CRYPTOGRAPHY WITH ELLIPTIC CURVES

Tarun Narayan Shankar
GMR Institute of Technology, Rajam,
Srikakulam, AP, Pin:-532127
Ph:-9440175353
tnshankar2003@yahoo.co.in

G. Sahoo
Dept. of computer science & Engineering
Birla Institute of Technology, Mesra, Ranchi- 835215
Ph:-9431187542
gsahoo@bitmesra.ac.in

ABSTRACT
The paper describes the basic idea of Elliptic Curve Cryptography(ECC) and its implementation through co-ordinate geometry for data encryption. Elliptic curve cryptography is an asymmetric key cryptography. It includes (i) public key generation on the elliptic curve and its declaration for data encryption and (ii) private key generation and its use in data decryption depended on the points on two dimensional elliptical curve. We also discuss the implementation of ECC on two finite fields, prime field and binary field. An overview of ECC implementation on two dimensional representation of plaintext coordinate systems and data encryption through Elgamal Encryption technique has been discussed. Much attention has been given here on the mathematics of elliptic curves starting with their derivations and the proof of how points upon them form an additive abelian group for cryptographic purposes, specifically results for the group formed by an elliptic curve over a finite field, E(Fp),E(F_2^m), and showing how this can form public key cryptographic systems for use in both encryption and key exchange. Finally, we describe how to encrypt the data with the alphabetical table.

Categories and Subject Descriptors
E.3. [**Data Encryption**]: Public key *cryptosystems*, standards.

General terms: - Algorithm, Security, Performance

Keywords:-Cryptography, Elliptic Curves, ECC, Keys, Field, Encryption, Decryption, Public, Private.

1 INTRODUCTION
Elliptic Curve Cryptography (ECC) is a newer approach, and considered as an marvelous technique with low key size for the user, and have a hard exponential time challenge for an intruder to break into the system. In ECC a 160-bit key provides the same security as compared to the traditional crypto system RSA[7] with a 1024-bit key, thus lowers the computer power. Therefore, ECC offers considerably greater security for a given key size. Consequently, a key with smaller size makes it possible a much more compact implementations for a given level of security, which means faster cryptographic operations, running on smaller chips or more compact software. 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. Elliptic curve cryptography 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 by Miller[3] and Koblitz[1].Elliptic curve cryptography is not easy to understand by attacker. So not easy to break.

The choice of the type of elliptic curve is dependent on its domain parameters, the finite field representation, elliptic curve algorithms for field arithmetic[6] as well as elliptic curve arithmetic. The optimum selection of these parameters also depends on the security conditions under consideration. There are several research papers on this subject available in the literature covering different areas like hardware and software implementations. In the above respect it can be mentioned here that one can define encryption points as e_i and e_j by a specified algorithm but it is not yet possible for the case of plain text. In this paper we have discussed about the encryption for cryptography with Elliptical curves E(F*p*) ,(F_2^m) and an attempt has been made to represent plaintext in two dimensional form with the help of an alphabetical table so that Elgamal encryption technique[10] can be used for the said ECC. It can be mentioned here that ECC produces both private key and public key. Private key is known as secret key. In symmetric key cryptography single key uses for both encryption and decryption. In asymmetric key algorithm it however uses only for decryption of encrypted message. In asymmetric key cryptography, public key is used for message encryption[2] and widely distributed for public. Elliptic curve cryptography is asymmetric key cryptography by nature.

For the completeness of the paper, the description and use of the elliptic curves is given in few of the subsequent section. In section 4 we describe the methodology for encryption for plaintext followed by conclusion in the last section.

2 ELLIPTIC CURVE CRYPTOGRAPHY(ECC)

2.1 What makes ECC Important? The Discrete Logarithm
The security due to ECC relies on the difficulty of Elliptic Curve Discrete Logarithm Problem. Let P and Q be two points on an elliptic curve such that kP = Q, where k is a scalar. Given P and Q, it is computationally infeasible to obtain k. If k is sufficiently

large, k is the discrete logarithm of Q to the base P. Hence the main operation involved in ECC is related to the point multiplication i.e. multiplication of a scalar k with any point P on the curve to obtain another point Q on the curve.

