International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

Elliptic Curves and their Applications in Cryptography

Preeti Sharma
M.Tech Student
Mody University of Science and Technology,
Lakshmangarh

Nisheeth Saxena
Assistant Professor
Mody University of Science and Technology,
Lakshmangarh

***Abstract* – This paper gives an introduction to elliptic curves. The basic operations of elliptic curves and Elliptic curve arithmetic are described further. How Elliptic curves are useful for Elliptic curve cryptography is also discussed. Various algorithm of ECC are mentioned. The paper also discusses the basics of prime and binary field arithmetic.**

Keywords: Elliptic Curves, Discrete Logarithm Problem, Elliptic Curve Cryptography, Public Key Cryptography.

I. INTRODUCTION

In an open network such as internet, Data security is very important. The data transferred from the one system to the over public network can be secure by the method of encryption. Various cryptographic technologies are already present to protect data during transmission over the internet. Public key cryptography system are based on sound mathematical foundations that are designed to make the problem hard for an intruder to break into the system. Various public key algorithm are DH, RSA, DSA, ECDH and ECDSA.

The use of elliptic curves in public key cryptography was indenpendently proposed by Koblitz and Miller in 1985 [1] and up till now enormous amount of work has been done.

Elliptic curves cryptography (ECC) is a newer approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields, with a novelty of low key size for the user, and hard exponential time challenge for an intruder to break into the system, In the ECC a 160 bits key, provides the same security as the RSA 1024 bits key, thus the lower computer power is required. The advantage of the elliptic curve cryptosystem is the absence of the sub exponential time of algorithms, for attack.

The principal attraction of the ECC, compared to the RSA is that it appears to offer equal security for a smaller key size, thus reducing the processing overhead.

II. ELLIPTIC CURVES

The Elliptic curves are not ellipses [2]. They are named as the Elliptic curves because they are described by the cubic equations, and equations with highest degree three. An elliptic curve is a smooth and projective algebraic curve, on which there is a specified point of O, which called as point at infinity and ZERO POINT. An elliptic curve E in its standard form is described as the

$$Y^2 = X^3 + AX + B$$

This is a cubic equation as highest degree of this equation is three. Where, the values of 'A' and 'B' are predefined and the $4A^3 + 27B^2 \neq 0$.where all the calculations are performed modulo p. Every value of the 'A' and 'B' gives a different elliptic curve. All the points of (X, Y) which satisfies the above equation of plus a point at infinity lies on the elliptic curve.

The variables and coefficients of the elliptic curve equation are restricted to the elements in a finite field, which results in the definition of the finite Abelian group.

III. ABELIAN GROUPS

An abelian group is a set, A, together through an operation '*' that combines any of the two elements a and b to form of another element of denoted a * b. The symbol '*' is a general place holder for a concretely given operation. To qualify as an abelian group, the set and operation, (A, *), must satisfy five requirements known as the Abelian group of axioms:

Closure: For all the, *b* in *A*, the result of the operation '*a* * *b*' is also in *A*.

Associativity: For all *a*, *b* and *c* in *A*, the equation (*a* * *b*) * *c* = *a* * (*b* * *c*) holds.

Identity element: There exists an elements *e* in *A*, such that for all the elements *a* in *A*, then the *e* * *a* = *a* * *e* = *a* holds.

Inverse element: For each *a* in *A*, there exists an the element *b* in *A*,as *a* * *b* = *b* * *a* = *e*, *e* is the identity element.

Commutativity: For all *a*, *b* in *A*, *a* * *b* = *b* * *a*.

The Discrete logarithm problem:

Consider the equation Q = kP, where the Q,P belong to the $E_p(a, b)$ and k < p:

- If k and p are given, it is very easy to compute Q.
- But if the P and Q are given, it is comparatively hard to determine the k, if k is sufficiently large.

This is the Discrete logarithm Problem for the Elliptic Curve [2] and due to the complexity of the Discrete logarithm Problem Elliptic curve cryptography is hard to break.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

IV.ELLIPTIC CURVE OVER REAL NUMBERS

The Elliptic curves are defined over the real numbers. In the equation:

$$Y^2 = X^3 + AX + B$$

A and B are the real numbers, X and Y take on the values in real numbers. When the values of A and B are given, the plot consists of both positive and negative values of Y for each value of X. Thus each curve is symmetric about Y=0.

