International Journal of
Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.02,Issue.19,
December-2013,
Pages:2186-2194

www.semargroups.org,
www.ijsetr.com

A Study of Elliptic Curves Cryptography

IBRAHIM QADER ALI[1], DR. SWAPNIL SRIVASTAVA[2]

[1]Research Scholar, Dept of Mathematics, SHIATS, Allahabad, UP-INDIA, E-mail: nahroindo@gmail.com.
[2]Asst Prof, Dept of Mathematics & Statics, SBS, SHIATS, Allahabad, UP-INDIA.

Abstract: Curve Cryptography (ECC) has been adopted by the US National Security Agency (NSA) in Suite "B" as part of its "Cryptographic Modernization Program ". Additionally, it has been favored by an entire host of mobile devices due to its superior performance characteristics. ECC is also the building block on which the exciting field of pairing/identity based cryptography is based. This widespread use means that there is potentially a lot to be gained by researching efficient implementations on modern processors such as IBM's Cell Broadband Engine and Philip's next generation smart card cores. ECC operations can be thought of as a pyramid of building blocks, from instructions on a core, modular operations on a finite field, point addition & doubling, elliptic curve scalar multiplication to application level protocols. This is a study about applying ideas from mathematical methodology to problems in cryptography. Elliptic curve cryptography (ECC) is becoming the algorithm of choice for digital signature generation and authentication in embedded context. Elliptic curve cryptography (ECC) is a kind of Public Key Cryptography founded in the theory of groups, the elliptic curve cryptography in real number over Galois Field $E_p(a,b)$ is obtained by computing $x^3 + ax + b \ mod \ p$ for $0 \leq x \leq p$. The constants a and b is non negative integers smaller than the prime number p and must satisfy the condition: $4a^3 + 27b^2 mod \ p \neq 0$ For each value of x, one need to determine whether or not it is an $quadratic \ residue$. if it is the case, then there are two values in the elliptic group. If not, then the point is not in the elliptic group $E_p(a,b)$. Then it given points on the Cartesian plan, those point can use in more application (radio, medical, …). Cryptography is a notoriously difficult subject to reason about: it is acknowledged within the cryptography community that many of the existing proofs are so complicated that they are near impossible to verify, However, performance of ECC and the underlying modular arithmetic on embedded processors remains a concern, ECC Analog of the Diffie-Hellman Key Exchange, Use the elliptic curve $Eq(a,b)$ and pick a point in the set $G = (x,y)$ such that G has a large order. if nG=0 (the point at infinity), but if $0 < nA < n$, For the key exchange both $Eq(a,b)$ and G are public elements. $P_A = nAG$ and $P_B = nBG$. A and B swap their "public" values and then calculate K, A calculates $K = nAPB$ and calculates $K = nBPA$. These are both equal to $n_An_BP_B$ and that one who intercepts P_A and P_B cannot calculate nA, nB, or K, due to the difficulty of the discrete log problem for elliptic curves. The Cryptographic Scheme Using Elliptic Curves use the elliptic curve $Eq(a,b)$ and pick a point in the set $G = (x,y)$ such that G has a large order. Cryptosystems have the potential to provide relatively small block size, high-security public key schemes that can be efficiently implemented. As with other known public key schemes, such as RSA and discrete exponentiation in a finite field, some care must be exercised when selecting the parameters involved, in this case the elliptic curve and the underlying field. Embedded plaintext to points in Elliptic curve there is Encryption and Decryption any message text by using the EC, we explain that in one example show how the point is encryption and decryption.

Keywords: Elliptic Curves Cryptography (ECC), Encryption and Decryption.

I. INTRODUCTION

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. The basic idea has remained constant: modify the message so as to make it unintelligible to anyone but the intended recipient. Typically, we represent a message M by a finite string of symbols from a finite alphabet. We use e(M) to denote the encryption of M and let d be the decrypting function satisfying the fundamental relationship.

$$d(e(M)) = M \qquad (1)$$

For all messages M in practice, e can be regarded as a function or algorithm with a collection of parameters. Any such parameter is called a key, and is usually denoted by K. The encrypted string is

$$C = e(M, K) \quad (2)$$

is called the cipher, cipher-text, or cryptogram; again, decryption obeys

$$d(C, K) = M. \quad (3)$$

The message M is often called the plaintext. Thus, formally, we define a cryptosystem to be a triple (M, K, C), where M and C are sets and K is the finite set of keys with the additional hypothesis that there exist functions (or algorithms) e and d such that $e : M \times K \rightarrow C, d : C \times K \rightarrow M,$ and, for each $(M,K)\, E\, M \times K, d(e(M,K),K) = M.$ We now describe several well known examples of cryptosystems. Throughout, will denote the language of the system, which we usually take to be the letters of the English alphabet, sometimes augmented by a 'blank' or 'space'.

II. RESIDUE AND RESIDUE THEORY ZERO OF ANALYTIC FUNCTION

A zero of analytic function $f(z)$ is the value of z for which $f(z) = 0$.

A. Singular point

A point at which a function $f(z)$ is not analytic is known as a singular point or singularity of the function. For example, the function $\frac{1}{z-2}$ has a singular point at $z - 2 = 0 \; or \; z = 2.$

1. Isolated singular point: If $z = a$ is a singularity of $f(z)$ and if there is no other singularity within a small circle surrounding the point $z = a$ is said to be an isolated singularity of the function f(z); otherwise it is called non-isolated. For example, the function $\frac{1}{(z-1)(z-3)}$ has two isolated singular points, namely z=1 and z=3, $[(z-1)(z-3) = 0 \; or \; z = 1,3]$ Example of non-isolated singularity. Function $\frac{1}{sin\frac{\pi}{z}}$ is not analytic at the points where $sin\ \frac{\pi}{z}$ =0 at the point $\frac{\pi}{z}$ = nπ , the point $z = \frac{1}{n}$ (n=1,2,3,…) Thus z =1, $\frac{1}{2}, \frac{1}{3}, \ldots, z = 0$ are the point of singularity, z=0 is the non-isolated singularity of the function $\frac{1}{sin\frac{\pi}{z}}$ because in the neighborhood of z=0 there are infinite number of other singularities $z = \frac{1}{n}$, where n is very large.