2.2 What is Elliptic Curve? Its Derivation and Use

Note that elliptic curves are not ellipses. They are so named because of the fact that ellipses are formed by quadratic curves. Elliptic curves are always cubic and have a relationship to elliptic integrals in mathematics [4][9] where the elliptic integral can be used to determine the arc length of an ellipse. An elliptic curve in its standard form is described by

$$y^2 = x^3 + ax + b \quad ...(2.1)$$

For the polynomial, $x^3 + ax + b$, the discriminant can be given as

$$D = -(4a^3 + 27b^2) \quad ...(2.2)$$

This discriminant must not become zero for an elliptic curve polynomial $x^3 + ax + b$ to possess three distinct roots. 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.

3 ELLIPTIC CURVE ARITHMETIC

3.1 3.1 An Algebraic Expression for Adding Two Points on An Elliptic Curve over F*p*.

Let F*p*, where *p* an odd prime number, be a prime finite field. In Fig(1.1), given two points $P = (x_1,y_1)$ and $Q = (x_2,y_2)$ on an elliptic curve E(a,b), we have to compute the point P + Q.

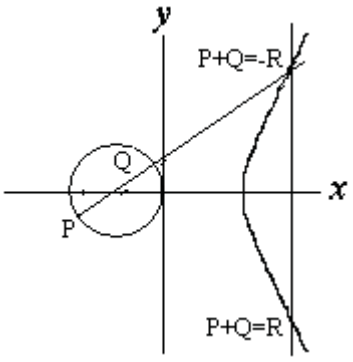

Figure 1.1 Algebraic curve for x^3 -x

We first draw a straight line through P and Q. Next, we find the third intersection of this line with the elliptic curve denote this point of intersection by R. Then P + Q is equal to the mirror reflection of R about the x-axis. In other words, if the points P, Q and -R are the three intersections of the straight line with the curve, then

$$P + Q = -R \quad \ldots(3.1)$$

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

$$y = \alpha x + \beta (\text{mod } p) \quad \ldots(3.2)$$

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

$$\alpha = (y_1 - y_2)/(x_1 - x_2) \ (\text{mod } p) \quad ...(3.3)$$

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

$$(\alpha x + \beta)^2 = x^3 + ax + b \ (\text{mod } p) \quad ...(3.4)$$

must hold. Since $y = \alpha x + \beta$ is the straight line through the points P and Q and the equation of the elliptic curve is

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

for there to be three points of intersection between the straight line and the elliptic curve, the cubic form in equation (3.4) must have three roots. We already know two of these roots, since they must be x_1 and x_2, corresponding to the points P and Q. Being a cubic equation, equation (3.4) has at most three roots and the remaining root x_3 is the x-coordinate of the third point R. Further, equation (3.4) 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 (3.4) as

$$x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + (b - \beta^2) = 0 \quad ...(3.5)$$

we can have

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

The x-coordinate of R is then given by

$$x_3 = \alpha^2 - x_1 - x_2 \ (\text{mod } p) \quad \ldots(3.6)$$

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

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

we can write y_3 as

$$y_3 = \alpha (x_3 - x_1) + y_1 \ (\text{mod } p) \quad ...(3.7)$$

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 (3.1) we can write

$$y_3 = -y_1 + \alpha (x_1 - x_3) \ (\text{mod } p) \quad ...(3.8)$$

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 as above.

3.2 Algebraic Expressions for Finding O

Let us consider the following figure(1.2).

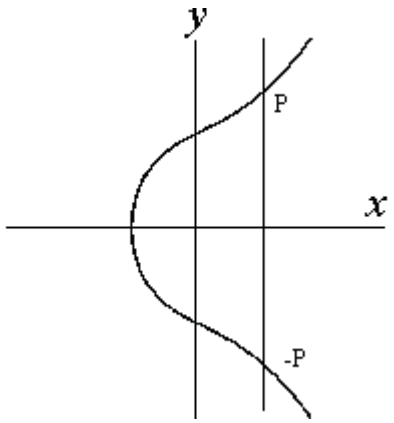

Figure 1.2 Algebraic curve for $x^3 + x + 1$

Now,

(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 $P + Q = O$

3.3 Expression for Calculating 2P from P.

The slope of the tangent at a point (x, y) is obtained by differentiating both sides of the curve equation (2.1), that is

$$2y\ (dy/dx) = 3x^2 + a$$

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

$$\alpha = 3x_1^2 + a / 2y_1 (\mathrm{mod}\ p) \qquad ...(3.9)$$

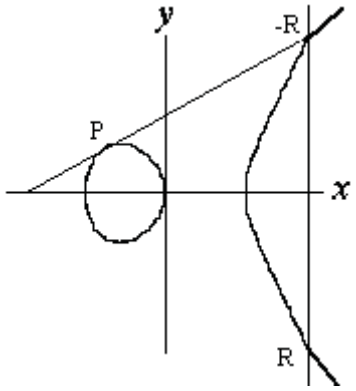

Figure 1.3 Algebraic curve for $x^3 - x$ (2P = -R)

