ECC algorithms have been in use in many real time applications such as Secures Socket Layers and E-Commerce applications. Even, the low cost chip implementation of ECC algorithms have been developed and slowly they started embedding in the commercial security products. It is expected that soon the ECC is will replace all popular public key cryptosystems such as RSA and Diffie-Hellman cryptosystems.

VII. Acknowledgements

I would like to express my sincere gratitude to the Management and Principal of Swarna Bharathi Institute of Technology(SBIT), Khammam for their strong support and encouraging us for publishing the papers. I would also like to thank Mrs. S. Neelima, Assoc. Prof., Department of Computer Science & Engineering, SBIT and Mrs. Y. Laxmi Prasanna, Assoc. Prof., Department of Computer Science & Engineering, SBIT for giving their valuable suggestions during preparation of this technical paper.

References

[1] R.L.Rivest, A.Shamir and L.Adleman: A Method for obtaining digital signatures and public key cryptosystems. Technical report, Laboratory for Computer Science, MIT (1978)

[2] Whitfield Diffie, Martin E Hellman: New directions in Cryptography. In: 10th IEEE International Symposium on Information Theory, pp. 29--40. Ronneby, Sweden, June 21-24, 1976.

[3] Matt Blumenthal: Encryption:Strength and Weaknesses of Public Key Cryptography, Department of Computer Sciences, Villanova University, Villanova (1999)

[4] Victor S. Miller: Use of elliptic curves in cryptography, Exploratory of Computer Sciences, IBM Research, Yorktown Heights, NewYork, 1998.

[5] Tarun Narayan Shanker, G.Sahoo: Cryptography with elliptic curves. IJCSA, Vol.2 Issue.1, pp 38—42, April/May 2009

[6] Ikshwansu Nautiayal, Madhu Sharma: Encryption using Elliptic Curve Cryptography using Java as implementation tool.IJARCSSE, Vol.4 Issue.1, pp. 620—625, Jan 2014

[7] D.Sravana Kumar, Ch.Suneetha, A.Chandrasekhar: Encryption of data using Elliptic Curves over Finite fields, IJDPS, Vol.3 Issue.1, pp. 301—308, Jan 2012

Mr. Madhira Srinivas, working as an Associate Professor in the Department of Computer Science and Engineering(CSE), Swarna Bharathi Institute of Science & Technology(SBIT), Khammam. He obtained B.Tech degree from REC, Warangal and M.Tech degree from JNTUH, Hyderabad. Now he is pursuing Ph.D. in Computer Science and Engineering from JNTUH, Hyderabad. His research areas include Cryptography & Network Security, Computer Networks, Unix Internals, Computer Graphics and Operating Systems.

Dr. Porika Sammulal, working as an Assistant Professor in the Department of Computer Science & Engineering(CSE) of JNTUH College of Engineering, Jagityal. He obtained Ph.D from Osmania University(OU), Andhra Pradesh and M.Tech degree from JNTUH, Hyderabad. His areas of specialization includes Cryptography & Network Security, Data Mining and Warehousing, Grid Computing, Cluster Computing, Cloud Computing and UnixInternals.