B. Pole of order m

Let a function F(x) nave an isolated singular point z=a can be expanded in a laurent's series around z=a, giving

1. Definition of the Residue at a Pole

Let $z = a$ be a pole of order m of a function $f(z)$ and C_1 circle of radius r with centre at $z = a$ which does not contain any other singularities except at $z - a$ then $f(z)$ is analytic within the annulus $r < |z - a| < R$ can be expanded within the annulus**.**

2. Residue at Infinity

Residue of $f(z)\ at\ z - \infty$ is defined as $-\frac{1}{2\pi i}\int_c f(z)\, dz$ Where the integration is taken round C in anti-clockwise direction. Where C is a large circle containing all finite singularities of $f(z)$.

3. Method of Fining Residues

a. Residue at simple pole

If $f(z)$ has a simple pole at $z = a$, then

$$Res\, f(z) = \lim_{z \to a}(z - a) f(z)$$
$$Res\ (at\ z = a) = \lim_{z \to a}(z - a) f(z) \quad (4)$$

If $f(z)$ is of the form

$$f(z) = \frac{\emptyset(a)}{\psi(a)} \quad (5)$$

Where $\psi(a) = 0, but\ \emptyset(a) \neq 0$

$$Res\ (at\ z = a) = \frac{\emptyset(a)}{\psi'(a)}$$

b. Residue at a pole of order n, if $f(z)$ has a pole of order n at $z = a$, then

$$Ras\ (at\ z = a) = \frac{1}{(n-1)!}\left\{\frac{d^{n-1}}{dz^{n-1}}[(z-a)^n f(z)]\right\}_{z=a} \quad (6)$$

c. Residue at a pole $z = a$ of any order (simple or of order m) $Res\, f(a) = coefficient\ of \frac{1}{t}$

d. Residue of $f(z)\ at\ z = \infty$

$$= \lim_{z \to \infty}\{-z f(z)\} \quad (7)$$

C. The Finite Field $\mathbb{F}_p^*$

The finite field $\mathbb{F}_p^*$is the prime finite field containing p elements. Although there is only one prime finite field $\mathbb{F}_p^*$for each odd prime p, there are many different ways to represent the elements of$\mathbb{F}_p^*$. Here the elements of $\mathbb{F}p$ should be represented by the set of integers: $\{0,1,2,3, \ldots . p-1\}$ with addition and multiplication defined as follows:[rodolf lidl, herald niederreiter 2005][(46)]

- Addition: If $a, b \in \mathbb{F}p$, then a+ b = r in $\mathbb{F}p$, where $r \in [0, p-1]$ is the remainder when the integer a+ b is divided by p. This is known as addition $modulo\, p$ and written $a + b \equiv r\ (mod\ p)$.

- Multiplication: If $a, b \in \mathbb{F}p$, then $a, b = s$ in $\mathbb{F}p$, where $s \in [0, p-1]$ is the remainder when the integer a b is divided by p. This is known as multiplication $modulo\ p$ and written $a.b \equiv s\ (mod\ p)$.

Addition and multiplication in $\mathbb{F}p$ can be calculated efficiently using standard algorithms for ordinary integer arithmetic. In this representation of $\mathbb{F}p$, the additive identity or zero element is the integer 0, and the multiplicative identity is the integer 1. It is convenient to define subtraction and division of field elements just as it is convenient to define subtraction and division of integers. To do so, the additive inverse (or negative) and multiplicative inverse of a field element must be described:

- Additive inverse: If $a \in \mathbb{F}p$, then the additive inverse $(-a)$ of $a\ in\ \mathbb{F}p$ is the unique solution to the equation $a + x \equiv 0\ (mod\ p)$.
- Multiplicative inverse: If $a \in \mathbb{F}p$, $a \neq 0$, then the multiplicative inverse a^{-1} of $a\ in\ \mathbb{F}p$ is the unique solution to the equation $a.x \equiv 1\ (mod\ p)$.

D. The Finite Field $\mathbb{F}2^m$

The finite field $\mathbb{F}2^m$ is the characteristic 2 finite field containing 2^m elements. Although there is only one characteristic 2 finite field $\mathbb{F}2^m$ for each power $2^m of\ 2$ with $m \geq 1$, there are many different ways to represent the elements of $\mathbb{F}2^m$. Here the elements of $\mathbb{F}2^m$ should be represented by the set of binary polynomials of degree $m-1$ or less: $\{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0;\ a_i \in \{0,1\}\}$ with addition and multiplication defined in terms of an irreducible binary polynomial $f(x)$ of degree m, known as the reduction polynomial, as follows:

- Addition: If $a = a_{m-1}x^{m-1} + \ldots a_0,\ b = b_{m-1}x^{m-1} + \ldots b_0 \in \mathbb{F}2^m$, then $a + b = r\ in\ \mathbb{F}2^m$, where $r = r_{m-1}x^{m-1} + \ldots r_0$ with $ri \equiv ai + bi\ (mod\ 2)$.
- Multiplication: If

$$a = a_{m-1}x^{m-1} + \ldots a_0,$$
$$b = b_{m-1}x^{m-1} + \ldots b_0 \in \mathbb{F}2^m, \text{ then}$$
$$a.b = s\ in\ \mathbb{F}2^m, \quad (8)$$

Where, $s = s_{m-1}x^{m-1} + \ldots s_0$, is the remainder when the polynomial ab is divided by $f(x)$ with all coefficient arithmetic performed modulo 2.