V. BASIC OPERATIONS ON ELLIPTIC CURVES

A. Point Multiplication

The basic operations of elliptic curve involve point multiplication which is achieved by point addition and point doubling. In the point multiplication a point on the Elliptic Curve say the P is multiplied with a positive integer to obtain the another point of Q on the same Elliptic curve, using the Elliptic curve equations.

i.e. Q = KP

Let K = 15

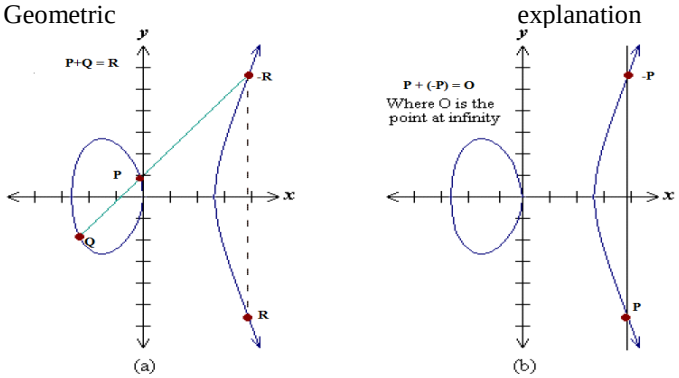
So, Q = 15 P= (2 (2 (2P+P) +P)) + P

So this example shows that the point multiplication is consummate by using the point addition and the point doubling repeatedly to get the result. This method is named as double and adds method. There are the other efficient methods for the point multiplication such as the NAF (Non – Adjacent Form) and wNAF the method for the point multiplication [3].

B. Point Addition:

It is the addition of the two points of the elliptic curve, say P and Q , to get another point R on the same Elliptic curve.

Geometric explanation



Consider the 2 point of P and Q on the Elliptic curve as shown in the figure (a).

Then two conditions arises

- If Q =! –P, then a line drawn through the points of P and Q will intersect the Elliptic curve at exactly one more point –R. The reflection of the –R gives the point R, with respect to the x axis. The R point is the result of the addition of P and Q.Thus R = P+Q
- If Q = -P, the line through this point intersect at a point at the infinity O.

Hence Q + (-Q) = O, where O is additive identity of the Elliptic curve group, shown in the figure (b).

Analytical Explanation:

Consider the two distinct points $P(X_P, Y_P)$ and $Q(X_Q, Y_Q)$ .The slope of line joining these two points is S.

$$s = (Y_Q - Y_P)/(X_Q - X_P)$$

As we know that the R = P + Q, and R is also the point on EC so the coordinates of the R (X_R, Y_R) are calculated by-

$$X_R = S^2 - X_P - X_Q$$

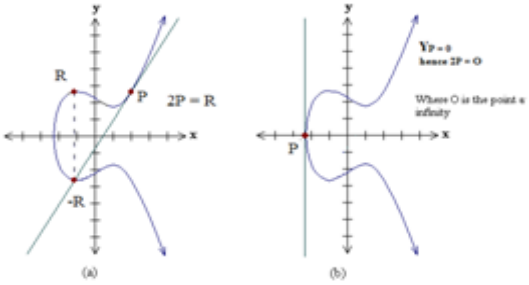
$$Y_R = -Y_P + S(X_P - X_R)$$

C. Point Doubling:

The Point doubling is addition of a point say P to itself to get the another point on the elliptic curve.

So the R = P+P =2P

Geometric explanation:



To double a point P to get R, i.e. to find R = 2P, consider a point P on an Elliptic Curve as shown in figure (a). If y coordinate of the point J is not zero then the curve line at P will intersect the elliptic curve at accurately one more point –R. The reflection of the point –R with respect to x-axis gives the point R, which is the result of doubling the point P.

Thus R = 2P.

If y coordinate of the point P is zero then the curve at this point intersects at a point at infinity O. Hence 2P = O when $Y_P = 0$. This is shown in the figure (b).