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 .

$$(\alpha x + \beta)^2 = x^3 + ax + b\ (\mathrm{mod}\ p) \qquad ...(3.10)$$

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

$$x_3 = \alpha^2 - 2x_1\ (\mathrm{mod}\ p) \qquad ...(3.11)$$

Since the point R must also lie on the straight line

$$y = \alpha x + \beta$$

substituting (3.11) in this equation yields

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

$$y_3 = \alpha(x_3 - x_1) + y_1 \qquad ....(3.12)$$

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

$$y_3 = \alpha (x_1 - x_3) - y_1\ (\mathrm{mod}\ p) \qquad ...(3.13)$$

Similarly, for the same purpose if we consider elliptic curve over the, then field F_2^m [11]the addition of two points defined as

$$(x_1,y_1) + (x_2,y_2) = (x_3,y_3)$$

can be expressed as

$$(x_3,y_3) = (\alpha^2 + \alpha + x_1 + x_2 + a\ ,\ \alpha(x_1+x_3)+x_3+y_1) \qquad ...(3.14)$$

where

$$\alpha = (y_1+y_2)/(x_1+x_2)$$

3.4 Polynomial Arithmetic

Elliptic curve over field F_2^m[5][8]involves arithmetic of integer of length of m bits. These numbers can be considered as binary polynomial of degree m–1. The binary string

$(a_{m-1},\ldots a_1, a_0)$ can be expressed as polynomial

$$a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_2x^2 + a_1x + a_0$$

where a_i is either 0 or 1. For example, a 3-bit number 101_2 can be represented by the polynomial $x^2 + 1$.Similar to the modulus p operation on modular arithmetic, there is an irreducible polynomial of degree m in polynomial arithmetic. If in any operation the degree of polynomial is greater than or equal to m, the result is reduced to a degree less than m using irreducible polynomials. Analogous to the binary polynomial if in any operation the coefficient becomes greater than 1, it can be reduced to 0 or 1 by modulo 2 operation.

3.5 Irreducible polynomial

If in any polynomial arithmetic operation the resultant polynomial is having degree greater than or equal to m, it can be reduced to a polynomial of degree less than m by the irreducible polynomial. For $m \in \{113,131,163,193,233,239,283,409,571\}$ we just define here the following irreducible functions from the literature.

F_2113 : $f(x) = x^{113} + x^9 + 1$

F_2131 : $f(x) = x^{131} + x^8 + x^3 + x^2 + 1$

F_2163 : $f(x) = x^{163} + x^7 + x^6 + x^3 + 1$

F_2193 : $f(x) = x^{193} + x^{15} + 1$

F_2233 : $f(x) = x^{233} + x^{74} + 1$

F_2239 : $f(x) = x^{239} + x^{36} + 1$

F_2283 : $f(x) = x^{283} + x^{12} + x^7 + x^5 + 1$

F_2409 : $f(x) = x^{409} + x^{87} + 1$

F_2571 : $f(x) = x^{571} + x^{10} + x^5 + x^2 + 1$

4 PLAINTEXT ENCRYPTION

From the above basic theory on elliptic curve cryptography, in this section we describe the concept of plaintext encryption by defining a two-dimensional alphabetic table. It is worth noting that in the case of elliptic curve cryptography there is no specified rule and/ or algorithm to specify the letters of the English alphabet as well as special symbols. For this , a 6x5 table(Table 1) has been formed here for both the upper case and lower case letters of the English alphabet along with some of the other symbols like **,** , **.** , **?** and space for illustration purpose only. Other symbols of punctuation marks and special characters can also be considered in a similar way. Note that such tables play some important role in ECC as two-dimensional plaintext co-ordinate representation requires to add with any point on the elliptic curve.

Now, for any plaintext to be encrypted we add or multiply co-ordinates of a given character with selected points on the elliptic curve . For this purpose we consider the respective co-ordinates of the respective character. All the coordinate points should be on the surface of the elliptic curve**.** We illustrate the process with the following examples.

	0	1	2	3	4
0	A a	B b	C c	D d	E e
1	F f	G g	H h	I i	J j
2	K k	L l	M m	N n	O o
3	P p	Q q	R r	S s	T t
4	U u	V v	W w	X x	Y y
5	Z z	,	.	?	

Table 1. Two-dimensional alphabetical table.