Addition and multiplication in $\mathbb{F}2^m$ can be calculated efficiently using standard algorithms for ordinary integer and polynomial arithmetic. In this representation of $\mathbb{F}2^m$, the additive identity or zero element is the polynomial 0, and the multiplicative identity is the polynomial 1.

E. Elliptic Curves Over $\mathbb{F}_p$

Let $\mathbb{F}_p$ be a prime finite field so that p is an odd prime number, and let $a, b \in \mathbb{F}_p$ satisfy $4.a^3 + 27.b^2 \neq 0 (mod\ p)$. Then an elliptic curve $E(\mathbb{F}_p)$ over $\mathbb{F}p$ defined by the parameters $a, b \in \mathbb{F}_p$ consists of the set of solutions or points $P = (x, y)$ for $x, y \in \mathbb{F}_p$ to the equation:

$$y^2 \equiv x^3 + a.x + b\ (mod\ p) \quad (9)$$

The addition rule is specified as follows:

1. Rule to add the point at infinity to itself:
   $O + O = O$.
2. Rule to add the point at infinity to any other point:

$$(x,y) + O = O + (x,y) = (x,y) for\ all\ (x,y) \in E(\mathbb{F}_p). \quad (10)$$

3. Rule to add two points with the same x-coordinates when the points are either distinct or have $y - coordinate\ 0$.

$$(x,y) + (x,y) = O\ for\ all\ (x,y) \in E(\mathbb{F}_p) \quad (11)$$

I.e. the negative of the point $(x, y)\ is\ (x, y) = (x, y)$.

4. Rule to add two points with different x-coordinates: Let $(x_1, y_1) \in E(\mathbb{F}_p))\ and\ (x_2, y_2) \in E(\mathbb{F}_p)$ be two points such that $x_1 \neq y_1$. Then

$$(x_1,y_1) + (x_1,y_1) = (x_3,y_3), \quad (12)$$

where:

$$x_3 \equiv \lambda^2 - x_1 - x_2 (mod\ p);$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1\ (mod\ p);$$
$$and\ \lambda \equiv \frac{y_2 - y_1}{x_2 - x_1} (mod\ p):$$

5. Rule to add a point to it (double a point): Let $(x_1, y_1) \in E(\mathbb{F}_p)$ be a point with $y1 \neq 0$. Then

$$(x_1,y_1) + (x_1,y_1) = (x_3,y_3), \quad (13)$$

Where: $x_3 \equiv \lambda^2 - 2.x_1\ (mod\ p);$
$y_3 \equiv \lambda(x_1 - x_3) - y_1 (mod\ p);$ and
$\lambda \equiv \frac{3x_1^2 + a}{2y_1}\ (mod\ p):$

The set of points on $E(\mathbb{F}_p)$ forms a group under this addition rules. Furthermore the group is abelian - meaning that $P_1 + P_2 = P_2 + P_1$, for all points $P_1, P_2 \in E(\mathbb{F}_p)$. Notice that the addition rule can always be computed efficiently using simple field arithmetic.

F. Elliptic Curves over $\mathbb{F}_{2m}$

Let $\mathbb{F}_{2m}$ be a characteristic 2 finite field, and let $a, b \in \mathbb{F}_{2m}$ satisfy $b \neq 0$ in $\mathbb{F}_{2m}$. Then a (non-super

singular) elliptic curve $E(\mathbb{F}_{2^m})$ over $\mathbb{F}_{2^m}$ defined by the parameters $a, b \in \mathbb{F}_{2^m}$ consists of the set of solutions or points $P = (x, y)$ for $x, y \in \mathbb{F}_{2^m}$ to the equation:

$$y^2 + x.y = x^3 + a.x2 + b \; in \; \mathbb{F}_{2^m} \tag{14}$$

Together with an extra point O called the point at infinity. (Here the only elliptic curves over $\mathbb{F}_{2^m}$ of interest are non-super singular elliptic curves). The number of points on $E(\mathbb{F}_{2^m})$ is denoted by $\#E(\mathbb{F}_{2^m})$. The Hasse Theorem states that:

$$2^m + 1 - 2\sqrt{2^m} \leq \#E(\mathbb{F}2^m) \leq 2^m + 1 + 2\sqrt{2^m} \tag{15}$$

It is again possible to define an addition rule to add points on E as it was in next Sections. The addition rule is specified as follows:

1. Rule to add the point at infinity to itself: $O + O = O$;
2. Rule to add the point at infinity to any other point:

$$(x,y) + O = O + (x,y) = (x,y) for \; all (xmy) \in E(\mathbb{F}_{2^m}); \tag{16}$$

3. Rule to add two points with the same x-coordinates when the points are either distinct or have x-coordinate:

$$(x,y) + (x, x+y) = O \; for \; all \; (x,y) \in E(\mathbb{F}_{2^m}) \tag{17}$$

I.e. the negative of the point (x, y) *is* $(x, y) = (x, x + y)$.