Analytical Explanation:

Consider a point $P(X_P, Y_P)$where X_p =! 0

Let the R = 2P, $R(X_R, Y_R)$

Then the coordinates of $R(X_R, Y_R)$are calculated by-

$$X_R = S^2 - 2X_P$$

$$Y_R = S(X_P - X_R) - Y_R$$

S is the curve at the point P and a is the parameter chosen with the Elliptic Curve.

$$S = (3X_P^2 + a)/2Y_P$$

If the yP = 0, then 2J = O, where O is the point at infinity and zero point.

Note: The operation defined above are on real numbers. Operation over the actual numbers are slow and incorrect due to round off error. To make cryptographic operation fast and accurate and more efficient the Elliptic Curve Cryptography is defined over the two finite fields described in the next section.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

VI. ELLIPTIC CURVE CRYPTOGRAPHY IS DEFINED OVER TWO FINITE FIELDS

- Elliptic curves over Prime Field Fp
- Elliptic curves over Binary Field F_{2^m}

The variables and the coefficients of Elliptic Curve equation are all restricted to these finite fields. The operations in these sections are defined on affine coordinate system, which is a normal coordinate system in which each point is represents by vector(X,Y).

Elliptic curves over Prime Field Fp:
The cubic equation for the Prime Field Fp is-

$$Y^2 \bmod p = (X^3 + AX + B) \bmod p, \text{ where}$$

$$4A^3 + 27B^2 \bmod p \neq 0.$$

So the values of variables and coefficients of cubic equation are between 0 through p-1(set of integers), in this finite field. All the operations as addition, subtraction, multiplication, division are performed in modular arithmetic and the values are chosen from 0 and p-1.to make cryptosystem more secure the Prime no p is chosen in a such way that there is finitely large number of points on elliptic curve.SEC specifies curves with p ranging between 112-521[4]. The algebraic rules for point addition and point doubling can be adapted for elliptic curves over Fp. So the operations of elliptic curve over prime field Fp are described below

Point Addition
Consider the two distinct points P and Q such that P = (X_P, Y_P) and Q = (X_Q, Y_Q)
Let R = P + Q where R = (X_R, Y_R), then
$X_R = (s^2 - X_P - X_Q) \bmod p$
$Y_R = (s (X_P - X_R) - Y_P) \bmod p$
$s = ((Y_P - Y_Q)/(X_Q - X_P)) \bmod p$, s is the slope of line through P and Q.
If Q = -P i.e. Q = $(X_P, -Y_P \bmod p)$ then P + Q = O. where O is point at infinity.
If Q = P then P + Q = 2P then the point doubling equations are used.
Also P + Q = Q + P

Point Subtraction
Consider two the distinct points P and Q such that P = (X_P, Y_P) and Q = (X_Q, Y_Q)

Then the P - Q = P + (-Q) where -Q = $(X_Q, -Y_Q \bmod p)$
The Point subtraction is used in the certain employment of the point multiplication such as NAF.

Point Doubling
Consider a point P such that the P = (X_P, Y_P), where $Y_P \neq 0$
Let R = 2P where the R = (X_R, Y_R), Then
$X_R = (s^2 - 2X_P) \bmod p$
$Y_R = (s(X_P - X_R) - Y_P) \bmod p$
$s = ((3X^2_P + a) / (2Y_P)) \bmod p$, s is the curve at the point P and a, is one of the parameters chosen with the elliptic curve.
If the $Y_p = 0$ then 2P = O, where O is point at the infinity.

In case of the finite group $E_p(a,b)$, the numbers of the points N is bounded by-

$$p + 1 - 2\sqrt{p} \leq p + 1 + 2\sqrt{p}$$

Example: Consider an Elliptic Curve $E_{29}(1, 1)$, its equation is given by:-

$$Y^2 \bmod 29 = (X^3+X+1) \bmod 29 \qquad (1)$$

Where prime no is p = 29,

And the constants of the prime field (A,B) be (1,1), as satisfying the following condition.

$$4A^3+27B^2 \bmod p \neq 0.$$

Consider the affine coordinates of prime field (X,Y) be (0,1) calculated by eq(1).So, other points satisfying the eq (1) are given in Table 1, they are found on Elliptic Curve.