Example 1. For the encryption plain text 'Boy', the two dimensional co-ordinate representation is

$\{P_1, P_2, P_3\}=\{(0,1),(2,4),(4,4)\}$

Example 2. When the text considered to be 'I am here' the required representation is

$\{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9\} = \{(1,3),(5,4),(0,0),(2,2),(5,4),(1,2),(0,4),(3,2),(0,4)\}$

It can be said here that for more security point of view the above alphabetic table may also be formed randomly, that is, by assigning any position in the table chosen randomly to any character or symbol. After defining an appropriate table, respective coordinates can be assigned as described below.

4.1 Algorithm 1(Alp_Tab_Val_Asn) :

Step 0. Generate appropriate alphabetic table

Step 1. Use an appropriate data structure to store the text to be encrypted.

Step 2. Read the table in row-major form and find the character stored in that position.

Step 3. Note the row and column values.

Step 4. Assign these values to the same character in all positions it appears.

Now, we define an analogous algorithm due to ElGamal[10] for encprypting the required text as follows:

4.2 Algorithm 2(Elp_Cur_Enc_Dec):

Step 0. Select E(a,b)with an elliptic curve over GF(p) or GF(2^m).

Step 1. Select a point on the curve $e_i = (x_i, y_i)$.

Step 2. Select g

Step 3. Calculate $e_j = (x_j, y_j) = g * e_i$

Step 4. Announce e_i ,e_j as public key and keep *"g"* as a private key.

Step 5. {Encryption} Now select h a number in plaintext P and calculate pair of points on the text as ciphertext.

Step 6. $C_i = h * e_i$

$C_j = (xp_i, yp_j) + h * e_j$ (Where plain text $P_i = (xp_i, yp_j)$)

Step 7. {Decryption} After receiving ciphertext C_i and C_j calculate

P(plain text) with the private key g .

$(xp_i, yp_j) = C_j - (g * C_i)$

[Here the (-)sign means adding with inverse.]

Step 8. Read the characters from the co-ordinates(xp_i, yp_j)

5 CONCLUSION

In this study, we provide a brief overview of elliptic curve cryptography and have developed an alphabetical table for ECC data encryption and decryption in a suitable manner. The strength of encryption depends on its key and if we use the alphabetical table then there will be no impact on strength and runtime performance. Runtime will be faster by this process, i.e. the use of alphabetical table will provide better performance in this regard.

Morever, Public key is used for message encryption in the case of socket layer security. It is clearly evident from the above that the alphabetical table described here can be used as a reference to build elliptic curve cryptography software for providing socket layer security.

6 REFERENCES

[1] Koblitz N., Menezes A.J., and Vanstone S.A. The state of elliptic curve cryptography. *Design, Codes, and Cryptography.* Vol 19, Issue 2-3, 2000, 173-193.

[2] Lenstra A., and Verheul E. *Selecting cryptographic key sizes*. Third International Workshop on Practice and Theory in Public Key Cryptography-PKC 2000. LNCS 1751, 2000.

[3] Miller V. Use of elliptic curves in cryptography. *Advances in Cryptography-Crypto '85*. LNCS 218, Springer Verlag, 1986,417-426.Silverman,The Arithmetic of Elliptic curves,Springer-Verlag,New york,1986.

[4] Tate,J.The arithmetic of elliptic curves .Invent.Math.23(1974),171-206.

[5] S. Bajracharya, C. Shu, K. Gaj, and T. El-Ghazawi, Implementation of Elliptic Curve Cryptosystems over GF(2n) in Optimal Normal Basis on a Reconfigurable Computer.

[6] Menezes A.J., Teske E., and Weng A. *Weak fields for ECC*.CORR 2003-15, Technical Report, University of Waterloo, 2003..

[7] Rivest R., Schamir A. and Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21, 1978, 120-126.

[8] C. Shu, S. Kwon, and K. Gaj, Reconfigurable Computing Approach for Tate Pairing Cryptosystems over Binary Fields *submitted to IEEE Transactions on Computers.*

[9] Certicom. Information on the Certicom ECC challenge,http://www.certicom.com/research/ecc hallenge.html

[10] ElGamal, T., A public key cryptosystem and a signature scheme based on discrete logarithm,IEEE Trans. Inform, Theory, IT-31, no.4, pp469-472, July 1985.

[11] Hankerson, D.,Hernandez, L. J., and Menezes A. Software implementation of elliptic curve cryptography over binary fields, CHESS 2000,LNCS 1965, 1-24,2000.