4. Rule to add two points with different x-coordinates: Let $(x_1, y_1) \in E(\mathbb{F}_{2^m})$ and $(x_2, y_2) \in E(\mathbb{F}_{2^m})$ be two points such that $x_1 \neq x_2$. Then

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3). \tag{18}$$

Where, $x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \; in \; \mathbb{F}_{2^m}$;

$$y_3 = \lambda.(x_1 + x_3) + x_3 + y_1 \; in \; \mathbb{F}_{2^m};$$

$$and \; \lambda = \frac{y_1 + y_2}{x_1 + x_2} \; in \; \mathbb{F}_{2^m};$$

5. Rule to add a point to itself (double a point): Let $(x_1, y_1) \in E(\mathbb{F}2^m)$ be a point with $x_1 \neq 0$. Then

$$(x_1, y_1) + (x_1, y_1) = (x_3, y_3), \tag{19}$$

Where, $x_3 = \lambda^2 + \lambda + a \; in \; \mathbb{F}_{2^m}$;

$$y_3 = x_1^{\,2} + (\lambda + 1).x_3 \; in \mathbb{F}_{2^m};$$

$$and \lambda = x_1 + \frac{y_1}{x_1} \; in \; \mathbb{F}_{2^m};$$

III. THE DISCRETE LOGARITHM PROBLEM

Let p be a prime and let a, b be integers that are nonzero mod p. suppose we know that there exists an integer k such that

$$a^k \equiv b \; (mod \; p). \tag{20}$$

The classical discrete logarithm problem is to find k. since k + (p − 1) is also a solution, the answer k should be regarded as being defined mod $p - 1$, or mod a divisor d of p − 1 if $a^d \equiv 1 \; (mod \; p)$.

IV. THE ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

The hardness of the elliptic curve discrete logarithm problem is essential for the security of all elliptic curve cryptographic schemes.

Definition: The elliptic curve discrete logarithm problem $(ECDLP)$ is: given an elliptic curve E defined over a finite field, a point $P \in E(\mathbb{F}_q)$ of order n, and a point $Q \in \langle P \rangle$, find the integer $l \in [0, n-1]$ such that $Q = lP$. The integer l is called the discrete logarithm of Q to the base P, denoted $l = log_P Q$.

A. Pollard's ρ Method

The space complexity of Pollard's algorithm depends on the implementation of the match finding procedure. The naive approach of storing the sequence entries (x_i, a_i, b_i) in a structure sorted by the first component (for instance in a balanced tree) and looking up later entries needs to store $O\sqrt{n}$ elements as Shanks's method. Pollard suggested a cycle finding technique due to Floyd, which consists of computing $(x_i, a_i, b_i, x_{2i}, a_{2i}, b_{2i})$ until $x_i = x_{2i}$. This happens as soon as i is a multiple of λ and not less than μ. Practically no storage space is required by this approach, since x_{i+1} and $x_{2(i+1)}$ can be computed from the previous values x_i and x_{2i} by three applications of the iterating function via $x_{i+1} = F(x_i)$ and $x_{2(i+1)} = F(F(x_i))$ Since Floyd's algorithm usually does not detect the first possible match, the expected value of i for which a match is detected is higher than the expected value of λ; for a true random mapping it is: $\frac{\pi^2}{12}\sqrt{\frac{\pi}{2}n} \approx 1.03\sqrt{n}$. Moreover, the values $x_1, \ldots\ldots, x_i$ are computed twice to obtain the sequences (x_i) and (x_{2i}), so that the total number of function evaluations is on average $3\frac{\pi^2}{12}\sqrt{\frac{\pi}{2}n} \approx 3.09\sqrt{n}$. The $p - method$ can be parallelized by starting the iterations on different machines and reporting the values obtained to a central server, which stores them and searches them for collisions. However, if all computed group elements were stored, then the time saved by the parallelization would be

more than compensated by the extra time needed on the central machine for the look-up of matches.

B. Pohlig-Hellman Method

If the group order n is not prime, then it is possible to take advantage of the factorization of n by breaking the discrete logarithm problem in G into a number of discrete logarithm problems in the Sylow groups of$G$, which are the maximal subgroups of prime power order. Moreover, in these groups the problem can be solved by iteratively taking logarithms in the subgroup of the corresponding prime order. Hence the following algorithm, which has been described in [Pohlig and Hellman, 1978] and has independently been discovered by Roland Silver, and Richard Schroeppel and$H$. Block runs in about $O(\sqrt{p}\log p)$ if p is the largest prime factor of n. The time needed for the combination of the results by the Chinese Remainder Theorem is in $O(r\ log_2 n)$ bit operations (see [Cohen, 1993], pp. 12-20); since a group element is represented by at least $log_2 n$ bits, any group operation takes at least $log_2 n$ bit operations, and the overall complexity of the algorithm remains unchanged by this last step.

C. Index Calculus Methods

By choosing n a large prime and noting that the input size of the discrete logarithm problem is in $\Omega(logn)$, it is easy to see that the algorithms presented so far are fully exponential. This is not incidental; Shoup showed in [Shoup, 1997] that any algorithm for computing discrete logarithms in an arbitrary group requires $\Omega(\sqrt{p}\log p)$steps, where$p$ is the largest prime factor of n. So in the generic setting one cannot hope to improve substantially on the Pohlig-Hellman method presented in the previous section. More efficient algorithms can only be developed for specific groups, exploiting additional structure.