Table 1: set of points on EC

(1,1)	(1,12)	(1,4)
(1,9)	(4,2)	(4,11)
(5,1)	(5,12)	(7,0)
(8,1)	(8,12)	(10,6)
(10,7)	(11,2)	(11,11)

This table can be extended further; we have shown only the few points.

The Point addition and the point doubling are basic the EC operations as mentioned earlier. The Elliptic curve cryptographic primitives require scalar point multiplication. When the point multiplication, i.e. the point addition or the point doubling is performed on a point of the EC it is compulsory that the resulting point should also lie on same EC, this is described by the example given below.

Point Addition:
Let two points of the EC P(6,7) and Q (10,5).
Let a third point R(X_R,Y_R)

So R=P+Q
By the equations mentioned in the point addition in section,

S = 14
$X_R = 6$
$Y_R = 22$
So R (6,22) is achieved by point addition method and this point is also on Elliptic Curve $E_{29}(1,1)$.

Point Doubling:
In point doubling both the point are same i.e.
P=Q.
So R = P+P
Let P(6,7)
By the point doubling equations
S = 14
$X_R = 10$
$Y_R = 24$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

So R(10,24) is achieved by the point doubling method and this point is also on the Elliptic Curve E_{29} (1,1).

Elliptic curves over Binary Field F_2^m:

The equation of the Elliptic Curve on a binary field F_2^m is $Y^2 + XY = X^3 + AX^2 + B$,

Where$B \neq 0$. The elements of the finite field are integers of length at most m bits. These numbers can be considered as a binary polynomial of degree m-1. In binary polynomialthe coefficients can only be 0 or 1. Polynomials of degree m – 1 or lesser are in all the operation such as addition, subtraction, division, multiplication. To make the cryptosystem secure the m is chosen in such a way that there is finitely large number of points on the elliptic curves. The SEC specifies curves with ranging between 113-571 bits [5].

The algebraic rules for point addition and point doubling can be adapted for elliptic curves over F_2^m. So the operations of the elliptic curve over Binary field $F_2^m$are described below.

Point Addition

Consider the two distinct points P and Q such that P $=(X_P, Y_P)$ and Q = (X_Q, Y_Q)

Let R = P + Q where R = (X_R, Y_R), then

$X_R = S^2 + S + X_P + X_Q + a$

$Y_R = s (X_P + X_R) + X_R + Y_P$

$s = (Y_P + Y_Q)/(X_Q + X_P)$, s is the slope of line through P and Q.

If Q = -P i.e. Q = $(X_P, X_P + Y_P)$ then P + Q = O. where O is the point at infinity.

If Q = P then Q + P = 2P then the point doubling equations are used.

Also Q + P = P + Q

Point Subtraction

Consider the two distinct points P and Q such that P = (X_P, Y_P) and Q = (X_Q, Y_Q)

Then the P - Q = P + (-Q) where -Q = $(X_Q, X_Q + Y_Q)$

The Point subtraction is used in the certain implementation of the point multiplication such as NAF.

Point Doubling

Consider a point P such that the P = (X_P, Y_P), where $X_P \neq 0$

Let R = 2P where R = (X_R, Y_R)Then

$X_R = S^2 + S + a$

$Y_R = X_P^2 + (s + 1) * X_R$

$s = (X_P + Y_P)/ X_P$, S is the tangent at the point P and a is one of the parameters chosen with the Elliptic Curve.

If $X_P = 0$ then 2P = O, where O is the point at the infinity.

VII. FIELD ARITHMETIC

For the operation performed in ECC modular arithmetic or polynomial arithmetic is chosen. These arithmetic's are described below:

- Modular Arithmetic: The modular arithmetic performed on a no say 'p' involves arithmetic in range from 0 to p-1. If in any operation the number falls out of this range then result is wrapped around to fall in the range 0 to p-1. And for that mod operator is used.
- Polynomial Arithmetic: In Binary Field F_2^m arithmetic of integer of the length m bits is used. These number scan be considered as binary polynomial of degree m-1.

Consider a binary string (R_{m-1}…… R_1 R_0) can be expressed as the polynomial

$R_{m-1}x_{m-1} + R_{m-2}x_{m-2} + ... + R_2 x_2 + R_1x + R_0$ where R_i = 0 or 1.