1. Multiplication over an elliptic curve group

The multiplication over an elliptic group $E_p(a,b)$ is the equivalent operation of the modular exponentiation in RSA. Figure 1and 2 show the curve P+Q when $p \neq Q$ and 2p= p+p. Let $P=(3,10)\in E_{23}(1,1)$. *Then* $2P=(x_3,y_3)$ is equal to:

$$2P = P + P = (x_1,y_1) + (x_1,y_1) \tag{21}$$

Since P=Q and $x_2 = x_1$ the values of λ, x_3 and y_3 are given by:

$$\lambda = \frac{3x_1^2+a}{2y_1} mod p = \frac{3\times(3^2)+1}{2\times 10} mod\ 23 = \frac{5}{20} mod\ 23 = 4^{-1} mod\ 23 = 6$$
$$x_3 = \lambda^2 - x_1 - x_2\ mod p = 6^2 - 3 - 3\ mod\ 23 = 30\ mod 23 = 7$$
$$y_3 = \lambda(x_1 - x_3) - y_1\ mod p = 6\times(3-7) - 10\ mod 23 = -34 mod 23 = 12$$

Therefore $2P=(x_3,y_3)=(7,12)$. Since; Point $Q = nP$ multiplication-Repeated point addition and doubling:

$$2p = p + p$$
$$9p = 2(2(2p))p \tag{22}$$

-public key operation

$$Q(x,y) = kp(x,y) \tag{23}$$

Q=public key
P=base point (curve parameter)
n=order of p

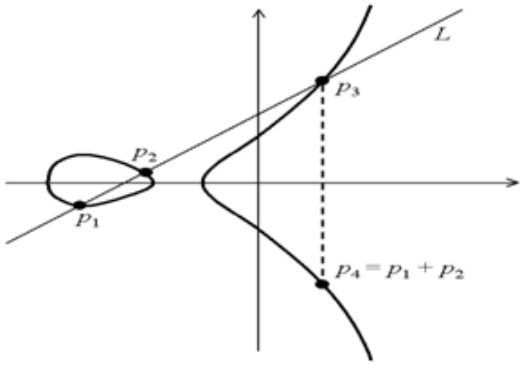

Fig 1: $P + Q\ when\ p \neq Q$

D. Elliptic curve discrete logarithm

Give public key kp find privet key$k$. Best known attack, pollard's rho method with running time $\frac{(\pi n)^{1/2}}{2}$. The multiplication kP is obtained by repeating the elliptic curve addition operation k times by following the same additive rules.

1. Examples

Example 1: Let $P=(3,10)$ and $Q=(9,7)$ in $E_{23}(1,1)$ Find $P+Q$?

$$\lambda = \frac{y_Q - y_P}{x_Q - x_p} mod_p = \frac{7-10}{9-3} = \frac{-3}{6} = (-3)(6^{-1}) mod_{23}$$
$$= -3(4) = -12 = 11 mod_{23} = 11 \quad \lambda = 11$$
$$x_R = \lambda^2 - x_P - x_Q\ mod_{23} = 11^2 - 3 - 9 = 109 = 17 mod_{23}$$
$$y_R = \lambda(x_P - x_R) - y_P = 11(3-17) - 10 = 11(-14) - 10$$
$$= 11(9) - 10 = 89 = 20 mod_{23} = 20$$

P+Q = (17, 20)

Example 2: Let $P=(3,10)$ and $Q=(9,7)$ in $E_{23}(1,1)$ Find $2p$?

$$\lambda = \frac{3x_1^2+a}{2y_1} mod p = \frac{3(3)^2+1}{2(10)} = \frac{28}{20} = \frac{7}{5} mod_{23}$$
$$= 7(5^{-1}) mod_{23} = 7(14) = 98 mod_{23} = 6 mod_{23} = 6$$

$$x_R = \lambda^2 - x_P - x_Q \bmod_{23} = 6^2 - 3 - 3 = 30 \bmod_{23} = 7 \bmod_{23} = 7$$
$$y_R - \lambda(x_P - x_R) - y_P \bmod p - 6(3-7) - 10 \bmod_{23}$$
$$= -24 - 10 = -34 = 12 \bmod_{23} = 12$$

2P = (7, 12)

Example 3: Let $P = (3,10)$ and $Q = (9,7)$ in $E_{23}(1,1)$ Find $4P$?

$$\lambda = \frac{3x_1^2 + a}{2y_1} \bmod p = \frac{3(7)^2 + 1}{2(12)} = \frac{148}{24} = \frac{148}{1} =$$
$$148(1^{-1}) \bmod_{23} = 148 = 10 \bmod_{23} = 10$$
$$x_R = \lambda^2 - x_P - x_Q \bmod_p = 10^2 - 7 - 7 = 86 = 17 \bmod_{23} = 17$$
$$y_R = \lambda(x_P - x_R) - y_P \bmod p = 10(7-17) - 12 =$$
$$-100 - 12 = -112 = 3 \bmod_{23} = 3$$

4P = 2(2P) = (17, 3) = -P, since 20 = -3 mod 23.

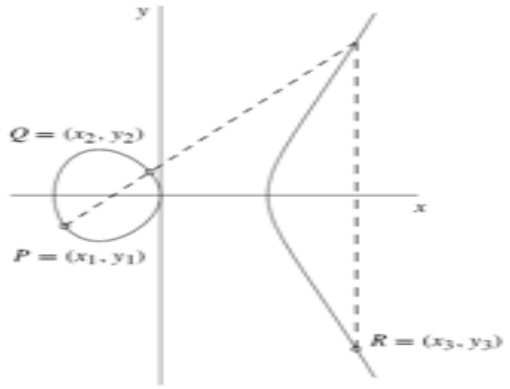

Fig 2: 2p=p+p

E. Embedded plaintext to points in Elliptic curve

If two communicating parties Alice and Bob want to communicate the messages then they agree upon to use an elliptic curve $Ep(a,b)$ where p is a prime number and α random point Q on the elliptic curve. Alice selects a large random number α which is less than the order of $Ep(a,b)$ and a point A on the elliptic curve. She computes $A_1 = \alpha(Q + A)$ and $A_2 = \alpha A$. She keeps the random number α and the point A as her private keys and publishes $A_1$and A_2 as her general public keys. Similarly Bob selects a large random number $\beta$and a point B on the elliptic curve. He computes $B_1 = \beta(Q + B)$ and$B_2 = \beta B$. He keeps the random number β and the point B as his private keys and publishes $B_1$and B_2as his general public keys. After publishing the public keys, the communicating parties again calculate the following quantities and publish them as their specific public keys of each other. Alice calculates $A_B = \alpha B_2$ and publishes it as her specific public key for Bob, (Alice's specific public key for Bob=a point A_B on the elliptic curve$E_p(a,b)$). Bob calculates $B_A = \beta A_2$ and publishes it as his specific public key for Alice, (Bob's specific public key for Alice=B_A, a point on the elliptic curve $E_p(a,b)$). The graph of the function is shown in Figure 3.

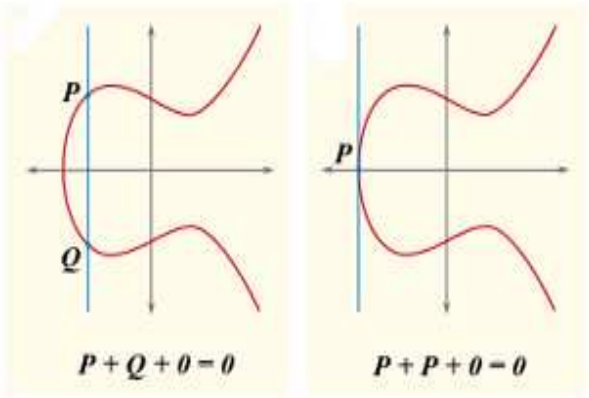

Fig 3: $P + Q + 0 = 0$ and $P + P + 0 = 0$

1. Encryption: If Bob wants to communicate the message M then all the characters of the message are coded to the points on the elliptic curve using the code table which is agreed upon by the communicating parties Alice and Bob. Then each message point is encrypted to a pair of cipher points F_1, F_2 . He uses a random number γ which is different for the encryption of different message points.

$$F_1 = \gamma Q$$
$$F_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B \qquad (24)$$

After encrypting all the characters of the message Bob converts the pair of points of each message point into the text characters using the code table. Then he communicates the cipher text to Alice in public channel.

2. Decryption: Alice receiving the cipher text, then converts the cipher text into the points on the elliptic curve and recognizes the points F_1 and F_2 of each character. Then she decrypts the message as follows.

$$M = F_2 - (\alpha F_1 + \alpha B_1 + B_A). \qquad (25)$$

Example

Considers an elliptic curve ($y^2 = x^3 + 2x + 9$) mod37, $E_{37}(2,9)$. the points on the elliptic curve $E_{37}(2,9)$. are {*, (5,25), (1,30), (21,32), (7,25), (25,12), (4,28), (0,34), (16,17), (15,26), (27,32), (9,4),(2,24), (26,5), (33,14), (11,17), (31,22), (13,30), (35,21), (23,7), (10,17), (29,6), (29,31), (10,20), (23,30), (35,16), (13,7), (31,15), (11,20), (33,23), (26,32), (2,13), (9,33), (27,5), (15,11), (16,20), (0,3), (4,9), (25,25), (7,12), (21,5), (1,7), (5,12),}

Let $Q = (9,4)$. Alice selects a random number$\alpha = 5$, any point $A = (10,20)$ on the elliptic curve. She computes

$$A_1 = \alpha(Q + A) = 5[(9,4) + (10,20)] = (1,7)$$

$$A_2 = \alpha A = (33,23).$$

She keeps the random number $\alpha = 5$ and the point A on the elliptic curve as her secret keys and publishes A_1 and A_2 as her public keys. Bob selects $\beta = 7, B = (11,20)$ on the elliptic curve. He computes

$$B_1 = \beta(Q + B) = (11,17)$$
$$B_2 = \beta B = (23,30).$$

He keeps the random number $\beta = 7$ and the point B on the elliptic curve as his secret keys and publishes B_1 and B_2 as his public keys. Alice calculates $A_B = \alpha B_2 = (15,11)$ and Bob calculates $B_A = \beta A_2 = (2,13)$. Alice publishes A_B as the specific public key for Bob and Bob publishes $B_A$as specific public key for Alice.

Encryption: If Bob wants to communicate the message 'attack' to Alice, Bob converts all the text characters of the message into the points on the elliptic curves using the agreed upon code table.

1. In the message 'attack' the first character 'a' corresponds to the point $(5, 25)$ using the code table. Bob selects a random number $\gamma = 8$ for encrypting the character 'a'. Then the point $(5, 25)$ is encrypted as $F_1 = \gamma Q = (1,30)$ this corresponds to the character 'b' in the conversion table. $F_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B = (2,13)$ This corresponds to '5' in the code table. So, the character 'a' in the plain text is encrypted to two characters $\{b,5\}$ in the cipher text.
2. 't' is a point $(10,17)$ in the code table. Let$\gamma = 12$, $F_1 = (21,32)$ this corresponds to 'c' in the code table. $F_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B = (2,24)$ This corresponds to 'l' in the code table. So, 't' is encrypted as $\{c, l\}$.
3. 't' is a point (10,17) in the code table. Let$\gamma = 19$, $F_1 = (4,9)$ this corresponds to '#' in the code table. $F_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B =$ (27,32) which corresponds to 'j' in the code table. So, 't' is encrypted as $\{\#, j\}$.
4. 'a' is a point (5,25) in the code table. Let$\gamma = 2$, $F_1 = (29,31)$ this corresponds to 'v' in the code table. $F_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B = (1,30)$ This corresponds to 'b' in the code table. So, 'c' is encrypted as$\{v, b\}$.
5. 'c' is a point (21,32) in the code table. Let$\gamma = 3$, $F_1 = (1,30)$ this corresponds to 'b' in the code table. $F_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B =$ (31, 22) which corresponds to 'p' in the code table. So, 'a' is encrypted as {b, p}.