For e.g., a 4 bit number 1001 can be represented by polynomial as x3 + 1.

In polynomial arithmetic there is an irreducible polynomial of degree m that is similar to the modulus p on modular arithmetic.

In binary polynomial the coefficients of the polynomial can be either 0 or 1. If in any operation the coefficient becomes greater than 1, it can be reduce to 0 or 1 by modulo 2 operation on the coefficient.

VIII. ELLIPTIC CURVE DOMAIN PARAMETERS

When two parties communicate, then prior to communication they should agree upon some parameters to have a secured and trusted communication using ECC. These parameters are called Domain parameters. There parameters are specific for both prime field and binary field describe below. There are several standard domain parameter defined by SEC. Domain parameters are specified before the communication begins.

Domain parameters for the EC over Prime Field $F_p$are (p, a, b, G, n, h).

Domain parameters for the EC over Binary field $F_2^m$are (m, f(x), a, b, G, n and h).

Where, p is the prime number defined for finite field.

a and b are the constants,

G is the generator point/base point (X_G, Y_G) point on the elliptic curve chosen for the cryptographic operations,

N is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between 0 and n-1,

h is the cofactor where h must be small (h<= 4) and, preferably h=1,

m is an integer defined for the finite field F_2^m. The elements of finite field F_2^m are integers of the length at most m bits,

f(x) is the complex polynomial of the degree m used for the elliptic curve operations.

IX. EC CRYPTOGRAPHY

Elliptic Curve Cryptography is a public key cryptography. In the public key cryptography each user or device taking part in the communication generally have a pair of keys i.e. a public key or a private key, and a set of the operations associated with the keys to do the cryptographic processes. The private key is known only to the particular user whereas the public key is distributes to all users talking part in the communication. The EC algorithm are specified in the communication. The EC algorithm are specified in the *SEC1: Elliptic Curve Cryptography* [6] .EC the cryptographic algorithms for key agreement and the digital signature are explained below.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

A. ECDSA-Elliptic Curve Digital Signature Algorithm:

A message sent by a device to another device should be authenticated and for that signature algorithm is used is used. For example consider two devices M and N. M sends a message to N.

To authenticate that message device M sign the message using its private key. Then device M sends that message and the signature to device N.

N verifies the signature by using the public key of device M. Since the device N knows M's public key, it can be verify that that message is sent by M and not.ECDSA is a variant of Digital Signature Algorithm that operates on the elliptic curve groups [7]. Before sending the signed messages both devices should agree up on the Elliptic Curve domain parameters. The Sender 'M' have a pair of the keys consisting of a private key P_M (which is randomly selected the integer less than n, where n is the order of the curve, an elliptic curve domain parameter) and a public key $U_M = P_M * G$ (G is the generator point, and the elliptic curve domain parameter). An overview of ECDSA process is defined below.

Signature Generation

For signing a message F by sender M, using M's private key P_M

1. Calculate e = HASH (F), where HASH is a cryptographic hash function, such asSHA-1
2. Select a random integer k from the [1,n − 1]3.
3. Calculate r = x1 (mod n), where (x1, y1) = k * G. If r = 0, go to step 2
4. Calculate $s = k^{-1} (e + P_M r)(\text{mod } n)$. If s = 0, go to step 2
5. The signature is the pair (r, s).

Signature Verification

For B to authenticate M's signature, N must have M's public key U_M

1. Verify that r and s are integers in [1,n − 1]. If not, the signature is invalid
2. Calculate e = HASH (F), where HASH is the same function used in the signature generation
3. Calculate the $w = s^{-1} (\text{mod } n)$
4. Calculate $u_1 = ew (\text{mod } n)$ and $u_2 = rw (\text{mod } n)$
5. Calculate the $(x1, y1) = u_1G + u_2U_M$
6. The signature is valid if x1 = r(mod n), invalid otherwise.

B. ECDH – Elliptic Curve Diffie Hellman:

ECDH is a key agreement protocol that allows two communicating parties to generate a shared secret key. This shared secret key can be used for private key algorithms. To generate a shared key between M and N using ECDH, Both have to approve upon the EC domain parameters revealed earlier.