TABLE 1: CODE TABLE

*	A	B	C
∞	(5, 25)	(1, 30)	(21,32)
d	e	f	g
(7,25)	(25,12)	(4,28)	(0,34)
h	i	j	k
(16,17)	(15,26)	(27,32)	(9,4)
l	m	n	o
(2,24)	(26,5)	(33,14)	(11,17)
p	Q	r	s
(31,22)	(13,30)	(35,21)	(23,7)
t	u	v	w
(10,17)	(29,6)	(29,31)	(10,20)
x	y	z	1
(23,30)	(35,16)	(13,7)	(31,15)
2	3	4	5
(11,20)	(33,23)	(26,32)	(2,13)
6	7	8	9
(9,33)	(27,5)	(15,11)	(16,20)
0	#	@	!
(0,3)	(4,9)	(25,25)	(7,12)
&	$	%	
(21,5)	(1,7)	(5,12)	

International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 307 Bob communicates $\{b,5;\ c,l;\ \#,j;\ v,b;\ b,p\}$as the cipher text to Alice in public channel.

Decryption: Alice after receiving the cipher text $\{b,5;\ c,l;\ \#,j;\ v,b;\ b,p\}$ converts the cipher characters into the points (1,30) ,(2,13), (21,32),(2,24) (4,9) ,(27,32) (29,31) (1,30) (1,30) (31,22). She decrypts the message taking two points at a time as the points F_1 andF_2.

1. $M = F_2 - (\alpha F_1 + \beta B_1 + B_A) = (5, 25)$ which corresponds to the character 'a' in the code table.
2. $M = F_2 - (\alpha F_1 + \beta B_1 + B_A) = (10,17)$ which corresponds to the character 't' in the code table.
3. $M = F_2 - (\alpha F_1 + \beta B_1 + B_A) = (10,17)$ which corresponds to the character 't' in the code table.
4. $M = F_2 - (\alpha F_1 + \beta B_1 + B_A) = (5,25)$ which corresponds to the character 'a' in the code table.
5. $M = F_2 - (\alpha F_1 + \beta B_1 + B_A) = (21,32)$ which corresponds to the character 'c' in the code table.

F. Projective coordinates (P)

In projective coordinates, the equation of E is

$$y^2Z = x^3 + axZ^2 + bZ^3 \qquad (26)$$

The point $(X_1 : Y_1 : Z_1)$ on E corresponds to the affine point $(X_1/Z_1, Y_1/Z_1)$ when $Z_1 \neq 0$ and to the point at infinity $P_\infty = (0 : 1 : 0)$ otherwise. The opposite of $(X_1 : Y_1 : Z_1)$ is $(X_1 : -Y_1 : Z_1)$.

1. Addition

Let $P = (X_1 : Y_1 : Z_1), Q = (X_1 : Y_1 : Z_1)$ such that $P \neq \pm Q$ and $P + Q = (X_3 : Y_3 : Z_3)$.Then the set

$$A = Y^2Z_1 - Y_1Z^2, \quad B = X^2Z_1 - X_1Z^2, \quad C = A^2Z_1Z_2 - B_3 - 2B^2X_1Z_2 \qquad (27)$$

so that

$$X_3 = BC, \quad Y_3 = A(B^2X_1Z_2 - C) - B^3Y_1Z_2, \quad Z_3 = B^3Z_1Z_2$$

2. Doubling

Let $[2]P = (X_3 : Y_3 : Z_3)$ then put

$$A = aZ_1^2 + 3X_1^2,$$
$$B = Y_1Z_1,$$
$$C = X_1Y_1B,$$
$$D = A^2 - 8C \qquad (28)$$

And

$$X_3 = 2BD, \quad Y_3 = A(4C - D) - 8Y_1^2B^2, \quad Z_3 = 8B^3$$

No inversion is needed, and the computation times are $12M + 2S$ for a general addition and $7M + 5S$ for a doubling. If one of the input points to the addition is given by $(X_2 : Y_2 : 1)$, i.e., directly transformed from affine coordinates, then the requirements for an addition decrease to $9M + 2S$.

G. Jacobian and Chudnovsky Jacobian coordinates (J and J^c)

With Jacobian coordinates the curve E is given by $y^2z = x^3 + a_4xz^4 + a_6z^6$. The point $(X_1 : Y_1 : Z_1)$ on E corresponds to the affine point $(X_1/Z_1^2, Y_1/Z_1^3)$ when $Z_1 \neq 0$ and to the point at infinity $P_\infty = (1 : 1 : 0)$ otherwise. The opposite of $(X_1 : Y_1 : Z_1)$ is $(X_1 : -Y_1 : Z_1)$.