Note: Any third party, who doesn't have access to the private details of each devices, will not be able to calculate the shared secret from the available public information.

An overview of ECDH process is defined below.

The EC domain parameters used are:

$E_q(A,B)$: Elliptic curve with the parameters A,B,q where q is prime number and an integer of form 2^m

G: the generator point on the elliptic curve whose order is large value n.

Both the devices M and N have a key pair consisting of a private key P (a randomly selected integer less than n, where n is the order of the curve, an elliptic curve domain parameter) and a public key U=P*G (G is the generator point, an the elliptic curve domain parameter).

The process of key exchange between M and N

1. M have a pair (P_M,U_M), where $U_M = P_M * G$
2. N have a pair (P_N,U_N), where $U_N = P_N * G$
3. M calculates its secret key $K = P_M * U_N$
4. N calculates its secret key $K = P_N * U_M$

Secret Key generated by both the devices is same, as-

$K = P_M * U_N = P_N * U_M$

$= P_M * P_N * G = P_N * P_M * G$

Elliptic curve with Elgamal System:

1. Bob choose elliptic curve E (a, b) over GF (p) and GF (2^n).
2. Bob choose a point on the curve $e_1(x_1, y_1)$
3. Bob choose an integer d.
4. Bob calculate $e_2(x_2, y_2) = d * e_1(x_1, y_1)$.
5. Bob announce E (a, b, p), $e_1(x_1, y_1)$ and $e_2(x_2, y_2)$ as your public key and keeps d as private key.

Encryption:

Alice selects P, point on the curve, as her plain text. She chose a random number r and computes

$$C_1 = r * e_1$$

$$C_2 = P + r * e_2$$

Decryption:

Bob after receiving C_1 and C_2, computes

$$P = C_2 - d * C_1$$

It can be explained as P + r * e2 - d * r * e1

=> P + r * d * e1 - d * r * e1 => P+O=P

$$P + r * e_2 - d * r * e_1 \Rightarrow P + r * d * e_1 - d * r * e_1$$

$$\Rightarrow P + O = P$$

X. APPLICATIONS

Elliptic curve cryptography is widely used in many of the areas[8].

Smart Cards

ECC is most popularly used in smart cards. Smart cards are being used as bank (credit/debit) cards, electronic tickets and personal identification (or registration) cards. Many manufacturing companies are producing smart cards that make use of elliptic curve digital signature algorithms. These manufacturing companies include Phillips, Fujitsu, MIPS Technology and Data Key, while vendors that sell these smart cards include Funge Wireless and Entrust Technologies.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

PDAs

PDAs have more computing power compared to most of the other mobile devices, like cell phones or pagers. PDAs are considered to be a very popular choice for implementing public key cryptosystems. But ECC is idol choice for PDAs because they still grieve from the limited bandwidth.

PCs

For implementing the ECC, Constrained devices have been considered to be the most suitable platforms. Recently, several companies have created software products that can be used on PCs to secure data, encrypt e-mail messages and even instant messages with the use of ECC.

CONCLUSION

In this paper we have provided an overview of Elliptic Curves and their operations. We have seen further what Elliptic curve arithmetic is and how they are solved. The use of Elliptic Curves in public key cryptography i.e. Elliptic Curve cryptography is describe in this paper. It is important that the point multiplication and field arithmetic should be efficient for efficient implementation of ECC. There are different methods for efficient implementation point multiplication and field arithmetic suited for different hardware configurations. Further we have mentioned the application areas of ECC.

REFERENCES

[1] N.Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation,volA8, 1987, pp.203 -209.
[2] W. Stallings,“ Cryptography and Network Security”, Prentice Hall, Fourth Edition.
[3] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes, Software Implementation ofElliptic Curve Cryptography over Binary Fields, 2000
[4] Certicom, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic CurveDomain Parameters, Version 1.0, September 2000
[5] Anoop MS, Elliptic curve cryptography : An implementation Guide
[6] Certicom, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography,Version 1.0, September 2000
[7] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of AppliedCryptography, CRC Press, 1996
[8] Standard specifications for public key cryptography, IEEE standard,pI363,2000.