1. Addition

Let $P = (X_1 : Y_1 : Z_1), Q = (X_1 : Y_1 : Z_1)$
$P \neq \pm Q$ and $P + Q = (X_3 : Y_3 : Z_3)$. Then
Set $A = X_1Z_2^2, B = X_2Z_1^2, C = Y_1Z_2^3,$
$D = Y_2Z_1^2, \quad E = B - A, F = D - C$
and $X_3 = -E^3 - 2AE^2 + F^2,$
$Y_3 = -CE^3 + F(AE^2 - X_3),$
$Z_3 = Z_1Z_2E.$

2. Doubling

Let $[2]P = (X_3 : Y_3 : Z_3).$
Set $A = 4X_1Y_1^2, B = 3X_1^2 + a_4Z^4_1$
and $X_3 = -2A + B^2,$
$Y_3 = -8Y_1^4 + B(A - X_3),$
$Z_3 = 2Y_1Z_1.$

The complexities are $12M + 4S$ for an addition and $4M + 6S$ for a doubling. If one of the points is given in the form $(X_1 : Y_1 : 1)$the costs for addition reduce to$8M + 3S$. The doubling involves one multiplication by the constanta_4. If it is small this multiplication can be performed by some additions and hence be neglected in the operation count. Especially if $a_4 = -3$ one can compute $T = 3X_1^2 - 3Z_1^4 = 3(X_1 Z_1^2)(X_1 + Z_1^2)$ leading to only $4M + 4S$ for a doubling. Their conclusion is that for most randomly chosen curves there exists an isogeny of small degree mapping it to a curve with$a_4 = -3$, which justifies that the curves in the standards have this parameter. The parameter $a_4 = 0$ is even more advantageous as the costs drop down to$3M + 4S$. However, this choice is far more special and the endomorphism ring $End(E)$ contains a third root of unity. In Jacobian coordinates, doublings are faster and additions slower than for the projective coordinate. To improve additions, a point P can be represented as a quintuple$(X_1, Y_1, Z_1, Z_1^2, Z_1^3)$.these coordinates are called Chudnovsky Jacobian coordinates. Additions and doublings are given by the same formulas as for J but the complexities are $11M + 3S$ and $5M + 6S$.

H. Modified Jacobian coordinates (J^m)

Modified Jacobian coordinates were introduced by Cohen et al. [COMI+ 1998]. They are based on **J** but the internal representation of a point P is the quadruple $(X_1, Y_1, Z_1, a_4Z_1^4)$ the formulas are essentially the same as for. The main difference is the introduction of $c = 8Y_1^4$ so that $Y_3 = B(A - X_3) - C$ and $a_4Z_3^4 = 2C(a_4Z_1^4)$ with the notation of Section G. An addition takes $13M + 6S$ and a doubling$4M + 4S$. If one point is in affine coordinates, an addition takes$9M + 5S$. As I takes on average between 9 and $40M$ and S is about$0.8M$, this system offers the fastest doubling procedure.

1. Example: Take $E_2: y^2 - x3 + 1132x + 278$ and let $P_2 = (1120, 1391)$ and $Q_2 = (894, 1425)$ be two affine points onE_2. We recall below the equation and the internal representation of P_2 and Q_2 for each coordinate system. Note that for projective like systems we put Z to some random value and multiply X and Y by the respective powers.

V. CONCLUSION

The elliptic curve cryptography over Galois field is solved and the addition, doubling operation over elliptic group also solved. Elliptic Curve Encryption is extending on Analog of the Diffie-Hellman Key Exchange and Cryptographic Scheme Using Elliptic Curves. (ECC) defined over finite prime fields and Choice of the coordinates at affine coordinates. The projective coordinates are solved in the three dim with two operations. Jacobian coordinates also are solved with two

operations. Modified Jacobian coordinates (J^m) are solved in example.

XI. REFERENCES

[1] National Institute for Standards and Technology, Digital signature standard", FIPS Publication 186, 1993. Available from http://csrc.ncsl.nist.gov/fips/.

[2] Ayan Mahalanobis, Di_e-Hellman Key Exchange Protocol, 2005, Florida Atlantic University Boca Raton, Florida.

[3] H. K. Das, Introduction to Engineering Mathmatics, 2010, S.chand & company Ltd.

[4] N. Koblitz, A Course in Number Theory and Cryptography, 2nd edition, Springer- Verlag, 1994.

[5 Reza Rezaeian Farashahi, Curves and Jacobians: Number Extractors and Efficient Arithmetic, 2008, Eindhoven University Press.

[6] Mark Stamp Richard M. Low, Appll Ed Cryptanalysis Breaking Ciphers In The Real World, The Wiley Bicentennial-Knowledgef Or Generations, Pp193-203, (2007).

[7] Takeo Kanade, Lecture Notes in Computer Science, May 26-28, 2010, Springer.

[8] Henri Cohen Gerhard Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, 2006, Chapman & Hall/CRC Taylor & Francis Group.

[9] Jonathan C. Herzog Diffi-Hellman key exchange, 2006, p65-p70, Chapman & Hall/CRC.

[10] Lawrence C. Washington, Introduction to Cryptography with Coding Theory , Prentice Hall, Pp137-142, (2002).

[11] N. Koblitz, A Course in Number Theory and Cryptography, 2nd edition, Springer- Verlag, 1994.

[12] William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, November 16, 2005, Prentice Hall.

[13] A. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

[14] Behrouz A. Forouzan , Data Communications And Networking / Behrouz A. Forouzan. -- 4th Ed, Mcgraw-Hill Forouzan Networking Series, Pp 935-956, (2007).

[15] Andreas Enge, Elliptic curve and their application to cryptography an introduction, 2009, Liuwer Academic Publisher.

[16] Tim G¨uneysu, Christof Paar, Jan Pelzl, on the security of elliptic curve cryptosystems against attacks with special-purpose hardware, may2012**,** http://www.researchgate.net/publication/228589576_On_the_security_of_elliptic_curve_cryptosystems_against_attacks_with_special-purpose_hardware.